CyFun®

CyberFundamentals 2025

Deutsch

Version 2025-10-01

INHALTSÜBERSICHT

EINFÜHRUNG

Das CyberFundamentals Framework ist ein Rahmenwerk, das dem Centre for Cybersecurity Belgium (CCB) gehört. Das Rahmenwerk besteht aus einer Reihe konkreter Maßnahmen und bietet ein klares, schrittweises Konzept, das Organisationen hilft:

- ihre Daten zu schützen,
- ihr Risiko für die häufigsten Cyberangriffe deutlich verringern,
- und ihre Cyberresilienz zu verbessern.

Die Anforderungen, die auch als Kontrollen oder Maßnahmen bezeichnet werden, werden durch relevante Erkenntnisse aus dem NIST Cybersecurity Framework[1], ISO 27001/ISO 27002, IEC 62443 und den CIS Critical security Controls (ETSI TR 103 305-1) unterstützt.

Das Rahmenwerk basiert auf **sechs Kernfunktionen**: regeln, identifizieren, schützen, erkennen, reagieren und wiederherstellen. Diese sechs Funktionen unterstützen eine klare Kommunikation in allen Bereichen der Organisation, sowohl im technischen als auch im nicht-technischen Bereich, und erleichtern so das Verständnis, die Gespräche und den Umgang mit Cyberrisiken. Durch die Verwendung einer gemeinsamen Sprache tragen sie dazu bei, die Cybersicherheit in umfassendere Geschäftsentscheidungen und in die Gesamtstrategie für das Risikomanagement zu integrieren.

- **Regeln**: Stellt sicher, dass die Cybersicherheit als strategische Priorität behandelt wird und nicht nur als technisches Thema. Dieser Punkt legt klare Erwartungen, Richtlinien, Zuständigkeiten und Befugnisse fest und sorgt dafür, dass diese in der gesamten Organisation bekannt gemacht und überprüft werden.
- **Identifizieren**: Hilft dabei, ein klares Verständnis dafür zu entwickeln, was für die Organisation am wichtigsten ist, z. B. Systeme, Mitarbeiter, Vermögenswerte, Daten sowie die Prozesse und Tools, die den Betrieb unterstützen. Diese Funktion hilft bei der Erkennung potenzieller Cyber-Bedrohungen und bildet die Grundlage für fundierte Entscheidungen über den Umgang mit Cybersicherheitsrisiken.
- **Schützen**: Es geht darum, Schutzmaßnahmen zu ergreifen, um die Wahrscheinlichkeit eines Cybervorfalls zu verringern oder seine Auswirkungen zu begrenzen. Dazu gehören technische Maßnahmen, Verfahren und Sensibilisierungsmaßnahmen.
- **Erkennen**: Unterstützt die Fähigkeit, Cybersicherheitsereignisse schnell zu erkennen. Eine frühzeitige Erkennung trägt zur Schadensbegrenzung bei und ermöglicht eine schnellere Reaktion.
- **Antworten**: Umfasst die Maßnahmen, die ergriffen werden, wenn ein Vorfall im Bereich der Cybersicherheit eintritt. Dies hilft, das Problem einzudämmen, die Kommunikation zu koordinieren und Störungen zu reduzieren.
- **Wiederherstellen**: Konzentriert sich auf die Wiederherstellung der betroffenen Services und Abläufe nach einem Vorfall. Dazu gehört auch, aus dem Vorfall zu lernen, um die Resilienz für die Zukunft zu verbessern.

1 Die Kodierung der Anforderungen entspricht den im NIST CSF Framework verwendeten Codes. Da nicht alle Anforderungen des NIST CSF anwendbar sind, können einige Codes, die im NIST CSF Framework vorhanden sind, fehlen.

Der CyberFundamentals Framework verwendet ein proportionales Sicherheitsmodell mit drei Sicherheitsstufen: *Basic*, *Important* und *Essential*, dem eine Einstiegsstufe vorangestellt ist: *Small*.

Die Einstiegsstufe **Small** ermöglicht es einer Organisation, eine erste Bewertung vorzunehmen. Sie ist für Mikro-Organisationen oder Organisationen mit begrenzten technischen Kenntnissen gedacht.

Die Sicherheitsstufe **Basic** umfasst Anforderungen an die Informations- und Cybersicherheit, die für alle Organisationen gelten. Sie bietet ein zuverlässiges Schutzniveau, indem sie Technologien und Verfahren einsetzt, die im Allgemeinen bereits verfügbar sind. Gegebenenfalls können diese Anforderungen angepasst und verbessert werden, um den spezifischen Bedürfnissen der Organisation besser zu entsprechen.

Auf der Sicherheitsstufe **Important** werden grundlegende Sicherheitsmaßnahmen verstärkt, um bekannte Cyberrisiken zu verringern und die Auswirkungen von Angriffen zu begrenzen, die von Bedrohungsakteuren mit begrenzten Ressourcen und Fähigkeiten durchgeführt werden.

Auf der Sicherheitsstufe **Essential** werden die Sicherheitsmaßnahmen der Sicherheitsstufe Important weiter verstärkt, um die höchsten Cybersicherheitsanforderungen zu erfüllen. Diese Maßnahmen umfassen moderne Sicherheitsfunktionen und sind so konzipiert, dass sie ausgefeilten Cyberangriffen standhalten, die von Bedrohungsakteuren mit erheblichen Ressourcen und Fachkenntnissen durchgeführt werden.

Kontrollen in Bezug auf Managementaspekte müssen bei jedem Zertifizierungsaudit – unabhängig davon, ob es sich um ein Erstaudit, ein Überwachungsaudit oder ein Rezertifizierungsaudit handelt – überprüft werden, wenn die CyFun®-Sicherheitsstufe „Essential“ auditiert wird. Diese Kontrollen entsprechen den Managementsystemprinzipien, die Zertifizierungsstellen gemäß ISO/IEC 17021-1 bei der Auditierung jeder Art von Managementsystem bewerten müssen.

Auf der Grundlage gängiger Arten von Cyberangriffen werden bestimmte Anforderungen als „**Schlüsselmaßnahmen**“ festgelegt. Diese müssen auf dieser Sicherheitsebene zusätzlich zu den Schlüsselmaßnahmen, die bereits auf der Sicherheitsebene Basic und der Sicherheitsebene Important gefordert werden, behandelt werden.


POLICIES

REGELN

Regeln

Die Umstände – Auftrag, Erwartungen der Stakeholder, Abhängigkeiten sowie gesetzliche, behördliche und vertragliche Anforderungen – im Zusammenhang mit den Entscheidungen der Organisation zum Management von Cybersicherheitsrisiken wurden verstanden.

GV.OC-01 Der Auftrag der Organisation wurde verstanden und fließt in das Cybersicherheitsrisikomanagement

GV.OC-01.1 Der Auftrag der Organisation wird festgelegt und kommuniziert und bildet die Grundlage für das Informations- und Cybersicherheitsrisikomanagement.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Mission der Organisation klar definiert und kommuniziert wird und als Grundlage für das Management von Informations- und Cybersicherheitsrisiken dient. Das Verständnis des Auftrags hilft zu erkennen, welche Risiken die Erreichung der strategischen Ziele beeinträchtigen könnten.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Der Auftrag der Organisation sollte durch Materialien wie Visions- und Missionserklärungen, Dienstleistungsstrategien oder Marketingdokumente vermittelt werden. Dies hilft bei der Ermittlung und Priorisierung von Risiken.
- Geschäftsprozesse und strategische Ziele sollten unter Berücksichtigung der Informations- und Cybersicherheit entwickelt werden. Dazu gehört auch das Verständnis, wie sich Risiken auf den Betrieb, Vermögenswerte, Einzelpersonen, Partner oder umfassendere gesellschaftliche Interessen auswirken können.
- Die Notwendigkeit des Schutzes sensibler Informationen, einschließlich personenbezogener Daten, sollte auf der Grundlage des Auftrags der Organisation und der Funktionsweise ihrer Systeme und Services beurteilt werden.
- Der Auftrag und die damit zusammenhängenden Geschäftsprozesse sollten regelmäßig, z. B. einmal im Jahr, überprüft werden, um sicherzustellen, dass sie relevant bleiben und weiterhin ein wirksames Risikomanagement unterstützen.

GV.OC-02 Interne und externe Stakeholder wurden verstanden und ihre Bedürfnisse und Erwartungen an das Management von Cybersicherheitsrisiken wurden verstanden und berücksichtigt

GV.OC-02.1 Die Organisation weist nach, dass sie die Bedürfnisse und Erwartungen sowohl interner als auch externer Stakeholder hinsichtlich des Managements von Informations- und Cybersicherheitsrisiken versteht und berücksichtigt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation die Bedürfnisse und Erwartungen sowohl interner als auch externer Stakeholder versteht und berücksichtigt, wenn sie Informations- und Cybersicherheitsrisiken managt. Dies trägt dazu bei, die Bemühungen im Bereich der Cybersicherheit mit den geschäftlichen Prioritäten, den rechtlichen Verpflichtungen und dem Vertrauen der Stakeholder in Einklang zu bringen.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Die Organisation sollte die wichtigsten internen Stakeholder wie Mitarbeiter, leitende Angestellte, Vorstandsmitglieder und interne Auditoren ermitteln. Ihre Rollen, Verantwortlichkeiten und Erwartungen in Bezug auf Cybersicherheit sollten verstanden und dokumentiert werden.
- Die wichtigsten externen Stakeholder, darunter Kunden, Lieferanten, Partner, Aufsichtsbehörden, Aktionäre, Dienstleister und externe Auditoren, sollten identifiziert und ihre Erwartungen in Bezug auf Compliance, Verträge und Datenschutz berücksichtigt werden.
- Die Bedürfnisse und Erwartungen der Stakeholder sollten mit Hilfe von Methoden wie Interviews, Umfragen, Vertragsprüfungen oder regulatorischen Analysen erfasst werden.
- Diese Erkenntnisse sollten in die Strategie zum Management von Cybersicherheitsrisiken des Unternehmens integriert werden, um eine Abstimmung mit den geschäftlichen und gesetzlichen Prioritäten zu gewährleisten.
- Es sollten regelmäßige Kommunikationskanäle eingerichtet werden, um die Stakeholder zu informieren und in Fragen der Cybersicherheit einzubeziehen.
- Die Erwartungen der Stakeholder sollten in regelmäßigen Abständen überprüft und aktualisiert werden, vor allem wenn sich die Geschäftsabläufe, die rechtlichen Anforderungen oder die Risikoexposition ändern.

GV.OC-03 Gesetzliche, behördliche und vertragliche Anforderungen an die Cybersicherheit werden verstanden und gemanagt

GV.OC-03.1 Gesetzliche und behördliche Anforderungen an die Informations- und Cybersicherheit werden ermittelt und umgesetzt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass gesetzliche, behördliche und vertragliche Anforderungen in Bezug auf die Informations- und Cybersicherheit ermittelt, überwacht und umgesetzt werden.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Es sollte ein Verfahren eingerichtet werden, um die einschlägigen rechtlichen und regulatorischen Anforderungen in Bezug auf die Informations- und Cybersicherheit zu verfolgen und anzuwenden.
- Diese Anforderungen sollten in alle relevanten Strategien, Verfahren und Geschäftsprozesse integriert werden.

- Zu den Bereichen, die abgedeckt werden sollten, gehören unter anderem:
  - Risikobewertung und Schutz von Informationssystemen
  - Reaktion auf Vorfälle, Geschäftskontinuität und Krisenmanagement
  - Sicherheit der Lieferkette und sichere Systementwicklung
  - Schwachstellenmanagement und sichere Konfiguration
  - Sicherheitsbewusstsein und Schulung
  - Kryptographische Kontrollen und sichere Kommunikation
  - Notfall-Kommunikationssysteme
  - Zugangskontrolle, Asset-Management und Multi-Faktor-Authentifizierung (MFA)
  - Koordinierte Offenlegung von Schwachstellen

GV.OC-03.2 **Gesetzliche, regulatorische und vertragliche Verpflichtungen im Zusammenhang mit der Informations- und Cybersicherheit werden kontinuierlich verwaltet, um sicherzustellen, dass sie korrekt und aktuell sind und wirksam angewendet werden.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die rechtlichen und behördlichen Anforderungen in Bezug auf die Informations- und Cybersicherheit kontinuierlich verwaltet, auf dem neuesten Stand gehalten und in der gesamten Organisation wirksam angewendet werden.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Es sollte ein strukturierter Prozess vorhanden sein, um die rechtlichen und regulatorischen Anforderungen in Bezug auf die Informations- und Cybersicherheit laufend zu erfüllen.
- Diese Anforderungen sollten dokumentiert, regelmäßig überprüft und aktualisiert werden, um Änderungen der Gesetze und Vorschriften Rechnung zu tragen.
- Der Ansatz der Organisation für die Einhaltung der Vorschriften sollte klar definiert sein, einschließlich der Rollen, Verantwortlichkeiten.und Rechenschaftspflicht.
- Es sollten Mechanismen zur Überwachung von Veränderungen in der rechtlichen und regulatorischen Landschaft eingeführt werden. Derartige Änderungen sollten eine Überprüfung der relevanten Richtlinien, Verfahren und Kontrollen auslösen, um eine kontinuierliche Einhaltung der Vorschriften zu gewährleisten.
- Belege für die Einhaltung der Vorschriften sollten aufbewahrt werden, um Prüfungen zu unterstützen und die Sorgfaltspflicht nachzuweisen.

GV.OC-04 Wesentliche Ziele, Fähigkeiten und Dienstleistungen, von denen externe Stakeholder abhängen oder die sie von der Organisation erwarten, werden verstanden und kommuniziert

GV.OC-04.1 **Die Organisation identifiziert, dokumentiert und kommuniziert die kritischen Ziele, Fähigkeiten und Dienstleistungen, auf die sich externe Stakeholder verlassen, priorisiert sie anhand ihrer Kritikalität und integriert diese Priorisierung in den Risikobewertungsprozess.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation versteht, welche kritischen Dienstleistungen, Fähigkeiten und Ziele für externe Stakeholder wichtig sind, diese nach ihrer Wichtigkeit priorisiert und in den Risikobewertungsprozess einbezieht.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Der Schwerpunkt dieser Kontrolle liegt auf den Leistungen, die die Organisation für andere erbringt, d. h. auf den Dienstleistungen und Funktionen, von denen externe Stakeholder abhängen (die nachgelagerte Lieferkette, z. B. Kunden, Partner oder Endverbraucher).
- Kritische Dienstleistungen und die internen Funktionen, die sie unterstützen, sollten eindeutig identifiziert werden.
- Es sollten Kriterien festgelegt werden, um zu bestimmen, wie wichtig jede Dienstleistung oder Fähigkeit sowohl aus interner als auch aus externer Sicht ist.
- Mit Hilfe einer Analyse der Auswirkungen auf das Geschäft kann ermittelt werden, welche Vermögenswerte und Abläufe für das Erreichen der wichtigsten Ziele von entscheidender Bedeutung sind und welche Folgen eine Unterbrechung dieser Abläufe haben würde.
- Es sollten Resilienzziele festgelegt und kommuniziert werden, z. B. wie schnell sich kritische Services bei Störungen erholen sollten.

GV.OC-04.2 Die Organisation definiert und dokumentiert Cybersicherheitsanforderungen für wesentliche Betriebsabläufe, validiert diese durch Tests und Audits, führt Aufzeichnungen über Ergebnisse und Korrekturmaßnahmen und aktualisiert die Anforderungen regelmäßig auf der Grundlage sich verändernder Risiken.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass wesentliche Vorgänge durch klar definierte und getestete Sicherheitsmaßnahmen geschützt werden und dass diese Maßnahmen wirksam und auf dem neuesten Stand bleiben, wenn sich die Risiken weiterentwickeln.

Um dieses Ziel zu erreichen, sollten folgende praktische Schritte berücksichtigt werden:

- Identifizierung & Dokumentation
  - Definition kritischer Services und ihrer Abhängigkeiten (z. B. Systeme, Lieferanten) durch eine strukturierte Risikobewertung.
  - Dokumentation der Sicherheits- und Betriebsanforderungen, einschließlich regulatorischer und branchenspezifischer Anforderungen (z. B. CyFun®, ISO/IEC 27001, IEC 62443).
- Validierung & Genehmigung
  - Einführung von Governance-Prozessen zur Überprüfung und Genehmigung der ermittelten Sicherheitsanforderungen.
  - Zuweisung der Rechenschaftspflicht an die relevanten Stakeholder (z. B. Sicherheitsteams, Compliance-Beauftragte, Führungskräfte).
- Prüfung & Sicherheit
  - Durchführung von Penetrationstests, Schwachstellenbewertungen und Simulationen von Vorfällen zur Validierung der Implementierung.
  - Sicherstellung der Durchführung von Audits zur Bewertung der Wirksamkeit und zur Ermittlung von Lücken in den Sicherheitsmaßnahmen.
  - Umsetzung von Abhilfemaßnahmen bei festgestellten Mängeln, um eine kontinuierliche Verbesserung zu gewährleisten.
- Aufzeichnungen & Compliance
  - Führung einer detaillierten Dokumentation der Testverfahren, Ergebnisse, Genehmigungen und Korrekturmaßnahmen.
  - Abstimmung des Sicherheitsrahmens mit den gesetzlichen Verpflichtungen, um die Einhaltung der Vorschriften und die Überwachung der Unternehmensführung zu gewährleisten.
- Kontinuierliche Überprüfung & Anpassung
  - Regelmäßige Neubewertung der Anforderungen als Reaktion auf sich entwickelnde Bedrohungen, Vorfälle und regulatorische Änderungen.
  - Sicherstellung, dass die Aufsichtsorgane Aktualisierungen und Verbesserungen überwachen, um die langfristige Cyber-Resilienz aufrechtzuerhalten.

GV.OC-04.3 Redundanz wird implementiert, um die von der Organisation, den Gesetzen und/oder Vorschriften definierten Verfügbarkeitsanforderungen zu erfüllen

Implementierungshinweise

Das Ziel dieser Kontrolle ist es, sicherzustellen, dass kritische Systeme und Dienste verfügbar bleiben, indem Redundanz in Übereinstimmung mit organisatorischen, rechtlichen und regulatorischen Verfügbarkeitsanforderungen implementiert wird.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Der Schwerpunkt dieser Kontrolle liegt darauf, sicherzustellen, dass wesentliche Dienste auch dann weiter laufen, wenn ein Teil des Systems ausfällt.
- Die Redundanz sollte in Schlüsselkomponenten wie Datenspeicherung, Netzinfrastruktur und kritische Systeme eingebaut werden. Beispiele hierfür sind:
  - Backup-Server, Load Balancer, RAID-Arrays und mehrere Rechenzentren
  - Ausfallsichere Internetverbindungen und mehrere Internetdienstanbieter (ISPs)
- Kritische Geräte und Dienste sollten gegen Stromausfälle und Versorgungsunterbrechungen geschützt werden:
  - Unterbrechungsfreie Stromversorgungen (USV), Notstromgeneratoren und redundante Stromverkabelung, 2 verschiedene Stromversorger usw.
  - Regelmäßige Tests und Wartungsverträge zur Gewährleistung der Zuverlässigkeit

GV.OC-04.4 Die Wiederherstellungszeit und die Wiederherstellungspunktziele für die Wiederaufnahme wesentlicher IKT-/OT-Systemprozesse werden definiert und überwacht.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation klare Wiederherstellungszeitziele (RTO) und Wiederherstellungspunktziele (RPO) für die Wiederherstellung wesentlicher IKT- und OT-Systemprozesse nach einer Störung definiert und überwacht.

Berücksichtigen Sie die folgenden Elemente für die Definition und Überwachung von RTOs und RPOs für kritische IKT-/OT-Systeme:

- **Definition von Governance und Richtlinien**
  - Legen Sie formelle Richtlinien und Verantwortlichkeiten für die Definition und Überwachung von RTO/RPO fest.
  - Gleichen Sie die Wiederherstellungsziele an die Rahmenwerke für Geschäftskontinuität und Notfallwiederherstellung an (z. B. ISO 22301, ISO/IEC 27031).
  - Stellen Sie die Zustimmung der Führungskräfte und die Einhaltung gesetzlicher Vorschriften sicher.
- **Analyse der geschäftlichen Auswirkungen (BIA)**
  - Identifizieren Sie gegenseitige Abhängigkeiten zwischen IKT- und OT-Systemen und deren Auswirkungen auf den Geschäftsbetrieb.
  - Bestimmen Sie akzeptable Schwellenwerte für Ausfallzeiten für verschiedene Systemkategorien.
- **Bewertung von Risiken und Bedrohungen**
  - Führen Sie realistische Bedrohungssimulationen durch (z. B. Ransomware-Übungen, DDoS-Stresstests).
  - Integrieren Sie Bedrohungsinformationen in Ihre Notfallplanung, um sich auf neue Risiken vorzubereiten.
- **Klassifizierung & Priorisierung von Systemen**
  - Definieren Sie abgestufte Wiederherstellungsstrategien auf der Grundlage der geschäftlichen Auswirkungen (z. B. Stufe 1 = sofortige Wiederherstellung, Stufe 2 = verzögerte Wiederherstellung).
  - Richten Sie Failover-Mechanismen für kritische OT-Prozesse ein, die kontinuierlich laufen müssen.
- **Strategien für Backup & Wiederherstellung**
  - Implementieren Sie unveränderliche Backups zum Schutz vor Ransomware.
  - Stellen Sie externe und cloudbasierte Wiederherstellungsoptionen für geografische Resilienz sicher.
  - Führen Sie regelmäßige Validierungs- und Integritätsprüfungen von Backups durch, um Ausfälle bei der Wiederherstellung zu vermeiden.

- **Prüfung & Validierung von Wiederherstellungszielen**
  - Führen Sie Tests zur Notfallwiederherstellung durch (Tabletop-Übungen, vollständige Wiederherstellungsübungen).
  - Messen Sie die Effektivität von RTO/RPO durch Echtzeitüberwachung und Simulationen der Reaktion auf Vorfälle
  - Richten Sie eine automatisierte Wiederherstellungsorchestrierung ein, um die Wiederaufnahme der Dienste zu beschleunigen
- **Kontinuierliche Überwachung & Verbesserung**
  - Nutzen Sie Echtzeit-Analysen, um Abweichungen von den erwarteten RTO/RPO-Werten zu bewerten.
  - Passen Sie die Wiederherstellungsziele auf Grundlage der aus Vorfällen und Audits gewonnenen Erkenntnisse an.

GV.OC-05 Ergebnisse, Fähigkeiten und Dienstleistungen, von denen die Organisation abhängt, werden verstanden und kommuniziert

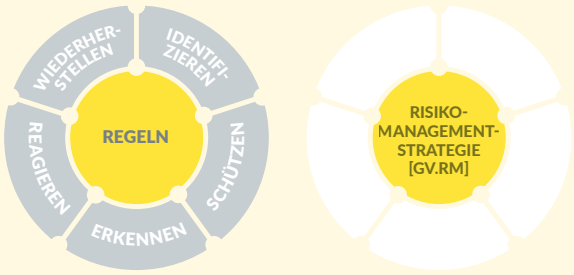
GV.OC-05.1 Die Organisation identifiziert, dokumentiert und kommuniziert ihre Rolle in der Lieferkette, einschließlich der externen Fähigkeiten, Services und Abhängigkeiten, auf die sie angewiesen ist (vorgelagert), sowie ihre Interaktionen mit nachgelagerten Stakeholdern.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation ihre Rolle innerhalb der Lieferkette identifiziert, dokumentiert und kommuniziert, indem sie die externen Fähigkeiten, Services und Abhängigkeiten, auf die sie angewiesen ist (vorgelagert), versteht und gleichzeitig ihre Interaktionen mit nachgelagerten Stakeholdern erkennt.

Diese Kontrolle konzentriert sich in erster Linie auf die vorgelagerte Lieferkette, also auf die Dinge, die die Organisation von anderen abhängig macht, und steht im Einklang mit GV.OC-04, das sich mit den Leistungen der Organisation für andere befasst. Zusammen liefern sie einen vollständigen Überblick über die Abhängigkeiten und Verantwortlichkeiten in der Lieferkette.

Um diese Kontrolle zu unterstützen, sollten folgende Punkte berücksichtigt werden:
- Die Rolle der Organisation in der Lieferkette sollte klar definiert werden, einschließlich dessen, was an andere geliefert wird (nachgelagert) und was von externen Quellen bezogen wird (vorgelagert).
- Abhängigkeiten von externen Ressourcen – z. B. Einrichtungen, Cloud-Anbieter und Lieferanten von Services, Produkten oder Fähigkeiten – sollten ermittelt und dokumentiert werden.
- Diese Abhängigkeiten sollten den entsprechenden Geschäftsfunktionen und organisatorischen Ressourcen zugeordnet werden, um ihre Auswirkungen auf den Betrieb zu verstehen.
- Besondere Aufmerksamkeit sollte externen Abhängigkeiten gewidmet werden, die potenzielle Fehlerquellen für kritische Services oder Fähigkeiten darstellen.
- Diese Informationen sollten an die zuständigen Mitarbeiter und die Stakeholder weitergegeben werden, um das Risikomanagement, die Kontinuitätsplanung und die koordinierte Reaktion zu unterstützen.
- Es sollten Kommunikationskanäle eingerichtet werden, um sicherzustellen, dass die Rollen und Abhängigkeiten in der Lieferkette innerhalb der Organisation und mit den wichtigsten Partnern klar verstanden werden.



Die Prioritäten, Einschränkungen, Risikotoleranz- und Risikobereitschaftserklärungen sowie Annahmen der Organisation werden festgelegt, kommuniziert und zur Unterstützung von Entscheidungen zum Betriebsrisiko genutzt

GV.RM-01 Die Risikomanagementziele sind festgelegt und von den Stakeholdern der Organisation gebilligt

GV.RM-01.1 Es werden Ziele für die Informationssicherheit/Cybersicherheit festgelegt, die von den Stakeholdern der Organisation vereinbart und von der Geschäftsleitung genehmigt werden

Implementierungshinweise

Um dieses Ziel zu unterstützen, sollten Organisationen:

- Die Grundsätze des Risikomanagements gemäß ISO/IEC 27005 befolgen, die Leitlinien zur Identifizierung, Bewertung und Minderung von Risiken für die Informationssicherheit liefern. Konkret:
  - Abschnitt 6.1 sollte zur Einführung eines strukturierten Risikobewertungsprozesses verwendet werden.
  - Abschnitt 6.3 sollte als Leitfaden für die Festlegung geeigneter Risikobehandlungsstrategien dienen.
- Kurz- und langfristige Informationen sowie Ziele im Bereich Cybersicherheit im Rahmen der jährlichen Strategieplanung und als Reaktion auf wesentliche organisatorische Veränderungen aktualisieren.
- In Organisationen des OT-Sektors sollte die Geschäftsleitung bei der Ermittlung von Risiken Gesundheits-, Sicherheits- und Umweltfaktoren berücksichtigen.
- Messbare Ziele (SMART) für Informations- und Cybersicherheit festlegen (z. B. Verbesserung der Qualität der Benutzerschulungen, Gewährleistung eines angemessenen Schutzes für industrielle Steuerungssysteme).
- Diese Ziele zur Messung und Steuerung von Risiken und Leistung in der gesamten Organisation nutzen.

GV.RM-02 Erklärungen zur Risikobereitschaft und Risikotoleranz werden erstellt, kommuniziert und aufrechterhalten

GV.RM-02.1 Erklärungen zur Risikobereitschaft und Risikotoleranz werden definiert, dokumentiert, von der Geschäftsleitung genehmigt, kommuniziert und aufrechterhalten.

Implementierungshinweise

Das Ziel von GV.RM-02.1 ist es, sicherzustellen, dass eine Organisation über ein klares und umsetzbares Verständnis ihrer Risikogrenzen verfügt, das die Entscheidungsfindung und die Risikomanagementpraktiken unterstützt.

Folgende Punkte sollten berücksichtigt werden, um dieses Ziel zu erreichen:

- Die Risikobereitschaft ist die Höhe und Art des Risikos, das eine Organisation bereit ist, einzugehen oder zu akzeptieren, und ist strategisch/qualitativ (Quelle: ISO/IEC 27005).
- Die Risikotoleranz ist die akzeptable Abweichung von dem durch die Risikobereitschaft und die Geschäftsziele festgelegten Niveau und ist taktisch/quantitativ (Quelle: ISACA).
- Die Risikobereitschaft der Organisation sollte ihre Rolle bei kritischen Infrastrukturen und in ihrem Sektor berücksichtigen.
- Organisationen im OT-Sektor sollten bei der Festlegung ihrer Risikobereitschaft die Prioritäten für Gesundheit, Sicherheit und Umwelt berücksichtigen.
- Die Aussagen zur Risikobereitschaft sollten in spezifische, messbare und allgemein verständliche Aussagen zur Risikotoleranz (SMART) übersetzt werden.
- Die organisatorischen Ziele und die Risikobereitschaft sollten regelmäßig auf der Grundlage der bekannten Risikoexposition und des Restrisikos angepasst werden.
- Mit AR-in-a-Box stellt die ENISA, die Agentur der Europäischen Union für Cybersicherheit, Organisationen die wesentlichen Tools und Ressourcen zur Verfügung, um das Bewusstsein für Cybersicherheit in ihren Betrieben effektiv zu schärfen. Diese ENISA-Do-It-Yourself Toolbox enthält einen Leitfaden für die C-Ebene.

GV.RM-03 Aktivitäten und Ergebnisse des Managements von Cybersicherheitsrisiken sind in die Risikomanagementprozesse des Unternehmens integriert

GV.RM-03.1 **Als Teil der organisationsweiten Risikomanagementstrategie wird eine umfassende Strategie zur Bewältigung von Informations- und Cybersicherheitsrisiken entwickelt und bei Änderungen aktualisiert.**

Implementierungshinweise

Diese Kontrolle konzentriert sich auf die Erstellung und Pflege einer spezifischen Strategie für das Management von Informations- und Cybersicherheitsrisiken. So wird sichergestellt, dass die Organisation über einen speziellen, umsetzbaren Plan verfügt, der sich mit der Bedrohungslandschaft weiterentwickelt.

Um dies zu ermöglichen, sollten folgende Punkte berücksichtigt werden:

- Eine organisationsweite Risikomanagement-Strategie umfasst eine Formulierung der Sicherheitsrisikotoleranz für die Organisation, Strategien zur Minderung des Sicherheitsrisikos, akzeptable Risikobewertungsmethoden, ein Verfahren zur Bewertung des Sicherheitsrisikos in der gesamten Organisation im Hinblick auf die Risikotoleranz der Organisation sowie Ansätze zur Überwachung des Risikos im Zeitverlauf.
- Informations- und Cybersicherheitsrisiken sollten zusammen mit anderen Unternehmensrisiken (z. B. Einhaltung von Vorschriften, finanzielle, betriebliche, regulatorische, Reputations- und Sicherheitsrisiken) erfasst und verwaltet werden.
- Die Strategie für das Management von Informations- und Cybersicherheitsrisiken sollte die Ermittlung und Zuweisung der erforderlichen Ressourcen zum Schutz der geschäftskritischen Vermögenswerte der Organisation beinhalten.
- Dies ist die cybersicherheitsspezifische Implementierung der in GV.RM-04.1 definierten allgemeinen Vision.

GV.RM-03.2 **Informations- und Cybersicherheitsrisiken werden im Rahmen der Risikomanagementprozesse des Unternehmens dokumentiert, von der Geschäftsleitung formell genehmigt und bei Änderungen aktualisiert.**

Implementierungshinweise

Diese Kontrolle sollte sicherstellen, dass die Strategie durch strukturierte Prozesse umgesetzt wird. Sie konzentriert sich auf die operative und Governance-Ebene, gewährleistet die Rechenschaftspflicht und die Rückverfolgbarkeit von Risiken und legt den Schwerpunkt auf formelle Prozesse und die Aufsicht.

Bei der Durchführung dieser Kontrolle sollten die folgenden Komponenten berücksichtigt werden:

Systematische Risikoermittlung

- Ziel: Proaktive Ermittlung von Informations- und Cybersicherheitsrisiken in der gesamten Organisation.
- Maßnahmen:
  - Regelmäßige Risikobewertungen sollten mit Methoden wie Bedrohungsmodellierung, Risiko-Workshops und Schwachstellen-Scans durchgeführt werden.
  - Die Risiken im Zusammenhang mit allen digitalen und physischen Vermögenswerten (Hardware, Software, Daten, Netzwerke) sollten zusammen mit den wichtigsten Metadaten (Standort, Eigentümer, Nutzung) in das Bestandsverzeichnis aufgenommen werden.
  - Nutzen Sie Quellen wie:
    - Protokolle über Sicherheitsvorfälle
    - Ergebnisse der Penetrationstests
    - Regulatorische Anforderungen
    - Informationen über Bedrohungen in der Branche
  - Erwägen Sie die Einbeziehung funktionsübergreifender Teams (IT/OT, Recht, Compliance, Geschäftsbereiche).
- Zu berücksichtigende Tools:
  - Vorlagen für die Risikobewertung
  - Plattformen für Bedrohungsinformationen (z. B. MISP, Recorded Future)
  - Inventare der Vermögenswerte und Datenflussdiagramme

Risikodokumentation im ERM-Rahmenwerk

- Ziel: Sicherstellen, dass Cybersicherheitsrisiken in den umfassenderen Prozess des Enterprise Risk Management (ERM) integriert werden.
- Maßnahmen:
  - Erwägen Sie die Verwendung eines zentralisierten Risikoregisters oder GRC-Tools zur Dokumentation:
    - Beschreibung des Risikos
    - Wahrscheinlichkeit und Auswirkungen
    - Eigentümer des Risikos
    - Vorhandene Kontrollen
    - Verbleibendes Risiko
    - Behandlungsplan
  - Das Cybersecurity-Risikomanagement sollte mit den strategischen Unternehmenszielen abgestimmt werden, um Relevanz und Unterstützung zu gewährleisten.
- Zu berücksichtigende Tools:
  - GRC-Plattformen
  - Excel/SharePoint (für kleinere Organisationen)

Formelle Genehmigung und Einbeziehung der Geschäftsleitung

- Ziel: Sicherstellung der Aufsicht durch die Geschäftsleitung und der Rechenschaftspflicht bei Risikoentscheidungen.
- Maßnahmen:
  - Risikobewertungen und Maßnahmenpläne sollten einem Risikoausschuss oder der Geschäftsleitung vorgelegt werden.
  - Erwägen Sie die Aufnahme von Cybersicherheitsrisiken in die vierteljährlichen Risikoberichte.
  - Es sollte eine formelle Genehmigung eingeholt werden bezüglich:
    - Risikoakzeptanz
    - Plänen zur Risikominderung
    - Mittelzuweisungen
- Zu berücksichtigende Tools:
  - Vorlagen für Vorstandsberichte
  - Risiko-Dashboards
  - Sitzungsprotokollen mit dokumentierten Genehmigungen

Kommunikation und Sensibilisierung

- Ziel: Sicherstellung, dass alle relevanten Stakeholder informiert und eingebunden sind.
- Maßnahmen:
  - Es sollten klare Kommunikationswege für Cybersicherheitsrisiken eingerichtet werden, einschließlich derjenigen von Lieferanten und Drittparteien.
  - Die genehmigten Risiken und Strategien zur Risikominderung sollten den zuständigen Teams mitgeteilt werden.
  - Die Sensibilisierung sollte durch Schulungen, Briefings und interne Kommunikation gefördert werden.
- Zu berücksichtigende Tools:
  - Interne Kommunikationsplattformen (z. B. Teams, Slack)
  - Pläne zur Risikokommunikation
  - Stakeholder-Karten

Kontinuierliche Überwachung und Updates

- Ziel: Risikodaten auf dem neuesten Stand halten und auf Veränderungen reagieren.
- Maßnahmen:
  - Es sollte eine kontinuierliche Überwachung implementiert werden, um Veränderungen in der Bedrohungslandschaft oder im organisatorischen Umfeld zu erkennen.
  - Erwägen Sie, Auslöser für Aktualisierungen zu definieren, z. B.:
    - Neue Bedrohungen oder Schwachstellen
    - Änderungen in Geschäftsprozessen oder IT-Systemen
    - Regulatorische Änderungen
  - Es sollte ein Änderungsmanagementprozess eingerichtet werden, der auch die Aktualisierung der Cybersicherheitsdokumentation umfasst.
  - Die dokumentierten Risiken sollten regelmäßig überprüft werden (z. B. vierteljährlich oder zweimal im Jahr).
- Zu berücksichtigende Tools:
  - Systeme zum Management von Änderungen
  - Kontinuierliche Überwachungstools
  - Kalender für die Risikoprüfung

Diese Kontrolle operationalisiert GV.RM-03.1, indem sie Cybersecurity-Risiken in den Rahmen des Enterprise Risk Management (ERM) einbettet und Governance und Rechenschaftspflicht sicherstellt.

GV.RM-04 Die strategische Ausrichtung, die geeignete Optionen für die Risikobewältigung beschreibt, ist festgelegt und kommuniziert

GV.RM-04.1 Es wird ein übergeordneter Plan oder eine Vision formell festgelegt und allen Beteiligten klar kommuniziert, wie Risiken zu handhaben sind, einschließlich der verschiedenen Strategien, die die Organisation anwenden kann, um mit identifizierten Risiken auf der Grundlage der Risikobereitschaft oder der Risikotoleranz umzugehen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die strategische Grundlage für das Risikomanagement zu schaffen, einschließlich:

- Risikotoleranz und Risikobereitschaft,
- Strategische Richtung für das Risikomanagement (z. B. Abschwächen, Übertragen, Akzeptieren),
- Sicherstellung einer abteilungsübergreifenden Abstimmung.
- Sicherstellung, dass alle in der Organisation das Gesamtbild der Vorgehensweise und des Managements von Risiken verstehen

Die Kontrolle konzentriert sich auf:

- Risikomanagement auf strategischer und organisatorischer Ebene.
- Erarbeitung einer formellen, übergreifenden Vision oder eines Plans.
- Kommunikation von Risikomanagement-Strategien (z. B. vermeiden, abmildern, übertragen, akzeptieren).
- Gilt für alle Arten von Risiken, nicht nur für die Cybersicherheit.

In Bezug auf die Kontrollen GV.RM-03.1, GV.RM-03.2 und GV.RM-05.1 ist diese Kontrolle der Ausgangspunkt; sie definiert die Risikophilosophie der Organisation, einschließlich der Risikobereitschaft und -toleranz, die alle anderen Aktivitäten leitet

GV.RM-05 Innerhalb der Organisation sind Kommunikationswege für Cybersicherheitsrisiken, einschließlich Risiken von Lieferanten und anderen Drittparteien, eingerichtet.

GV.RM-05.1 **Zur Unterstützung der hochrangigen Risikomanagement-Vision richtet die Organisation klare Kommunikationswege für Cybersicherheitsrisiken ein, einschließlich solcher, die von Lieferanten und Drittparteien ausgehen.**

Implementierungshinweise

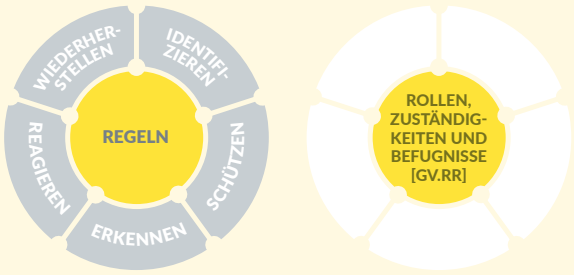
Ziel dieser Kontrolle ist es, sicherzustellen, dass Informationen über Cyber- und Informationssicherheitsrisiken innerhalb der Organisation und mit externen Parteien effektiv ausgetauscht werden.

Dieser Kontrollschwerpunkt auf operativer und taktischer Kommunikation ist spezifisch für Cybersicherheitsrisiken und betont die Kommunikationskanäle (z. B. Berichterstattung, Eskalation, Koordination), einschließlich externer Risiken von Lieferanten und Drittparteien.

Beachten Sie bei der Implementierung dieser Kontrolle die folgenden Elemente:

- **Definieren Sie Kommunikationsrollen und -verantwortlichkeiten**
  Weisen Sie klare Zuständigkeiten für die Meldung, Eskalation und Reaktion auf Cybersicherheitsrisiken in allen Abteilungen und gegenüber Drittparteien zu.
- **Richten Sie Kommunikationskanäle ein**
  Nutzen Sie strukturierte Kanäle wie E-Mail-Gruppen, Ticketing-Systeme, Plattformen für die Reaktion auf Vorfälle oder Tools für die Zusammenarbeit (z. B. Teams, Slack) für die rechtzeitige Risikokommunikation.
- **Beziehen Sie Drittparteien ein**
  Integrieren Sie Lieferanten und Partner in den Kommunikationsprozess durch Vertragsklauseln, gemeinsame Meldeprotokolle oder gemeinsame Reaktionspläne auf Vorfälle.
- **Dokumentieren und schulen Sie**
  Führen Sie ein Kommunikationsprotokoll oder Playbook und schulen Sie die zuständigen Mitarbeiter darin, wie und wann sie Cybersicherheitsrisiken melden sollen.
- **Überprüfen und verbessern Sie**
  Überprüfen und bewerten Sie regelmäßig die Effektivität der Kommunikation durch Tabletop-Übungen oder Nachbesprechungen nach Vorfällen.

Diese Kontrolle unterstützt die Implementierung von GV.RM-03.2, indem sie sicherstellt, dass identifizierte und dokumentierte Risiken an die richtigen Beteiligten weitergeleitet werden, um eine rechtzeitige Reaktion und Koordination zu ermöglichen.



Rollen, Zuständigkeiten und Befugnisse im Bereich der Cybersicherheit zur Förderung der Rechenschaftspflicht, der Leistungsbewertung und der kontinuierlichen Verbesserung sind festgelegt und kommuniziert

GV.RR-01 Die Unternehmensführung ist für Cybersicherheitsrisiken verantwortlich und rechenschaftspflichtig und fördert eine risikobewusste, ethische und sich ständig verbessernde Kultur

GV.RR-01.1 Die oberste Führungsebene der Organisation ist für Cybersicherheitsrisiken verantwortlich und rechenschaftspflichtig und fördert eine risikobewusste, ethische und sich kontinuierlich verbessernde Kultur.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die oberste Führungsebene für das Cybersicherheitsrisiko verantwortlich ist und eine risikobewusste und sich ständig verbessernde Kultur fördert.

Um dies zu ermöglichen, sollten folgende Punkte berücksichtigt werden:

- Die oberste Führungsebene einer Organisation sollte sich über ihre Aufgaben und Zuständigkeiten bei der Entwicklung, Umsetzung und Bewertung der Cybersicherheitsstrategie der Organisation einigen.
- Die Erwartungen der obersten Führungsebene an eine Sicherheitskultur, einschließlich der Hervorhebung positiver oder negativer Beispiele für das Management von Cybersicherheitsrisiken, sollten an die gesamte Organisation weitergegeben werden.
- Die oberste Führungsebene einer Organisation sollte den leitenden (Informations-)Sicherheitsbeauftragten (z. B. CSO, CISO) anweisen, eine umfassende Strategie für Cybersicherheitsrisiken aufrechtzuerhalten und diese mindestens jährlich sowie nach wichtigen Ereignissen zu überprüfen und zu aktualisieren (siehe auch GV.RR-02.2).
- Es sollten Überprüfungen durchgeführt werden, um sicherzustellen, dass die für das Management von Cybersicherheitsrisiken verantwortlichen Personen über angemessene Befugnisse verfügen und sich untereinander abstimmen.

GV.RR-02 Rollen, Verantwortlichkeiten und Befugnisse im Zusammenhang mit dem Management von Cybersicherheitsrisiken sind festgelegt, kommuniziert, verstanden und durchgesetzt

GV.RR-02.1 **Rollen, Verantwortlichkeiten und Befugnisse im Bereich Informationssicherheit und Cybersicherheit für Mitarbeiter, Lieferanten, Kunden und Partner werden dokumentiert, überprüft, genehmigt, auf dem neuesten Stand gehalten, kommuniziert und intern und extern koordiniert.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle internen und externen Parteien ihre Rollen, Zuständigkeiten und Befugnisse im Bereich der Cybersicherheit verstehen und erfüllen, um Lücken, Überschneidungen und Verzögerungen bei der Reaktion auf Vorfälle und der Einhaltung von Vorschriften zu verringern.

Folgendes sollte berücksichtigt werden:

- Beschreibung der Sicherheitsrollen, Verantwortlichkeiten und Befugnisse: Welche Personen innerhalb der Organisation sollten zu allen oder einem Teil der Unternehmensressourcen konsultiert, informiert, verantwortlich und rechenschaftspflichtig sein. Die Verwendung des RACI-Modells kann in Betracht gezogen werden. Anleitungen finden sich auch in den ENISA European Cybersecurity Skills Framework Role Profiles (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles).
- Einbeziehung der Rollen, Verantwortlichkeiten und Befugnisse für das Risikomanagement.
- Aufnahme von Verantwortlichkeiten und Leistungsanforderungen im Bereich der Informations- und Cybersicherheit in die Personalbeschreibungen.
- Klare Abgrenzung der Zuständigkeiten für Informations- und Cybersicherheit in den Bereichen operatives Geschäft, Risikofunktionen und Innenrevision.
- Bestimmung einer oder mehrerer spezifischer Rollen oder Positionen, die für die Planung, Bereitstellung von Ressourcen und Ausführung von Aktivitäten zum Risikomanagement der Informations-/Cybersecurity-Lieferkette verantwortlich und rechenschaftspflichtig sind.
- Einhaltung der vorherigen Richtlinie, Ausweitung der internen Sicherheitsrollen, Verantwortlichkeiten und Befugnisse auf die Rollen, Verantwortlichkeiten und Befugnisse im Bereich Informations-/Cybersicherheit und Risikomanagement in der Lieferkette.
- Entwicklung von Rollen, Zuständigkeiten und Befugnissen für Zulieferer, Kunden und Geschäftspartner, um die gemeinsame Verantwortung für anwendbare Informations-/Cybersicherheitsrisiken zu regeln, und sie in organisatorische Richtlinien und anwendbare Vereinbarungen mit Drittparteien zu integrieren.
- Interne Kommunikation der Rollen und Zuständigkeiten für das Risikomanagement in der Informations-/Cybersecurity-Lieferkette für Drittparteien.
- Festlegung von Regeln und Protokollen für den Informationsaustausch und die Berichterstattungsprozesse zwischen der Organisation und ihren Lieferanten.
- Berücksichtigung einer klaren Unterscheidung zwischen IT (Informationstechnologie) und OT (Betriebstechnologie) bei der Umsetzung dieser Kontrolle unter Beachtung der folgenden Punkte:
  - Rollen und Zuständigkeiten
    - IT: Definition von Rollen wie Systemadministrator, Netzwerksicherheitsanalytiker, Störfallbeauftragter.
    - OT: Definition von Rollen, wie z. B. Leitsystemingenieur, OT-Cybersicherheitsleiter, Anlagenbetreiber.
  - Dokumentation und Überprüfung
    - Sicherstellung, dass die IT- und OT-Rollen getrennt dokumentiert, aber aufeinander abgestimmt sind.
    - Die Überprüfungszyklen können unterschiedlich sein: IT (vierteljährlich/jährlich), OT (in Übereinstimmung mit den Wartungsfenstern).
  - Autorisierung und Aktualisierungen
    - Sicherstellung, dass sowohl die IT- als auch die OT-Dokumentation von der zuständigen Geschäftsleitung (z. B. CIO für IT, Betriebsleiter für OT) genehmigt wird.
    - Aktualisierungen in OT können aufgrund von Sicherheitsaspekten Änderungskontrollverfahren erfordern.
  - Kommunikation und Koordinierung
    - Intern: Sicherstellung, dass IT- und OT-Teams gemeinsame Reaktionspläne für Vorfälle haben.
    - Extern: Einbeziehung von Lieferanten und Partnern, die speziell für OT (z. B. ICS-Anbieter) und IT (z. B. Cloud-Anbieter) relevant sind.

GV.RR-02.2 Die Organisation ernennt einen leitenden Informationssicherheitsbeauftragten.

Implementierungshinweise

Ziel dieser Kontrollmaßnahme ist es, eine klare Führungsverantwortung für die Cybersicherheit zu schaffen, indem eine Führungskraft ernannt wird, die für die Strategie, die Aufsicht und die Abstimmung mit den Geschäftszielen zuständig ist.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Eine Führungskraft wird als hochrangiges Mitglied der Organisation definiert, das an wichtigen Entscheidungsprozessen beteiligt ist.
- Der leitende Informationssicherheitsbeauftragte, der auch der Chief Information Security Officer (CISO) sein kann, sollte über die Befugnisse, die Verantwortung und die Ressourcen verfügen, um eine organisationsweite Vision, Strategie und ein Programm zu koordinieren, zu entwickeln, umzusetzen, zu überwachen und aufrechtzuerhalten, um sicherzustellen, dass Informationswerte und -technologien angemessen geschützt sind.

GV.RR-03 Angemessene Ressourcen werden entsprechend der Strategie für Cybersicherheitsrisiken, den Rollen, Verantwortlichkeiten und Richtlinien zugewiesen

GV.RR-03-1 Ausreichende Ressourcen werden im Einklang mit der Cybersicherheits-Risikostrategie, den Rollen, Verantwortlichkeiten und Richtlinien zugewiesen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Cybersicherheit durch die Abstimmung der Ressourcenzuteilung (einschließlich Personal, Budget und Technologie) auf strategische Prioritäten, Rollen und Richtlinien wirksam unterstützt wird.

Um dies zu ermöglichen, sollten folgende Punkte berücksichtigt werden:

- Es sollten regelmäßige Managementüberprüfungen durchgeführt werden, um sicherzustellen, dass die Personen, die für das Management von Cybersicherheitsrisiken zuständig sind, über die erforderlichen Befugnisse verfügen.
- Ressourcenzuweisung und Investitionen sollten im Einklang mit der Risikobereitschaft der Organisation festgelegt werden
- Zur Unterstützung der Cybersicherheitsstrategie sollten angemessene und ausreichende Mitarbeiter, Verfahren und technische Ressourcen bereitgestellt werden
- Das Fachpersonal sollte über die für die OT-Sicherheit erforderlichen Spezialkenntnisse und -fähigkeiten verfügen, um die Zusammenarbeit mit OT-Ingenieuren zu ermöglichen, damit Warnungen richtig interpretiert und Bedrohungen wirksam bekämpft werden können.

GV.RR-03-2 **Die Organisation weist Rollen und Verantwortlichkeiten für die Überprüfung und Aktualisierung von Notfall- und Wiederherstellungsplänen zu und stellt sicher, dass diese den Veränderungen im Risikoumfeld Rechnung tragen und wirksam bleiben.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Reaktions- und Wiederherstellungspläne wirksam bleiben, indem Rollen und Verantwortlichkeiten für ihre regelmäßige Überprüfung und Anpassung an sich entwickelnde Risiken zugewiesen werden.

Um diese Kontrolle zu implementieren, sollten folgende Elemente berücksichtigt werden:

- Definieren und Zuweisen von Zuständigkeiten
  - Weisen Sie klare Rollen für die Pflege, Überprüfung und Aktualisierung der Reaktions- und Wiederherstellungspläne zu.
  - Stellen Sie sicher, dass die verantwortlichen Personen die Befugnis und die Ressourcen haben, um die festgestellten Änderungen umzusetzen.
  - Benennen Sie einen zentralen Koordinator oder ein Team, das den Aktualisierungsprozess überwacht und die Rechenschaftspflicht sicherstellt.
- Verständnis und Überwachung des organisatorischen Kontextes
  Regelmäßige Bewertung interner und externer Faktoren wie:
  - Organisatorische Struktur und kritische Systeme
  - Aufkommende Bedrohungen und Schwachstellen
  - Regulatorische Veränderungen und Marktdynamik
  - Erkenntnisse aus Vorfällen, Tests oder Übungen
- Aktualisierung der Pläne auf der Grundlage kontextueller Änderungen
  - Überarbeiten Sie die Pläne entsprechend:
    - Neuen oder sich entwickelnden Bedrohungen
    - Änderungen in der Technologie oder Infrastruktur
    - Bei den Tests ermittelten betrieblichen Herausforderungen oder Lücken
  - Die Aktualisierungen können Kontaktlisten, Kommunikationsprotokolle, Eskalationspfade und Ressourcenzuweisungen umfassen.
- Kommunizieren und schulen
  - Stellen Sie sicher, dass alle relevanten Stakeholder über Aktualisierungen informiert werden.
  - Bieten Sie Schulungen oder Informationsveranstaltungen an, um die Rollen und Verantwortlichkeiten in den überarbeiteten Plänen zu verdeutlichen.
- Testen und Verbessern
  - Führen Sie regelmäßig Übungen und Simulationen durch, um die Wirksamkeit der aktualisierten Pläne zu überprüfen.
  - Nutzen Sie die Ergebnisse, um Lücken zu erkennen und kontinuierliche Verbesserungen vorzunehmen.
- Kontinuierlicher Überprüfungszyklus
  - Legen Sie einen Zeitplan für die Überprüfung fest (z. B. vierteljährlich oder nach größeren Änderungen).
  - Integrieren Sie Planaktualisierungen in umfassendere Risikomanagement- und Governance-Prozesse.

GV.RR-04 Cybersicherheit ist Bestandteil der Personalpraxis

GV.RR-04.1 Mitarbeiter mit Zugang zu den kritischsten Informationen oder Technologien der Organisation werden authentifiziert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, kritische Vermögenswerte zu schützen, indem sichergestellt wird, dass nur authentifizierte Mitarbeiter auf sie zugreifen können.

Um dies zu erreichen, sollten folgende Punkte berücksichtigt werden:

- „Authentifiziert" bedeutet, dass der Benutzer seine Identität am Zugangspunkt technisch nachweisen muss, idealerweise mithilfe von MFA oder stärkeren Methoden, und nicht nur während des Onboardings validiert wird.
- Der Zugang zu kritischen Informationen oder Technologien sollte bei der Einstellung, beim Onboarding, während der Beschäftigung, bei einem Funktionswechsel und beim Offboarding (Beendigung des Beschäftigungsverhältnisses) berücksichtigt werden.
- Vor dem Onboarding neuer Mitarbeiter mit sensiblen Aufgaben sollten Hintergrundüberprüfungen durchgeführt werden, die in regelmäßigen Abständen wiederholt werden sollten. Bei der Überprüfung des Hintergrunds sollten jedoch die geltenden Gesetze, Vorschriften und ethischen Grundsätze im Verhältnis zu den geschäftlichen Anforderungen, der Klassifizierung der Informationen, auf die zugegriffen werden soll, und den wahrgenommenen Risiken berücksichtigt werden.
- Fachwissen im Bereich Cybersicherheit sollte *bei Entscheidungen über Einstellungen*, Schulungen und Mitarbeiterbindung als wertvolles Gut anerkannt werden.

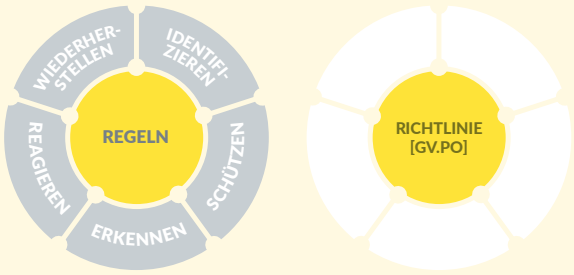
GV.RR-04.2 Es wird ein Cybersicherheitsprozess für das Personalwesen entwickelt und aufrechterhalten, der bei der Einstellung, während der Beschäftigung und bei Beendigung des Beschäftigungsverhältnisses Anwendung findet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Cybersicherheitsrisiken während des gesamten Lebenszyklus eines Mitarbeiters gemanagt werden, indem die Sicherheit in die HR-Prozesse integriert wird, von der Einstellung bis zur Kündigung.

Um dies zu ermöglichen, sollten folgende Punkte berücksichtigt werden:

- Überlegungen zum Cybersecurity-Risikomanagement sollten in die Prozesse der Personalabteilung integriert werden (z. B. Personalüberprüfung, Onboarding, Benachrichtigung über Änderungen, Offboarding)
- Der Prozess der Cybersicherheit im Bereich Human Resources sollte den Zugang zu kritischen Informationen oder Technologien, Hintergrundüberprüfungen, einen Verhaltenskodex sowie Rollen, Befugnisse und Verantwortlichkeiten usw. umfassen.
- Es sollte festgelegt und durchgesetzt werden, dass die Mitarbeiter verpflichtet sind, die Sicherheitsrichtlinien in Bezug auf ihre Rolle zu kennen, zu befolgen und einzuhalten.



Die Cybersicherheitsrichtlinie der Organisation ist festgelegt, kommuniziert und durchgesetzt.

GV.PO-01 Richtlinien für das Management von Cybersicherheitsrisiken werden auf der Grundlage des organisatorischen Kontexts, der Cybersicherheitsstrategie und der Prioritäten festgelegt, kommuniziert und durchgesetzt

GV.PO-01.1 Richtlinien und Verfahren für die Verwaltung von Informationen und Cybersicherheit werden erstellt, dokumentiert, überprüft, genehmigt, bei Änderungen aktualisiert, kommuniziert und durchgesetzt.

Implementierungshinweise

Diese Kontrolle bildet die Grundlage dafür, wie alle Informations- und Cybersicherheitsrichtlinien und -verfahren verwaltet werden sollten. Der Schwerpunkt liegt auf dem Governance-Lebenszyklus, von der Schaffung bis zur Durchsetzung, und gewährleistet die Ausrichtung auf die strategische Ausrichtung der Organisation.

Um diese Kontrolle effektiv zu implementieren, sollten Sie die folgenden Praktiken beachten:

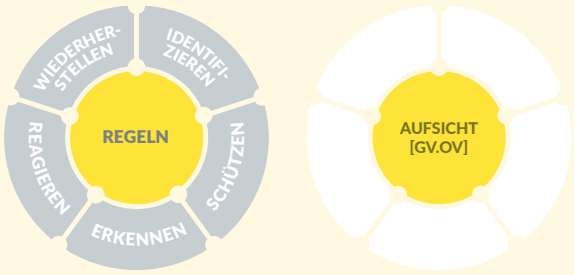
- Entwicklung klarer und praktischer Strategien, Prozesse und Verfahren, die:
  - akzeptable Verhaltensweisen und Erwartungen zum Schutz der Informationen und Systeme der Organisation definieren.
  - darlegen, wie die Geschäftsleitung von den Mitarbeitern erwartet, dass sie die Ressourcen des Unternehmens nutzen und schützen.
- Sicherstellung der Sensibilisierung der Mitarbeiter durch Vermittlung dieser Richtlinien, Prozesse und Verfahren:
  - beim Onboarding neuer Mitarbeiter.
  - immer dann, wenn wesentliche Aktualisierungen oder Änderungen vorgenommen werden.
  - Sorgen Sie für Zugänglichkeit, indem Sie alle relevanten Dokumente für die Mitarbeiter leicht zugänglich machen.
- Überprüfen und aktualisieren Sie regelmäßig (z. B. jährlich), um Folgendes zu reflektieren:
  - Organisatorische Veränderungen, wie Fusionen, Übernahmen oder neue vertragliche Verpflichtungen.
  - Technologische Entwicklungen, wie die Einführung künstlicher Intelligenz oder neuer Sicherheitstools.
- Definieren Sie Risikobewertungskriterien im Rahmen der Risikomanagementpolitik der Organisation:
  - Das Unternehmen sollte klare Kriterien für die Bestimmung der Wahrscheinlichkeit und der Auswirkungen von Risiken aufstellen und dokumentieren.
  - Diese Kriterien sollten auf den spezifischen Kontext der Organisation zugeschnitten sein und konsequent zur Bewertung und Priorisierung von Cybersicherheitsrisiken verwendet werden. Dadurch wird sichergestellt, dass risikobasierte Entscheidungen mit der Gesamtstrategie und der Risikobereitschaft der Organisation in Einklang stehen.

GV.PO-01.2 Die organisationsweiten Richtlinien und Verfahren zur Informations- und Cybersicherheit umfassen den Einsatz von Kryptographie und gegebenenfalls Verschlüsselung, spiegeln Änderungen der Anforderungen, Bedrohungen, Technologien und organisatorischen Rollen wider und werden von der Geschäftsleitung genehmigt, die deren Implementierung überwacht.

Diese Kontrolle baut auf GV.PO-01.1 auf und konzentriert sich auf den Inhalt und die Überwachung der Cybersicherheits- und Informationssicherheitspolitik selbst. Sie stellt sicher, dass bestimmte technische Themen (wie Kryptographie und Verschlüsselung) behandelt werden, dass die Richtlinien auf Veränderungen reagieren und dass die Geschäftsleitung aktiv an der Genehmigung und Überwachung beteiligt ist.

Die folgenden Elemente sollten berücksichtigt werden:

- **Umfang & Ziele definieren**
  Stellen Sie sicher, dass die Richtlinien organisationsweit gelten und mit den Geschäfts- und Risikoprioritäten übereinstimmen.
- **Kryptographie und Verschlüsselung einbeziehen**
  - Sprechen Sie die Verschlüsselung im Ruhezustand/während der Übertragung, die Schlüsselverwaltung und zugelassene Algorithmen an.
  - Legen Sie fest, wo eine Verschlüsselung erforderlich ist (z. B. persönliche Daten, Fernzugriff).
- **Richtlinien aktuell halten**
  Aktualisieren Sie die Richtlinien zur Berücksichtigung von Änderungen in:
  - Rechtlichen/regulatorischen Anforderungen
  - Bedrohungslandschaft
  - Technologie
  - Organisatorische Struktur
- **Aufsicht durch die Geschäftsleitung**
  - Fordern Sie eine formelle Genehmigung durch die Geschäftsleitung.
  - Beauftragen Sie einen Richtlinienverantwortlichen (z. B. den CISO) mit der Überwachung der Umsetzung und Einhaltung.
- **Zuweisung von Rollen & Verantwortlichkeiten**
- Nutzen Sie die ENISA ECSF Rollenprofile https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles) zur:
  - Definition von Rollen im Bereich der Cybersicherheit (z. B. Richtlinienbeauftragter, Risikomanager)
  - Abstimmung von Aufgaben, Fähigkeiten und Kompetenzen
- **Kommunikation & Schulung**
  Verbreitung von Richtlinien und Durchführung von rollenspezifischen Schulungen.
- **Überwachung & Durchsetzung**
  Nutzen Sie technische Kontrollen und Audits, um die Einhaltung der Vorschriften zu gewährleisten.



Die Ergebnisse der organisationsweiten Aktivitäten zum Management von Cybersicherheitsrisiken und Leistung werden zur Information, Verbesserung und Anpassung der Risikomanagementstrategie genutzt

GV.OV-02 Die Strategie für das Management von Cybersicherheitsrisiken wird überprüft und angepasst, um sicherzustellen, dass die organisatorischen Anforderungen und Risiken abgedeckt sind

GV.OV-02.1 Die Strategie für das Informations- und Cybersicherheitsrisikomanagement wird überprüft und angepasst, um sicherzustellen, dass die organisatorischen Anforderungen und Risiken abgedeckt sind.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Strategie zum Informations- und Cybersicherheitsrisikomanagement regelmäßig überprüft und aktualisiert wird, um die organisatorischen Anforderungen, sich verändernde Risiken und Compliance-Anforderungen zu reflektieren.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Die Strategie sollte die allgemeine Richtung und die Ziele für das Management von Informations- und Cybersicherheitsrisiken festlegen.
- Unterstützende Richtlinien und Verfahren sollten die praktische Implementierung der Strategie leiten.
- Die Strategie sollte Risiken für den Betrieb der Organisation, Vermögenswerte, Einzelpersonen und andere Entitäten, einschließlich potenzieller Auswirkungen auf den Datenschutz, behandeln.
- Überprüfungen sollten in geplanten Intervallen durchgeführt werden, auch durch interne Audits auf der Grundlage eines dokumentierten Auditprogramms, das Häufigkeit, Methoden, Verantwortlichkeiten und Berichterstattung festlegt.
- Audits sollten von kompetentem und unparteiischem Personal durchgeführt werden.
- Die Ergebnisse der Audits sollten überprüft werden, um zu beurteilen, ob die Strategie den internen Erwartungen entspricht und die gesetzlichen und regulatorischen Anforderungen erfüllt.
- Die Strategie sollte bei Bedarf aktualisiert werden, insbesondere nach Vorfällen oder Auditergebnissen.
- Die Nachweise der Audittätigkeiten und -ergebnisse sollten dokumentiert und der zuständigen Geschäftsführung vorgelegt werden.

GV.OV-03 Die Leistung des organisatorischen Managements von Cybersicherheitsrisiken wird bewertet und auf erforderliche Anpassungen hin überprüft

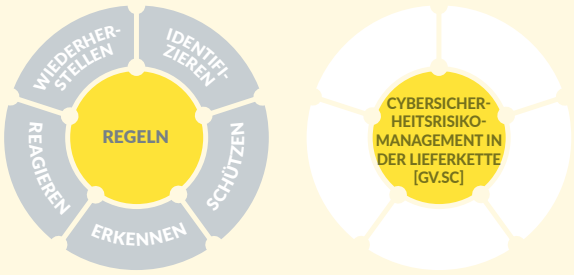
GV.OV-03.1 Die Leistung der Organisation im Bereich des Managements von Cybersicherheitsrisiken wird bewertet, überprüft und bei Bedarf angepasst

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Leistung einer Organisation im Bereich des Managements von Cybersicherheitsrisiken kontinuierlich bewertet, überprüft und bei Bedarf angepasst wird.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Es sollten wichtige Leistungsindikatoren (Key Performance Indicators – KPIs) ermittelt, eingeführt und regelmäßig überprüft werden, um sicherzustellen, dass die organisationsweiten Richtlinien und Verfahren die Ziele der Informations- und Cybersicherheit erreichen.
- Die wichtigsten informations- und cybersicherheitsbezogenen Risikoindikatoren sollten regelmäßig bewertet werden, um die Risiken für die Organisation zu ermitteln, einschließlich der Wahrscheinlichkeit und der möglichen Auswirkungen. Informations- und cybersicherheitsbezogene Risikoindikatoren sind zum Beispiel:
  - Die Anzahl der erkannten Cyberangriffe
  - Die Anzahl der erkannten Datenlecks
  - Die Zeit bis zur Erkennung
  - Die Zeit bis zur Wiederherstellung
  - Die Anzahl der Geräte, die nicht von der Organisation verwaltet werden
  - Der Umfang des Zugriffs verschiedener Nutzer auf sensible Daten
  - Die Anzahl der nicht aktuellen Softwareprogramme und Systeme
  - Die Anzahl der nicht verwalteten Netzwerkverbindungen
- Metriken zum Informations- und Cybersicherheitsrisikomanagement sollten gesammelt und der Führungsebene mitgeteilt werden.



Die Prozesse für das Cybersicherheitsrisikomanagement in der Lieferkette werden von organisatorischen Stakeholdern identifiziert, eingerichtet, verwaltet, überwacht und verbessert

GV.SC-01 Ein Programm zum Cybersicherheitsrisikomanagement in der Lieferkette, eine diesbezügliche Strategie, Ziele, Richtlinien und Prozesse sind etabliert und von den organisatorischen Stakeholdern akzeptiert

GV.SC-01.1 Ein Programm zum Cybersicherheitsrisikomanagement in der Lieferkette, eine diesbezügliche Strategie, Ziele, Richtlinien und Prozesse werden dokumentiert, überprüft, bei Veränderungen aktualisiert und von den organisatorischen Stakeholdern akzeptiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Cybersicherheitsrisiken in der Lieferkette durch ein dokumentiertes, von den Stakeholdern genehmigtes und regelmäßig aktualisiertes Risikomanagementprogramm proaktiv gemanagt werden.

Die nachstehenden Schritte sollten von Organisationen in Betracht gezogen werden, um ein Programm für das Cybersicherheitsrisikomanagement in der Lieferkette (C-SCRM) einzurichten, das auf ihre strategischen Ziele abgestimmt ist und von allen relevanten Stakeholdern unterstützt wird:

- Definieren Sie das Programm und die Strategie
  - **Identifizieren Sie die Ziele**: Definieren Sie klar, was das Unternehmen mit seinem C-SCRM-Programm erreichen möchte. Zu den Zielen können der Schutz vor Angriffen auf die Lieferkette, die Einhaltung von Vorschriften und die Aufrechterhaltung der Geschäftskontinuität gehören.
  - **Entwickeln Sie eine Strategie**: Skizzieren Sie eine übergeordnete Strategie, die mit den allgemeinen Cybersicherheits- und Geschäftsstrategien des Unternehmens in Einklang steht. Diese sollte eine Risikobewertung, Risikominderung und Pläne zur kontinuierlichen Überwachung umfassen.
- Beziehen Sie Stakeholder ein
  - **Identifizieren Sie Stakeholder**: Bestimmen Sie, wer die wichtigsten Stakeholder sind, einschließlich der Führungskräfte, der IT, der Beschaffung, der Rechtsabteilung und der Compliance-Teams.
  - **Einbeziehung der Stakeholder**: Beziehen Sie die Stakeholder frühzeitig in den Prozess ein, um ihre Mitwirkung und Zustimmung sicherzustellen. Dies kann durch Workshops, Meetings und regelmäßige Mitteilungen geschehen.
- Legen Sie Richtlinien und Prozesse fest
  - **Entwickeln Sie Richtlinien**: Erstellen Sie umfassende dokumentierte Richtlinien, die alle Aspekte des C-SCRM abdecken, einschließlich des Risikomanagements von Anbietern, der Reaktion auf Vorfälle und der Einhaltung von Vorschriften.
  - **Implementieren Sie Prozesse**: Definieren und dokumentieren Sie Prozesse für Risikobewertung, Anbieterbewertung, Vertragsmanagement und Reaktion auf Vorfälle. Stellen Sie sicher, dass diese Prozesse in bestehende Geschäftsabläufe integriert werden.

- Risikobewertung und -management
  - **Führen Sie Risikobewertungen durch**: Bewerten Sie regelmäßig die mit der Lieferkette verbundenen Risiken, einschließlich potenzieller Schwachstellen und Bedrohungen.
  - **Minimieren Sie Risiken**: Entwickeln und implementieren Sie Strategien zur Risikominimierung auf Grundlage der Bewertungsergebnisse. Dazu könnten die Diversifizierung der Lieferanten, die Verbesserung der Sicherheitskontrollen und die Erstellung von Notfallplänen gehören.
- Kontinuierliche Überwachung und Verbesserung
  - **Überwachen Sie kontinuierlich**: Implementieren Sie eine kontinuierliche Überwachung der Lieferkette, um neue Risiken frühzeitig zu erkennen und darauf zu reagieren. Dies umfasst die Überwachung der Leistung und Einhaltung der Vorschriften durch Lieferanten.
  - **Überprüfen und Verbessern**: Überprüfen Sie regelmäßig die Wirksamkeit des C-SCRM-Programms und nehmen Sie bei Bedarf Verbesserungen vor. Dies sollte Feedback von Stakeholdern und aus Vorfällen gewonnene Erkenntnisse umfassen.
- Schulung und Sensibilisierung
  Schulen Sie die Mitarbeiter: Bieten Sie Schulungs- und Sensibilisierungsprogramme für Mitarbeiter an, damit diese ihre Rolle im C-SCRM verstehen. Dazu gehören das Erkennen von Risiken in der Lieferkette und die Befolgung festgelegter Richtlinien und Verfahren.
- Dokumentation und Kommunikation
  - **Dokumentieren Sie alles**: Stellen Sie sicher, dass alle Richtlinien, Prozesse, Risikobewertungen und Pläne zur Risikominderung gut dokumentiert, auf dem neuesten Stand gehalten, vom zuständigen Management genehmigt und für alle Stakeholder zugänglich sind.
  - **Kommunizieren Sie effektiv**: Halten Sie einen offenen Kommunikationskanal mit den Stakeholdern aufrecht, um sie über den Fortschritt des Programms, Änderungen und etwaige Vorfälle auf dem Laufenden zu halten.

GV.SC-02 Cybersicherheitsrollen und -Verantwortlichkeiten für Lieferanten, Kunden und Partner werden intern und extern festgelegt, kommuniziert und koordiniert.

GV.SC-02.1 Drittanbieter melden jede Versetzung, Kündigung oder Versetzung von Mitarbeitern, die physischen oder logischen Zugriff auf geschäftskritische Systemelemente der Organisation haben.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Kontinuität und Sicherheit kritischer Systeme zu gewährleisten, indem Drittanbieter verpflichtet werden, personelle Veränderungen, die den Zugang betreffen, zu melden.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Zu den Drittanbietern gehören beispielsweise Dienstleister, Subunternehmer und andere Organisationen, die Systementwicklung, Technologiedienste, ausgelagerte Anwendungen oder Netz- und Sicherheitsmanagement anbieten.
- Regeln und Protokolle für den Informationsaustausch zwischen der Organisation und ihren Lieferanten und Unterlieferanten sollten in vertraglichen Vereinbarungen festgelegt werden.

GV.SC-03 Das Cybersicherheitsrisikomanagement in der Lieferkette ist in die Prozesse für Cybersicherheit und Unternehmensrisikomanagement, Risikobewertung und Verbesserungsprozesse integriert

GV.SC-03.1 Das Risikomanagement für die Informations- und Cybersicherheit in der Lieferkette ist in das Informations-/Cybersicherheits- und Unternehmensrisikomanagement, die Risikobewertung und die Verbesserungsprozesse integriert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Risiken für die Cybersicherheit in der Lieferkette durchgängig identifiziert, bewertet und gemindert werden, indem sie in die Risikobewertungen des Unternehmens, die Kontrollprüfungen und die kontinuierlichen Verbesserungszyklen einbezogen werden.

Um das Risikomanagement in der Lieferkette effektiv in umfassendere Rahmenwerke für Cybersicherheit und Unternehmensrisiken zu integrieren, sollten Organisationen Folgendes in Betracht ziehen:

Identifizierung von Ausrichtung und Überschneidung

- Bilden Sie bestehende Informationen/Prozesse zum Cybersicherheitsrisikomanagement und zum Unternehmensrisikomanagement (ERM) ab.
- Identifizieren Sie Berührungspunkte, an denen sich Risiken in der Lieferkette überschneiden:
  - Verwaltung der Lieferanten
  - Beschaffung
  - Geschäftskontinuität
  - Rechtliches und Compliance
- Dokumentieren Sie Überschneidungen, Duplizierungen oder Lücken, um die Integration zu optimieren.

Etablierung integrierter Kontrollsätze

- Entwickeln Sie einen einheitlichen Kontrollrahmen, der Folgendes umfasst:
  - Spezifische Kontrollen für die Cybersicherheit der Lieferkette (z. B. Zugang Dritter, Datenverarbeitung, Softwareintegrität).
  - Kontrollen aus bestehenden Cybersicherheitsstandards (z. B. ISO/IEC 27036).
- Stellen Sie sicher, dass die Kontrollen risikobasiert und skalierbar sind und sowohl auf die IT- als auch auf die OT-Umgebung abgestimmt sind.

Einbettung in Risikobewertungsprozesse

- Beziehen Sie spezifische Bedrohungsszenarien für die Lieferkette in Ihre Risikobewertungen ein (z. B. Kompromittierung von Lieferanten, gefälschte Hardware, Software-Schwachstellen).
- Bewerten Sie die Kritikalität und das Risiko der Lieferanten als Teil des Unternehmensrisikoregisters.
- Verwenden Sie abgestufte Risikobewertungen auf der Grundlage der Auswirkungen auf den Lieferanten und der Sensibilität der Dienste/Daten.

Einbeziehung in die kontinuierliche Verbesserung

- Integrieren Sie Erkenntnisse zu Risiken in der Lieferkette in:
  - Aus Vorfällen und Audits gezogene Erkenntnisse
  - Post-Mortem-Prüfungen von lieferantenbedingten Unterbrechungen
  - Zyklen zur Prozessverbesserung (z. B. PDCA)
- Aktualisieren Sie Richtlinien, Verfahren und Kontrollen auf Grundlage sich verändernder Bedrohungen und der Lieferantenleistung.

Eskalation wesentlicher Risiken an das Senior Management

- Definieren Sie Kriterien für die Wesentlichkeit (z. B. finanzielle Auswirkungen, regulatorische Risiken, Betriebsunterbrechungen).
- Richten Sie einen formellen Eskalationspfad zur Führungsebene und zu den Risikoausschüssen ein.
- Stellen Sie sicher, dass Risiken in der Materialversorgungskette:
  - Im Unternehmensrisikoregister reflektiert sind
  - In strategischen Risikodiskussionen angesprochen werden
  - Bei der Planung der Geschäftskontinuität und des Krisenmanagements berücksichtigt sind

GV.SC-05 Anforderungen zur Bewältigung von Cybersicherheitsrisiken in Lieferketten werden festgelegt, priorisiert und in Verträge und andere Arten von Vereinbarungen mit Lieferanten und anderen relevanten Dritten integriert

GV.SC-05.1 Es werden Anforderungen für den Umgang mit Cybersicherheitsrisiken und den Austausch sensibler Informationen in Lieferketten festgelegt, priorisiert, in Verträge und andere Arten von formellen Vereinbarungen integriert und durchgesetzt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, Anforderungen an die Cybersicherheit und den Umgang mit sensiblen Daten in Vereinbarungen über die Lieferkette festzulegen und durchzusetzen, indem sie in die Verträge aufgenommen und je nach Risiko priorisiert werden.

Um dies zu ermöglichen, sollten folgende Punkte berücksichtigt werden:

- Vertragliche Vereinbarungen und andere Arten von formellen Vereinbarungen mit Lieferanten und anderen relevanten Drittparteien sollten Erwartungen, Verantwortlichkeiten und Sicherheitsanforderungen definieren.
- Zu den Schlüsselelementen dieser Vereinbarungen gehören der Informationsaustausch zwischen der Organisation und ihren Lieferanten und Unterlieferanten, Sicherheitskontrollen, die Reaktion auf Vorfälle und die erforderliche Einhaltung von Normen und Vorschriften.
- Für Lieferanten, Produkte und Services sollten Sicherheitsanforderungen festgelegt werden, die in einem angemessenen Verhältnis zur Kritikalität und zu den möglichen Folgen einer Beeinträchtigung stehen.
- Alle Anforderungen an die Cybersicherheit und die Lieferkette, die Drittparteien einhalten müssen, sollten in Standardverträgen (d. h. in vorformulierten, allgemein verwendeten Begriffen und Klauseln, die Konsistenz, Einhaltung und Klarheit gewährleisten) enthalten sein. Der Vertrag sollte auch festlegen, wie die Einhaltung dieser Anforderungen überprüft wird.
- Erwägen Sie, in die Durchsetzung aufzunehmen, dass Drittanbieter und -nutzer (z. B. Lieferanten, Kunden, Partner) in der Lage sein sollten, das Verständnis ihrer Rollen und Verantwortlichkeiten nachzuweisen.
- Erwägen Sie die Festlegung von Sicherheitsanforderungen in Service-Level-Agreements (SLAs) zur Überwachung der Lieferanten auf akzeptable Sicherheitsleistung während des gesamten Lebenszyklus der Lieferantenbeziehung.
- Erwägen Sie, Lieferanten vertraglich zu verpflichten, ihre Mitarbeiter zu überprüfen und sich gegen Insider-Bedrohungen zu schützen.
- Ziehen Sie in Erwägung, Lieferanten vertraglich zu verpflichten, den Nachweis zu erbringen, dass sie akzeptable Sicherheitspraktiken anwenden, z. B. durch Selbsteinschätzung (z. B. CyFun®), Konformität mit bekannten Standards, Verifizierungen (z. B. CyFun®), Zertifizierungen (z. B. CyFun®) oder Inspektionen.
- Denken Sie daran, dass die Anforderungen der DSGVO erfüllt werden müssen, wenn Geschäftsinformationen personenbezogene Daten enthalten (gilt für alle Ebenen), d. h. Schutzmaßnahmen sollten in den vertraglichen Rahmen aufgenommen werden.

GV.SC-05.2 Vertragliche Informationen/Cybersicherheitsanforderungen für Lieferanten und externe Partner werden implementiert, um einen überprüfbaren Fehlerbehebungsprozess zu gewährleisten und sicherzustellen, dass Mängel, die bei Informations-/Cybersicherheitstests und -bewertungen festgestellt wurden, behoben werden.

Implementierungshinweise

Ziel dieser Kontrolle, die mit GV.SC-09.1 zusammenhängt, ist es, durchsetzbare Anforderungen in Lieferantenverträgen zu verankern, um die rechtzeitige Behebung von Mängeln und die Lösung von Cybersicherheitsproblemen zu gewährleisten, die bei Tests und Bewertungen festgestellt wurden.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Informationssysteme mit Software (oder Firmware), die von kürzlich bekannt gegebenen Softwarefehlern betroffen sind (und potenzielle Schwachstellen, die sich aus diesen Fehlern ergeben), sollten identifiziert werden.
- Neu veröffentlichte sicherheitsrelevante Patches, Service Packs und Hot Fixes sollten installiert werden, und diese Patches, Service Packs und Hot Fixes sollten vor der Installation auf ihre Wirksamkeit und mögliche Nebenwirkungen auf die Informationssysteme der Organisation getestet werden. Schwachstellen, die bei Sicherheitsbeurteilungen, der kontinuierlichen Überwachung, der Reaktion auf Zwischenfälle oder der Behandlung von Fehlern im Informationssystem entdeckt werden, werden ebenfalls zügig behoben. Die Behebung von Fehlern sollte als Notfalländerung in das Konfigurationsmanagement aufgenommen werden.
- Erwägen Sie, Lieferanten vertraglich dazu zu verpflichten, Informationen/Cybersicherheitsmerkmale, Funktionen und Schwachstellen ihrer Produkte und Dienstleistungen während der gesamten Lebensdauer des Produkts oder der Dauer der Dienstleistung offenzulegen.
- Erwägen Sie, Lieferanten vertraglich zu verpflichten, ein aktuelles Komponenteninventar (z. B. Software- oder Hardware-Stücklisten) für kritische Produkte bereitzustellen und zu pflegen.

GV.SC-05.3 Die Organisation legt vertragliche Anforderungen fest, die es ihr ermöglichen, die von Lieferanten und Drittpartnern implementierten Informations-/Cybersicherheitsprogramme zu überprüfen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation die Informations-/Cybersicherheitspraktiken von Lieferanten und Drittpartnern durch vertragliche Vereinbarungen bewerten und überprüfen kann.

Um dieses Ziel zu erreichen:

- **Anforderungen an die Informations-/Cybersicherheit**
  In den Verträgen sollten klare Erwartungen an die Informations-/Cybersicherheit definiert werden, einschließlich OT-spezifischer Kontrollen, sofern relevant.
- **Audit- und Bewertungsrechte**
  Vereinbarungen sollten der Organisation das Recht einräumen, die Informations-/Cybersicherheitsprogramme von Lieferanten und Partnern zu auditieren, zu bewerten oder zu überprüfen.
- **Verifizierungsmethoden**
  Die Konformität sollte durch Selbstbewertungen, Zertifizierungen durch Dritte oder planmäßige Sicherheitsbewertungen verifiziert werden.
- **Protokolle für den Informationsaustausch**
  In den Verträgen sollte festgelegt werden, welche Informationen/cybersicherheitsrelevanten Informationen wie oft und über welche Kanäle weitergegeben werden müssen.
- **Kontinuierliche Überwachung**
  Lieferanten sollten regelmäßig über ihre Informations-/Cybersicherheitslage berichten und Vorfälle melden, die den Betrieb beeinträchtigen könnten, insbesondere in OT-Umgebungen.
- **Konsequenzen bei Nichteinhaltung**
  In den Verträgen sollten Konsequenzen für die Nichteinhaltung von Informations-/Cybersicherheitsanforderungen festgelegt werden, z. B. Strafen oder Vertragskündigung.

GV.SC-06 Planung und Due Diligence werden durchgeführt, um Risiken zu reduzieren, bevor formelle Beziehungen zu Lieferanten oder anderen Dritten eingegangen werden

GV.SC-06.1 Vor dem Eingehen formeller Beziehungen mit Lieferanten oder anderen Dritten werden Planung und Due Diligence durchgeführt, um Risiken zu minimieren.

Implementierungshinweise

Ziel dieser Kontrolle ist es, Cybersicherheits- und Betriebsrisiken zu reduzieren, indem sichergestellt wird, dass vor dem Eingehen formeller Beziehungen mit Lieferanten oder Dritten eine angemessene Planung und Due Diligence durchgeführt wird.

Um dieses Ziel zu erreichen:

- **Risikobasierte Due Diligence**
  Die Due Diligence potenzieller Lieferanten sollte im Einklang mit der Beschaffungspolitik der Organisation durchgeführt werden und dem Risiko, der Kritikalität und der Komplexität der Beziehung entsprechen.
- **Bewertung der Cybersicherheit und der Risikofähigkeit**
  Der Reifegrad der Cybersicherheit, die Risikomanagementpraktiken und die OT-spezifischen Fähigkeiten der Lieferanten sollten auf ihre Eignung geprüft werden.
- **Risikobewertungen von Lieferanten**
  Risikobewertungen sollten durchgeführt werden, um sicherzustellen, dass sie mit den Geschäftsanforderungen und den geltenden Cybersicherheitsanforderungen, einschließlich der für OT-Umgebungen relevanten, übereinstimmen.
- **Produktintegrität und -sicherheit**
  Die Authentizität, Integrität und Sicherheit kritischer Produkte und Komponenten sollte vor der Beschaffung und dem Einsatz verifiziert werden, insbesondere bei OT-Systemen, bei denen Schwachstellen die Sicherheit und den Betrieb beeinträchtigen können.

GV.SC-07 Die Risiken, die von einem Lieferanten, seinen Produkten und Dienstleistungen sowie von anderen Dritten ausgehen, werden verstanden, aufgezeichnet, nach Prioritäten geordnet, bewertet, beantwortet und im Laufe der Geschäftsbeziehung überwacht

GV.SC-07.1 Die Risiken, die von einem Lieferanten, seinen Produkten und Dienstleistungen sowie anderen Drittparteien ausgehen, werden mindestens einmal jährlich und bei Änderungen während der Geschäftsbeziehung identifiziert, dokumentiert, priorisiert, gemindert und bewertet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Risiken im Zusammenhang mit Lieferanten, deren Produkten und Services sowie anderen Drittparteien während der gesamten Geschäftsbeziehung kontinuierlich identifiziert, bewertet, nach Prioritäten geordnet und verwaltet werden, insbesondere wenn Änderungen in kritischen Systemen auftreten.

Um dieses Ziel zu erreichen:

- **Maßgeschneiderte Risikobewertungen**
  Bewertungsformate und -häufigkeit sollten auf der Grundlage des Rufs des Lieferanten und der Kritikalität der gelieferten Produkte oder Services, einschließlich OT-Komponenten, angepasst werden.
- **Breitere Risikobetrachtungen**
  Risikobewertungen sollten potenzielle Serviceunterbrechungen und Konzentrationsrisiken einschließen, die sich auf den Betrieb oder die OT-Umgebung auswirken könnten.
- **Compliance-Nachweis**
  Lieferanten sollten die Einhaltung der vertraglichen Cybersicherheitsanforderungen nachweisen, z. B. durch Selbstbewertungen (z. B. CyFun®) Zertifizierungen, Garantien, Testergebnisse, Kennzeichnungen oder Auditberichte Dritter.
- **Laufende Überwachung**
  Kritische Lieferanten sollten während der gesamten Geschäftsbeziehung durch Inspektionen, Audits, Tests oder andere Bewertungsmethoden überwacht werden, um sicherzustellen, dass die Sicherheitsverpflichtungen weiterhin erfüllt werden.
- **Aktualisierungen des Risikoprofils**
  Änderungen bei den Services, Produkten oder Leistungen der Lieferanten sollten eine Neubewertung ihres Risikoprofils und ihrer Kritikalität auslösen, insbesondere wenn OT-Systeme betroffen sind.
- **Planung der Geschäftskontinuität**
  Es sollte ein Maßnahmenplan vorhanden sein, um unerwartete Unterbrechungen bei Lieferanten zu bewältigen und die Betriebskontinuität aufrechtzuerhalten.

GV.SC-07.2 Es wird eine dokumentierte Liste aller kritischen Lieferanten, Anbieter und Partner der Organisation erstellt, die an einem schwerwiegenden Vorfall beteiligt sein könnten. Diese Liste wird unter gebührender Berücksichtigung der Vertraulichkeit und Sicherheit auf dem neuesten Stand gehalten und online sowie offline verfügbar gemacht.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass eine zuverlässige, aktuelle Liste wichtiger Lieferanten, Anbieter und Partner sowohl online als auch offline gepflegt und zugänglich ist, um bei größeren Vorfällen eine schnelle Reaktion zu ermöglichen und gleichzeitig Vertraulichkeit und Sicherheit zu gewährleisten.

Um dieses Ziel zu erreichen:

- **Führen Sie ein umfassendes Verzeichnis**
  Es sollte eine vollständige Liste aller Lieferanten, Anbieter und Partner geführt werden, um diejenigen zu identifizieren, die für den Betrieb, einschließlich OT-Umgebungen, von kritischer Bedeutung sind.
- **Definieren Sie Kritikalitätskriterien**
  Es sollten klare Kriterien etabliert werden, um die Kritikalität von Lieferanten anhand von Faktoren wie den folgenden zu klassifizieren:
  - Sensibilität der verarbeiteten Daten
  - Zugang zu Systemen oder Netzwerken
  - Bedeutung für das Kerngeschäft oder OT-Funktionen
- **Dokumentieren Sie Schlüsselinformationen**
  Für jeden wichtigen Lieferanten sollte die Liste Folgendes enthalten:
  - Primäre und sekundäre Kontaktangaben
  - Beschreibung der erbrachten Dienstleistungen
  - Eskalationspfade und Verfügbarkeit von Support
- **Stellen Sie die Online- und Offline-Verfügbarkeit sicher**
  Die Liste sollte:
  - Regelmäßig aktualisiert und sicher gespeichert werden
  - Online- und Offline-Zugriff (z. B. gedruckte Kopien, verschlüsselte USB-Sticks) ermöglichen, um die Verfügbarkeit bei Cybervorfällen oder Ausfällen zu gewährleisten

GV.SC-07.3 Die Organisation auditiert geschäftskritische externe Dienstleister hinsichtlich der Einhaltung von Sicherheitsvorschriften.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass geschäftskritische Drittanbieter regelmäßig geprüft werden, um die Einhaltung der vereinbarten Sicherheitsanforderungen zu bestätigen und so die Risiken für den Betrieb und die kritischen Systeme zu kontrollieren.

Um dieses Ziel zu erreichen:

- **Identifizieren Sie kritische Anbieter**
  Die Kritikalität von Drittanbietern sollte anhand ihrer Auswirkungen auf den Betrieb, einschließlich OT-Systeme, und des von ihnen ausgehenden Risikos bewertet werden.
- **Akzeptable Prüfungsnachweise**
  Ergebnisse von Audits durch Dritte, wie Zertifizierungen, unabhängige Bewertungen oder Sicherheitsbescheinigungen, sollten gegebenenfalls als gültige Nachweise für die Konformität akzeptiert werden.
- **Führen Sie Sicherheitsaudits durch**
  Kritische Anbieter sollten regelmäßig Audits unterzogen werden, um zu verifizieren, dass sie ihre vertraglichen und richtlinienbasierten Sicherheitsverpflichtungen erfüllen.

GV.SC-07.4 Die Organisation stellt die Einhaltung der vertraglichen Verpflichtungen hinsichtlich Informations-/Cybersicherheit durch Lieferanten und Drittpartner sicher, indem sie regelmäßige Überprüfungen von unabhängigen Audits, Bewertungen und Evaluierungen durch Dritte vornimmt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, durch regelmäßige Überprüfungen unabhängiger Audits, Bewertungen und Evaluierungen durch Dritte sicherzustellen, dass Lieferanten und Drittpartner die vertraglichen Informations- und Cybersicherheitsverpflichtungen einhalten.

Um dieses Ziel zu erreichen:

- **Bauen Sie auf verwandten Kontrollen auf**
  Diese Kontrolle sollte in Übereinstimmung mit GV.SC-05.3 und GV.SC-07.1 implementiert werden, um die Lieferantenüberwachung zu stärken.
- **Integrieren Sie Risikobewertungen**
  Unabhängige Audits und Bewertungen durch Dritte sollten Bewertungen der Unternehmensanforderungen und geltenden Cybersicherheitsanforderungen umfassen, einschließlich Risiken in der Lieferkette und OT-spezifischer Risiken.
- **Nehmen Sie vor der Zusammenarbeit eine Verifizierung vor**
  Vor der Zusammenarbeit mit wichtigen Lieferanten sollten unabhängige Bewertungen überprüft werden, um die Einhaltung der vereinbarten Cybersicherheitsstandards und -verpflichtungen zu bestätigen.
- **Risikobasierte Prüfungstiefe**
  Die Prüfungstiefe und -häufigkeit sollte sich nach der Kritikalität der Produkte oder Dienstleistungen des Lieferanten richten. Kritischere Lieferanten sollten einer gründlicheren Bewertung unterzogen werden.

GV.SC-08 Relevante Lieferanten und andere Dritte werden in die Planung, Reaktion und Wiederherstellung von Vorfällen einbezogen

GV.SC-08.1 Die Organisation identifiziert und dokumentiert wichtige Mitarbeiter relevanter Lieferanten und anderer Drittparteien, um sie in die Planung, Reaktion und Wiederherstellung bei Vorfällen einzubeziehen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Vorbereitung auf einen Vorfall und die Wiederherstellung zu verbessern, indem sichergestellt wird, dass wichtige Mitarbeiter von kritischen Zulieferern und Drittparteien identifiziert und aktiv in die Reaktionsplanung und -ausführung einbezogen werden.

Um dieses Ziel zu erreichen:

- **Legen Sie Kommunikationsprotokolle fest**
  Es sollten klare Regeln und Verfahren für die Meldung des Vorfallsstatus und die Koordinierung der Reaktions- und Wiederherstellungsaktivitäten zwischen der Organisation und ihren geschäftskritischen Zulieferern festgelegt werden.
- **Definieren Sie Rollen und Zuständigkeiten**
  Rollen, Zuständigkeiten und Befugnisse für die Reaktion auf Vorfälle sollten sowohl für interne Teams als auch für externe Teilnehmer dokumentiert werden, einschließlich derjenigen, die OT-Systeme und -Infrastrukturen unterstützen.
- **Fördern Sie gemeinsames Lernen**
  Nach größeren Vorfällen sollten mit kritischen Zulieferern und Drittparteien gemeinsame Lessons-Learned-Sitzungen durchgeführt werden, um die künftige Koordination und Resilienz zu verbessern.

GV.SC-09 Sicherheitspraktiken in der Lieferkette sind in Programme zur Cybersicherheit und zum Risikomanagement im Unternehmen integriert, und ihre Leistung wird während des gesamten Lebenszyklus von Technologieprodukten und -dienstleistungen überwacht

GV.SC-09.1 Die Sicherheitspraktiken in der Lieferkette werden in die Programme für Informations-/Cybersicherheit und Unternehmensrisikomanagement integriert, und ihre Leistung wird während des gesamten Produkt- und Dienstleistungslebenszyklus überwacht.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Sicherheitspraktiken in der Lieferkette in die Programme der Organisation für Informationssicherheit, Cybersicherheit und Risikomanagement eingebettet sind und die Leistung während des gesamten Lebenszyklus von Produkten und Dienstleistungen überwacht und verbessert wird.

Um dieses Ziel zu erreichen:

- **Führen Sie einen Abgleich mit verwandten Kontrollen durch**
  Diese Kontrolle baut auf GV.SC-05.2 auf und stellt sicher, dass vertragliche Informationen und Cybersicherheitsanforderungen, wie z. B. die Behebung von Mängeln und die Beseitigung festgestellter Defizite, im Rahmen umfassenderer Risikoprogramme aktiv verwaltet werden.
- **Etablieren Sie Governance-Grundlagen**
  Die Sicherheitsrichtlinien für die Lieferkette sollten dokumentiert werden und sowohl die Erwartungen hinsichtlich der Informations- als auch der Cybersicherheit für Lieferanten und Dritte abdecken.
- **Integrieren Sie in Risikorahmen**
  Lieferkettenrisiken sollten in Unternehmens- und Informationssicherheits-Risikomanagementrahmen eingebettet werden, einschließlich OT-spezifischer Risiken und Abhängigkeiten.
- **Formalisieren Sie Sicherheitsanforderungen**
  Verträge und SLAs sollten eindeutige Klauseln zu Informationen und Cybersicherheit, Prüfungsrechten und Leistungskennzahlen enthalten.
- **Überwachen und bewerten Sie die Leistung**
  Risikobewertungen, Audit-Berichte und Aufzeichnungen über Vorfälle sollten regelmäßig überprüft werden, um die Lage des Lieferanten zu beurteilen und verbesserungswürdige Bereiche zu ermitteln.
- **Ermöglichen Sie die kontinuierliche Überwachung**
  Überwachungstools und KPIs sollten verwendet werden, um die Sicherheitsleistung des Lieferanten über den gesamten Lebenszyklus hinweg zu verfolgen, einschließlich der Reaktionszeiten auf Vorfälle und der Konformitätsraten.
- **Unterstützen Sie Sensibilisierung und Schulung**
  Schulungs- und Sensibilisierungsprogramme sollten sich sowohl mit den internen Teams als auch mit den Lieferanten auf die Informations- und Cybersicherheitsrisiken der Lieferkette beziehen.
- **Stellen Sie die Abdeckung des gesamten Lebenszyklus sicher**
  Die Dokumentation sollte zeigen, dass die Sicherheit der Lieferkette von der Beschaffung bis zur Außerbetriebnahme berücksichtigt wird, insbesondere für OT-Systeme und -Komponenten.

GV.SC-010 Risikomanagementpläne für die Cybersicherheit in der Lieferkette enthalten Bestimmungen für Aktivitäten, die nach Abschluss einer Partnerschaft oder eines Dienstleistungsvertrags stattfinden

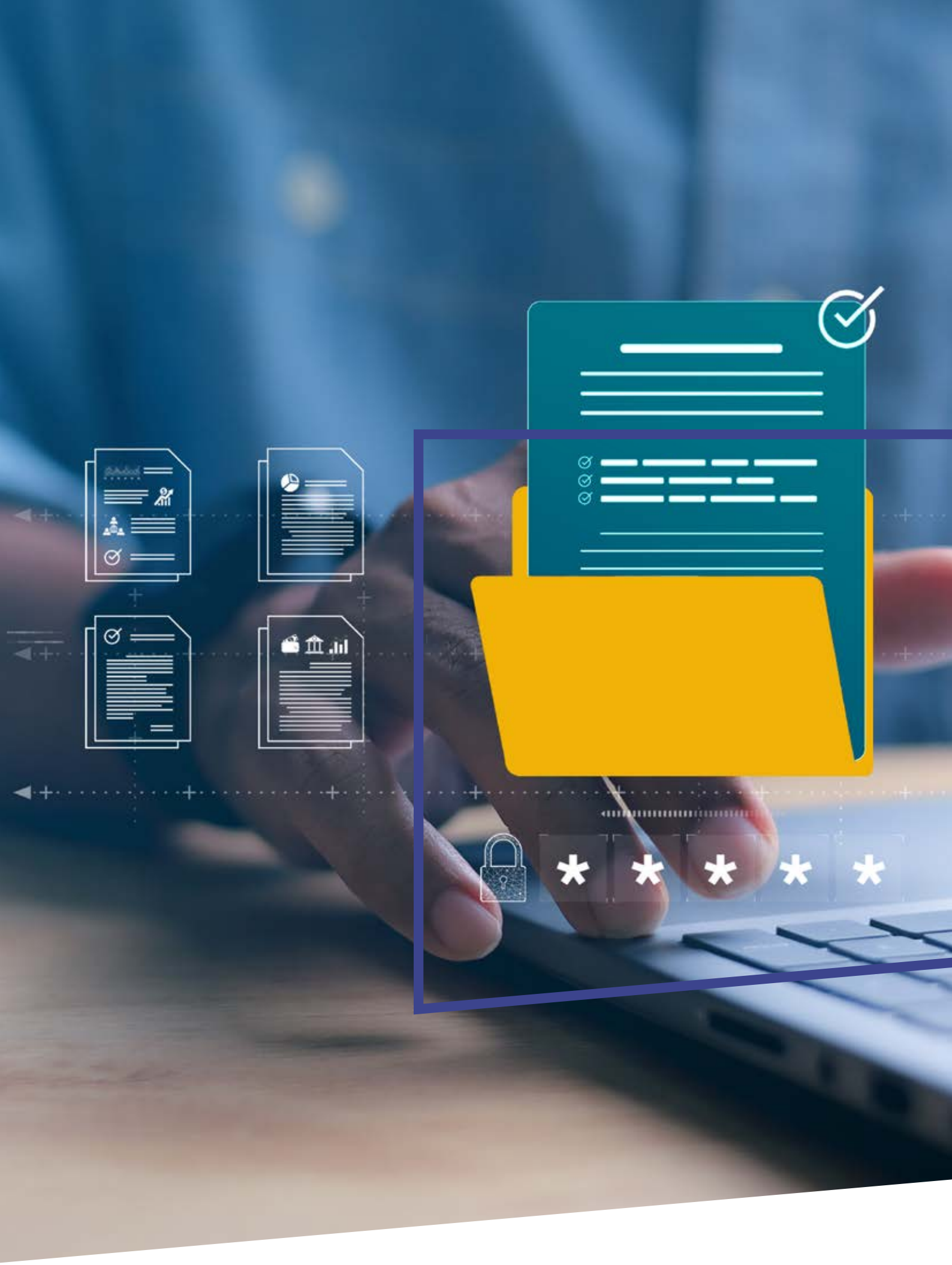
GV.SC-10.1 **Pläne für das Risikomanagement in der Lieferkette im Bereich Cybersicherheit enthalten Maßnahmen und Verantwortlichkeiten für das Management von Risiken, die nach Beendigung einer Lieferantenbeziehung oder eines Dienstleistungsvertrags auftreten können.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass verbleibende Risiken für die Cyber- und Informationssicherheit nach Beendigung der Lieferantenbeziehungen wirksam angegangen werden, um so Störungen, die Offenlegung von Daten und Schwachstellen in betrieblichen und OT-Umgebungen zu verhindern.

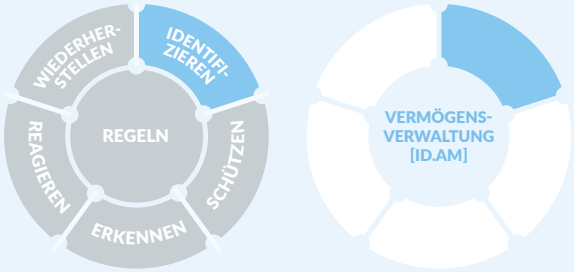
Um dieses Ziel zu erreichen:

- **Planen Sie die Beendigung der Beziehung**
  Formale Offboarding-Verfahren sollten für die Beendigung von Lieferantenbeziehungen sowohl unter normalen als auch unter ungünstigen Bedingungen, einschließlich Verstößen, Insolvenz oder Sicherheitsvorfällen, festgelegt werden.
- **Stellen Sie einen sicheren Übergang oder Ausstieg sicher**
  Für kritische Dienste sollten Übergangspläne entwickelt werden, um die Kontinuität aufrechtzuerhalten und die Widerstandsfähigkeit der Lieferkette zu gewährleisten, einschließlich Ausweichlieferanten oder interner Alternativen.
- **Entziehen Sie den Zugriff und sichern Sie Daten**
  Der Zugriff von Lieferanten auf Systeme, Netzwerke und Daten sollte unverzüglich entzogen werden. Alle Berechtigungsnachweise und Fernzugriffstools sollten deaktiviert oder entfernt werden.
- **Sichern Sie organisatorische Vermögenswerte**
  Geräte, Speichermedien und Dokumente, die organisatorische Daten enthalten, sollten sicher zurückgegeben oder bereinigt werden. Kontrollen sollten eine unbefugte Aufbewahrung oder Weitergabe sensibler Informationen verhindern.
- **Bewältigen Sie die Obsoleszenz von Komponenten**
  Es sollten Pläne vorhanden sein, um Komponenten oder Dienste am Ende ihrer Lebensdauer zu verwalten und eine kontinuierliche Unterstützung oder sichere Ersatzlösungen zu gewährleisten, insbesondere für OT-Systeme.
- **Überwachen Sie Restrisiken**
  Nach der Beendigung sollten Risiken identifiziert, bewertet und bei Bedarf an das Senior Management weitergegeben werden. Diese Risiken sollten im Rahmen des Risikomanagementprozesses des Unternehmens verfolgt werden.



IDENTIFIZIEREN

Identifizieren



Vermögenswerte (z. B. Daten, Hardware, Software, Systeme, Einrichtungen, Dienstleistungen, Mitarbeiter), die es der Organisation ermöglichen, ihre Geschäftsziele zu erreichen, werden entsprechend ihrer relativen Bedeutung für die Organisationsziele und die Risikostrategie der Organisation identifiziert und verwaltet.

ID.AM-01 Inventare der von der Organisation verwalteten Hardware werden geführt

ID.AM-01.1	Es wird ein Inventar der physischen und virtuellen Infrastrukturressourcen – wie Hardware, Netzwerkgeräte und Cloud-gehostete Umgebungen –, die die Informationsverarbeitung unterstützen, erstellt, überprüft und bei Änderungen aktualisiert.

Implementierungshinweise

Das Ziel dieser Kontrolle ist es, sicherzustellen, dass kritische Systeme und Services verfügbar bleiben, indem Redundanz in Übereinstimmung mit organisatorischen, rechtlichen und regulatorischen Verfügbarkeitsanforderungen implementiert wird.

Während sich ID.AM-01.1 auf die Infrastrukturebene konzentriert, ist diese Kontrolle eng mit ID.AM-02.1 verknüpft, die die Software und die darauf aufbauenden Services, wie Anwendungen, Plattformen und digitale Tools, verfolgt. Zusammen ergeben sie ein vollständiges Bild der Technologieumgebung der Organisation.

Um das Ziel von ID.AM-01.1 zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Organisationen sollten alle physischen und virtuellen Infrastrukturen identifizieren und dokumentieren, die die Informationsverarbeitung unterstützen, darunter Server, Workstations, Netzwerkgeräte, Speichersysteme und in der Cloud gehostete Ressourcen.
- Das Inventar sollte Schlüsselattribute wie Art, Standort, Eigentümer, Konfiguration und Lebenszyklusstatus des Vermögenswerts enthalten.
- Organisationen sollten nach Möglichkeit automatisierte Tools zur Erkennung und Verwaltung von Vermögenswerten in Betracht ziehen, um Genauigkeit und Aktualisierungen in Echtzeit zu gewährleisten.
- Das Inventar sollte regelmäßig überprüft und aktualisiert werden, insbesondere nach Änderungen wie Verlegungen, Stilllegungen oder Verlagerungen.
- Das Inventar sollte für alle relevanten Stakeholder zugänglich sein und in die Prozesse des Risikomanagements und der Reaktion auf Vorfälle integriert werden.

ID.AM-01.2 **Das Inventar der Vermögenswerte des Unternehmens, die mit Informationen und Informationsverarbeitungseinrichtungen in Zusammenhang stehen, spiegelt Veränderungen im Kontext der Organisation wider und umfasst alle Informationen, die für eine effektive Rechenschaftspflicht erforderlich sind.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Inventare der Vermögenswerte die betriebliche Transparenz unterstützen, eine verantwortungsvolle Eigentümerschaft ermöglichen und sich an Veränderungen in der Struktur, Technologie und Risikolandschaft der Organisation anpassen.

Um dieses Ziel zu erreichen:

- **Fügen Sie wichtige Details zu den Vermögenswerten hinzu**
  Die Inventare sollten die wichtigsten Angaben wie Hersteller, Gerätetyp, Modell, Seriennummer, Gerätename, Netzwerkadresse und Standort enthalten. OT-Vermögenswerte sollten gegebenenfalls einbezogen werden.
- **Unterstützen Sie die Rechenschaftspflicht**
  Aufzeichnungen der Vermögenswerte sollten die Rückverfolgbarkeit von Maßnahmen und Entscheidungen ermöglichen, um sicherzustellen, dass die Verantwortlichen identifiziert und für die Ergebnisse zur Rechenschaft gezogen werden können.
- **Berücksichtigen Sie organisatorische Änderungen**
  Inventare sollten aktualisiert werden, um Änderungen wie die Verlagerung von Vermögenswerten, Upgrades oder die Stilllegung von Vermögenswerten zu berücksichtigen, einschließlich solcher, die OT-Umgebungen betreffen.

ID.AM-01.3 **Wenn nicht autorisierte Hardware erkannt wird, wird sie für eine mögliche Ausnahmebehandlung unter Quarantäne gestellt, entfernt oder ersetzt, und das Inventar wird entsprechend aktualisiert.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, Sicherheitsrisiken zu verringern, indem sichergestellt wird, dass nicht autorisierte Hardware umgehend identifiziert, isoliert und beseitigt wird, während gleichzeitig ein genaues und nachvollziehbares Inventar geführt wird.

Um dies zu erreichen:

- **Definieren Sie nicht zugelassener Hardware**
  Jede Hardware, die nicht zugelassen ist oder für die es keine dokumentierten Ausnahmen gibt, sollte als nicht zugelassen bezeichnet werden.
- **Reagieren Sie auf Erkennung**
  Nicht autorisierte Hardware sollte zur Überprüfung unter Quarantäne gestellt, entfernt oder gegebenenfalls ausgetauscht werden. Das Inventar der Vermögenswerte sollte entsprechend aktualisiert werden.
- **Beziehen Sie OT-Überlegungen ein**
  Nicht autorisierte Geräte in OT-Umgebungen sollten aufgrund möglicher Auswirkungen auf die Sicherheit und den Betrieb mit erhöhter Vorsicht behandelt werden.

Beispiele für nicht autorisierte Hardware können sein:

- **Nicht zugelassene Endpunkte**: Persönliche oder nicht registrierte Laptops, Desktops oder mobile Geräte, die ohne Autorisierung mit dem Netzwerk verbunden sind.
- **Externe Speichergeräte**: USB-Laufwerke oder externe Festplatten, die nicht für die Verwendung zugelassen sind und die das Risiko von Malware oder Datenlecks bergen.
- **Nicht geprüfte IoT- und OT-Geräte**: Intelligente Geräte, Sensoren oder industrielle Komponenten, die ohne ordnungsgemäße Prüfung angeschlossen werden, stellen ein Risiko für IT- und OT-Umgebungen dar.
- **Nicht autorisierte Netzwerkausrüstung**: Ohne Genehmigung installierte drahtlose Zugangspunkte oder Switches, die möglicherweise die Netzwerksicherheitskontrollen umgehen.

ID.AM-01.4	**Es werden Mechanismen zur Erkennung des Vorhandenseins von nicht autorisierten Hardware- und Firmware-Komponenten in der IKT-/OT-Umgebung der Organisation identifiziert.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, nicht autorisierte Hardware- und Firmware-Komponenten in IKT- und OT-Umgebungen proaktiv zu identifizieren, um so eine zeitnahe Reaktion zu ermöglichen und das Risiko einer Gefährdung oder Betriebsunterbrechung zu verringern.

Um dieses Ziel zu erreichen:

- **Automatisieren Sie, wo dies möglich ist**
  Erkennungsmechanismen sollten automatisiert werden, wo dies sicher und technisch möglich ist, insbesondere in komplexen oder risikoreichen Umgebungen.
- **Überwachen Sie Netzwerke kontinuierlich**
  Netzwerke sollten kontinuierlich überwacht werden, um neue oder nicht autorisierte Hardware- und Firmware-Komponenten zu erkennen. Erkannte Änderungen sollten automatische Aktualisierungen des Vermögenswertinventars auslösen.
- **Richten Sie einen Reaktionsprozess ein**
  Es sollte ein definierter Prozess vorhanden sein, um nicht autorisierte Komponenten regelmäßig zu überprüfen und zu behandeln.
  - Für nicht autorisierte Hardware, siehe **ID.AM-01.3**
  - Für nicht autorisierte Firmware, siehe **ID.AM-02.4**
- **Berücksichtigen Sie OT-spezifische Aspekte**
  Erkennungsmethoden in OT-Umgebungen sollten bei der Identifizierung nicht autorisierter Komponenten Sicherheits-, Verfügbarkeits- und anbieterspezifische Einschränkungen berücksichtigen.

ID.AM-02 Inventare der von der Organisation verwalteten Software, Services und Systeme werden geführt

ID.AM-02.1	**Ein Inventar von Software, digitalen Services und Geschäftssystemen, die innerhalb der Organisation verwendet werden, wird dokumentiert, überprüft und bei Änderungen aktualisiert.**

Implementierungshinweise

Diese Kontrolle stellt sicher, dass alle Software, digitalen Services und Geschäftssysteme, die innerhalb der Organisation verwendet werden, identifiziert, verfolgt und regelmäßig aktualisiert werden. Sie konzentriert sich auf die funktionalen und immateriellen Teile der Technologieumgebung, wie Anwendungen, Plattformen und Cloud-Services, die auf der zugrunde liegenden Infrastruktur arbeiten oder mit ihr interagieren. Die Aktualisierung dieses Inventars unterstützt die betriebliche Kontinuität, stärkt die Sicherheit und hilft bei der Erfüllung von Compliance-Anforderungen.

Sie ist eng mit ID.AM-01.1 verknüpft, das die physische und virtuelle Infrastruktur (wie Server, Netzwerkgeräte und Cloud-Umgebungen) abdeckt, die diese Systeme unterstützt.

Zusammen bieten beide Kontrollen einen vollständigen Überblick über die Technologielandschaft der Organisation, von der grundlegenden Infrastruktur bis hin zu den Anwendungen und Services, die den Geschäftswert liefern.

Um dieses Ziel zu erreichen, sollten folgende Schritte berücksichtigt werden:

- **Identifizierung von Software und Services**
  Das Inventar sollte alle Anwendungen, Cloud-Services, APIs und Geschäftssysteme (z. B. ERP, CRM, HR-Plattformen) umfassen.
- **Aufzeichnung wichtiger Informationen**
  Jeder Eintrag sollte Version, Eigentümer, Zweck, Lizenztyp und Einsatzumgebung enthalten.
- **Wo möglich Automatisierung verwenden**
  Zur genauen Erkennung und Aktualisierung von Software und Services sollten automatisierte Erkennungstools eingesetzt werden.
- **Pflegen einer Software-Stückliste (Software Bill of Materials, SBOM)**
  Für kritische oder intern entwickelte Software sollte eine SBOM gepflegt werden, um Komponenten und Abhängigkeiten zu verfolgen.
- **Das Inventar auf dem neuesten Stand halten**
  Das Inventar sollte regelmäßig überprüft und aktualisiert werden, insbesondere nach Installationen, Upgrades oder Umzügen.
- **Abstimmung mit dem Infrastrukturinventar (ID.AM-01.1)**
  Software-Datensätze sollten mit der Infrastruktur, auf der sie laufen, verknüpft werden, um einen vollständigen Überblick über die Technologieumgebung zu erhalten.

ID.AM-02.2 Das Inventar, das widerspiegelt, welche Software, Services und Systeme in der Organisation verwendet werden, spiegelt Änderungen im Kontext der Organisation wider und enthält alle Informationen, die für eine wirksame Rechenschaftspflicht erforderlich sind.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass das Inventar an Software, Services und Systemen aktuell und vollständig bleibt, so dass eine Rückverfolgbarkeit, eine verantwortliche Eigentümerschaft und eine Anpassung an Änderungen im Betriebs- und Risikokontext der Organisation möglich sind.

Um dieses Ziel zu erreichen:

- **Beziehen Sie wichtige Bestandsdetails ein**
  Inventare sollten relevante Attribute wie Softwaretitel, Herausgeber, Datum der Erstinstallation oder -nutzung, Geschäftszweck, Version, Bereitstellungsmethode und Außerbetriebnahmedatum erfassen. Gegebenenfalls sollten URLs oder Quellen von App-Stores angegeben werden.
- **Unterstützen Sie die Rechenschaftspflicht**
  Inventaraufzeichnungen sollten die Rückverfolgbarkeit von Maßnahmen und Entscheidungen ermöglichen, um sicherzustellen, dass die Verantwortlichen identifiziert und für die Nutzung und Verwaltung von Software und Services zur Rechenschaft gezogen werden können.
- **Berücksichtigen Sie organisatorische Änderungen**
  Inventare sollten aktualisiert werden, um Änderungen wie neue Bereitstellungen, Upgrades oder Entfernungen widerzuspiegeln, einschließlich solcher, die OT-Systeme und eingebettete Softwarekomponenten betreffen.

ID.AM-02.3 Die Personen, die für die Verwaltung von Softwareplattformen und -anwendungen innerhalb der Organisation verantwortlich und rechenschaftspflichtig sind, werden formell identifiziert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Softwareplattformen und -anwendungen ordnungsgemäß verwaltet werden, indem klar festgelegt wird, wer für den täglichen Betrieb verantwortlich ist und wer für die Gesamtaufsicht und die Ergebnisse rechenschaftspflichtig ist.

Um dieses Ziel zu erreichen:

- **Definieren Sie Rollen klar**
  Die Personen, die für die Verwaltung der Software verantwortlich sind, sollten formell benannt werden. Dies sind die Personen, die die Arbeit ausführen, technische Entscheidungen treffen und operative Aufgaben durchführen (z. B. Entwickler, Systemadministratoren, Tester).
- **Weisen Sie Rechenschaftspflicht zu**
  Eine separate Rolle sollte formell zugewiesen werden, um den erfolgreichen Abschluss von softwarebezogenen Aufgaben zu überwachen und zu genehmigen. Dazu können Projektmanager, Produktverantwortliche oder Teamleiter gehören.
- **Wenden Sie dies auf alle Umgebungen an**
  Diese Rollen sollten sowohl für IT- als auch für OT-Umgebungen definiert werden, um sicherzustellen, dass auch die in industriellen Systemen verwendete Software ordnungsgemäß geregelt ist.

ID.AM-02.4 Wenn nicht autorisierte Software erkannt wird, wird sie für eine mögliche Ausnahmebehandlung unter Quarantäne gestellt, entfernt oder ersetzt, und das Inventar wird entsprechend aktualisiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, Sicherheits-, Betriebs- und Compliance-Risiken zu minimieren, indem sichergestellt wird, dass nicht autorisierte Software umgehend identifiziert, angemessen behandelt und im Software-Inventar der Organisation ausgewiesen wird.

Um dies zu erreichen:

- **Definieren Sie nicht autorisierte Software**
  Software, die ohne ordnungsgemäße Lizenzierung, Genehmigung oder dokumentierte Ausnahmen installiert oder verwendet wird, sollte als nicht autorisiert eingestuft werden.
- **Verstehen Sie die Risiken**
  Nicht autorisierte Software kann Folgendes mit sich bringen:
  - **Sicherheitslücken** (z. B. Malware oder Hintertüren)
  - **Datenschutzrisiken** (z. B. unzulässiger Umgang mit Daten)
  - **Ineffizienzen im Betrieb** (z. B. Kompatibilitätsprobleme)
  - **Verlust der Kontrolle** über Software-Nutzung und -Updates
- **Legen Sie Reaktionsverfahren fest**
  Nicht autorisierte Software sollte für eine mögliche Ausnahmebehandlung unter Quarantäne gestellt, entfernt oder ersetzt werden. Das Inventar der Software sollte entsprechend aktualisiert werden.
- **Unterstützen Sie durch zentralisierte Verwaltung**
  Ein zentralisierter Softwareverwaltungsprozess sollte eingerichtet werden, um die Auswahl von Anbietern, Legacy-Software und Sicherheitskontrollen zu überwachen.
- **Nutzen Sie, wenn zutreffend, SBOMs**
  Software-Stücklisten (Software Bills of Materials, SBOMs) sollten genutzt werden, um Komponenten, Bibliotheken und Module nachzuverfolgen und die Einhaltung von Lizenzbestimmungen und das Schwachstellenmanagement zu unterstützen, insbesondere bei OT- und eingebetteten Systemen.

ID.AM-02.5 Es werden Mechanismen zur Erkennung des Vorhandenseins von nicht autorisierter Software in der IKT-/OT-Umgebung der Organisation identifiziert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Mechanismen vorhanden sind, um nicht autorisierte Software in allen IKT- und OT-Umgebungen aufzuspüren und so eine rechtzeitige Reaktion zu ermöglichen und ein genaues Softwareinventar zu führen.

Um dieses Ziel zu erreichen:

- **Automatisieren Sie, wo dies möglich ist**
  Erkennungsmechanismen sollten automatisiert werden, wo dies sicher und technisch angemessen ist, insbesondere in komplexen oder hochriskanten Umgebungen.
- **Überwachen Sie alle Plattformen**
  Alle Plattformen, einschließlich physischer Systeme, virtueller Maschinen, Container und eingebetteter OT-Systeme, sollten kontinuierlich auf neue oder nicht autorisierte Software überwacht werden. Erkannte Änderungen sollten automatische Aktualisierungen des Softwareinventars auslösen.
- **Richten Sie einen Überprüfungsprozess ein**
  Es sollte ein Prozess vorhanden sein, um nicht autorisierte Software regelmäßig zu untersuchen und zu beseitigen. Wenn nicht autorisierte Software entdeckt wird, sollte **ID.AM-02.4** angewendet werden.
- **Passen Sie die Erkennung an OT-Umgebungen an**
  In OT-Umgebungen sollten Erkennungsmechanismen so angepasst werden, dass Betriebsstörungen vermieden werden. Passive Überwachung, vom Anbieter zugelassene Tools und geplante Scans sollten in Betracht gezogen werden, um Sicherheit und Systemverfügbarkeit zu gewährleisten.

ID.AM-03 Darstellungen der autorisierten Netzwerkkommunikation der Organisation sowie der internen und externen Netzwerkdatenflüsse werden gepflegt

ID.AM-03-2	**Die Netzwerkkommunikation und die internen Datenflüsse der Organisation werden abgebildet, dokumentiert, genehmigt und bei Änderungen aktualisiert.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die interne Netzwerkkommunikation und die Datenflüsse klar verstanden, ordnungsgemäß dokumentiert und auf dem neuesten Stand gehalten werden, um einen sicheren Betrieb und eine fundierte Entscheidungsfindung in IKT- und OT-Umgebungen zu unterstützen.

Um dieses Ziel zu erreichen:

- **Legen Sie Netzwerkgrundlagen fest**
  Kommunikations- und Datenflüsse über kabelgebundene, drahtlose und cloudbasierte Infrastrukturen (z. B. IaaS) sollten abgebildet, dokumentiert und autorisiert werden. Aktualisierungen sollten vorgenommen werden, wenn sich Änderungen ergeben.
- **Dokumentieren Sie die technischen Details**
  Die erwarteten Netzwerk-Ports, Protokolle und Services, die zwischen autorisierten Systemen verwendet werden, sollten aufgezeichnet werden, um die Überwachung und Fehlerbehebung zu unterstützen.
- **Integrieren Sie mit dem Konfigurationsmanagement**
  Die Prozesse des Konfigurationsmanagements sollten die Pflege und Validierung der Netzablaufdokumentation unterstützen.
- **Stellen Sie eine resiliente Dokumentation sicher**
  Die Netzablaufdokumentation sollte sicher und nicht nur auf dem darin beschriebenen Netz gespeichert werden. Es sollte eine geschützte Offline-Kopie (z. B. ein verschlüsseltes externes Laufwerk oder ein Ausdruck) aufbewahrt werden, um die Verfügbarkeit bei Ausfällen oder Vorfällen sicherzustellen.

ID.AM-03-3 **Die Netzwerkkommunikation und die externen Datenflüsse der Organisation werden abgebildet, dokumentiert, genehmigt und bei Änderungen aktualisiert.**

Implementierungshinweise

Das Ziel dieser Kontrolle ist es, sicherzustellen, dass die externe Netzwerkkommunikation klar verstanden, kontrolliert und überwacht wird, um das Risiko eines unbefugten Zugriffs, eines Datenlecks oder einer Dienstunterbrechung in IKT- und OT-Umgebungen zu verringern.

Um dieses Ziel zu erreichen:

- **Bilden Sie externe Abläufe ab und dokumentieren Sie sie**
  Kommunikations- und Datenflüsse zwischen der Organisation und externen Parteien sollten abgebildet, dokumentiert und autorisiert werden. Diese Aufzeichnungen sollten aktualisiert werden, wenn sich Änderungen ergeben.
- **Setzen Sie Zugriffskontrollen durch**
  Netzwerkverbindungen sollten auf ausdrücklich autorisierte Schnittstellen beschränkt werden, um die Angriffsfläche zu verringern und unbefugte Datenübertragungen zu verhindern.
- **Verstärken Sie die Überwachung bei Bedarf**
  Bei erhöhtem Risiko sollte die Überwachung intensiviert werden. Dies kann Echtzeitwarnungen, erweiterte Protokollierung oder häufigere Audits externer Netzwerkaktivitäten umfassen.
- **Verhindern Sie Informationslecks**
  Das Risiko von Datenlecks durch elektromagnetische Emissionen oder Seitenkanalangriffe sollte bewertet werden. Gegebenenfalls sollten Abhilfemaßnahmen wie EMSEC- oder TEMPEST-Kontrollen durchgeführt werden, insbesondere bei Systemen, die mit sensiblen oder klassifizierten Informationen arbeiten.

Die beiden Kontrollen – ID.AM-03-3 und ID.AM-04.2 – sind eng miteinander verbunden, konzentrieren sich aber auf unterschiedliche Bereiche des Informationsflusses und der Netzwerkaktivität. Diese Kontrolle, ID.AM-03-3, deckt die Interaktionen der Netzwerkschicht mit externen Entitäten ab, einschließlich:

- Internetverkehr (z. B. ausgehender Web-Zugang, DNS-Anfragen, E-Mail-Verkehr).
- VPN-Verbindungen, Fernzugriff und Kommunikation mit Cloud-Diensten.
- Jegliche Kommunikation, die über die Grenzen der Organisation hinausgeht, unabhängig davon, ob sie ein bestimmtes externes System betrifft.

ID.AM-04 Inventare der von Lieferanten erbrachten Dienste werden geführt

ID.AM-04.1 **Organisationen führen eine übersichtliche und aktuelle Liste aller von ihnen genutzten externen Services, einschließlich der Art und Weise, wie diese mit ihren Systemen verbunden sind. Diese Services sind vor ihrer Nutzung zu überprüfen und zu genehmigen, und die Liste ist zu aktualisieren, wenn sich Änderungen ergeben.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle von der Organisation genutzten externen Services eindeutig identifiziert, überprüft und auf dem neuesten Stand gehalten werden, um das Risiko eines unbefugten Zugriffs, nicht verwalteter Abhängigkeiten von Drittparteien oder einer Unterbrechung von Services in IKT- und OT-Umgebungen zu verringern.

Um dieses Ziel zu erreichen:

- **Führen Sie ein Inventar externer Services**
  Alle externen Services, auf die sich die Organisation stützt, sollten identifiziert und dokumentiert werden. Dazu gehören Services die sowohl in IT- als auch in OT-Umgebungen verwendet werden. Das Inventar sollte immer dann aktualisiert werden, wenn Services hinzugefügt, geändert oder entfernt werden.
- **Beschreiben und bilden Sie Serviceverbindungen ab**
  Die Art und Weise, wie jeder externe Service mit internen Systemen verbunden ist, sollte klar beschrieben und dokumentiert werden. Dazu gehören Fernzugriffstools, Cloud-basierte SCADA-Plattformen und vom Anbieter verwaltete OT-Systeme.
- **Überprüfen und genehmigen Sie Services vor der Nutzung**
  Externe Services sollten vor ihrer Nutzung überprüft und genehmigt werden. Dieser Prozess sollte verifizieren, dass der Service mit den internen Sicherheits-, Compliance- und Betriebsanforderungen übereinstimmt.
- **Kategorisieren und klassifizieren Sie Services**
  Externe Services sollten nach Typ (z. B. IaaS, SaaS, APIs) kategorisiert und anhand ihrer Kritikalität und Datensensibilität klassifiziert werden. Dies trägt dazu bei, Prioritäten für die Aufsicht und das Risikomanagement zu setzen.
- **Integrieren Sie mit dem Risiko- und Änderungsmanagement**
  Das Inventar sollte in umfassendere Risiko- und Änderungsmanagementprozesse integriert werden. Jede Änderung bei externen Services sollte eine Überprüfung der damit verbundenen Risiken und der erforderlichen Kontrollen auslösen.

ID.AM-04.2 Die Organisation bildet den Informationsfluss zu/von externen Systemen ab, dokumentiert und genehmigt ihn und aktualisiert ihn bei Änderungen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass der Informationsfluss zu und von externen Systemen klar verstanden, sicher verwaltet und auf dem neuesten Stand gehalten wird, um das Risiko von Datenlecks, unbefugtem Zugriff oder Störungen in IKT- und OT-Umgebungen zu verringern.

Um dieses Ziel zu erreichen:

- **Identifizieren Sie Datenpfade und bilden Sie diese ab**
  Alle Pfade, über die Daten in die Systeme des Unternehmens gelangen oder diese verlassen, sollten identifiziert und dokumentiert werden. Dazu gehören Funktionen, Ports, Protokolle und Dienste, die sowohl in IT- als auch in OT-Umgebungen verwendet werden.
- **Dokumentieren Sie Datenflüsse im Detail**
  Die Aufzeichnungen sollten die Arten der übertragenen Daten, die beteiligten Systeme und die angewandten Sicherheitsmaßnahmen (z. B. Verschlüsselung, Authentifizierung, Zugriffskontrollen) beschreiben. Dies unterstützt die Transparenz und den sicheren Umgang mit Daten.
- **Autorisieren und kontrollieren Sie den Zugriff**
  Nur benannte und autorisierte Mitarbeiter sollten Datenübertragungen genehmigen und verwalten dürfen. Dies hilft dabei, unbefugten Zugriff zu verhindern und die Verantwortlichkeit sicherzustellen.
- **Bewerten und aktualisieren Sie regelmäßig**
  Die Dokumentation des Informationsflusses sollte überprüft und aktualisiert werden, wenn sich Systeme, Prozesse oder externe Verbindungen ändern. Dadurch wird sichergestellt, dass die Kontrollen wirksam bleiben und an das aktuelle Umfeld angepasst werden.

Die beiden Kontrollen – ID.AM-03-3 und ID.AM-04.2 – sind eng miteinander verbunden, konzentrieren sich aber auf unterschiedliche Bereiche des Informationsflusses und der Netzwerkaktivität. Diese Kontrolle konzentriert sich auf granulare, inhaltsspezifische Datenflüsse zwischen der Organisation und bestimmten externen Systemen. Sie umfasst:

- Datenübertragungen zu/von Plattformen von Drittanbietern wie CRM-Systemen, Cloud-Speicheranbietern und externen APIs.
- Dateiübertragungen, API-Aufrufe und Datenbanksynchronisation mit externen Systemen.

ID.AM-05 Priorisierung von Vermögenswerten auf der Grundlage von Klassifizierung, Kritikalität, Ressourcen und Auswirkungen auf den Organisationszweck

ID.AM-05.1 Die Vermögenswerte der Organisation werden auf der Grundlage von Klassifizierung, Kritikalität und Geschäftswert nach Prioritäten geordnet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Unternehmensressourcen, wie Geräte, Systeme, Services, Daten und Geschäftsprozesse, auf der Grundlage ihrer Klassifizierung, ihrer Kritikalität und ihres Geschäftswerts priorisiert werden.

Diese Priorisierung hilft, die Schutzbemühungen auf die wichtigsten Ressourcen zu lenken und die Betriebskontinuität, Sicherheit und Compliance zu unterstützen.

Um dies zu ermöglichen, sollten folgende Schritte berücksichtigt werden:

- **Identifizierung von Vermögenswerten**
  Alle relevanten Vermögenswerte, darunter Geräte, Systeme, Software, Cloud-Services, Daten, Mitarbeiter und Geschäftsprozesse, sollten identifiziert und in einem zentralen Inventar erfasst werden.
- **Klassifizierung von Vermögenswerten**
  Jeder Vermögenswert sollte auf der Grundlage seiner Funktion klassifiziert werden:
  - Als primäre Vermögenswerte sollten diejenigen definiert werden, die direkt die Kerngeschäftsfunktionen unterstützen.
  - Sekundäre Werte sollten als solche definiert werden, die primäre Werte unterstützen, schützen oder ermöglichen.
- **Bewertung der Kritikalität**
  - Die Organisation sollte bewerten, wie kritisch die einzelnen Vermögenswerte für die Geschäftskontinuität sind.
  - Die Bewertung sollte potenzielle Auswirkungen wie Betriebsunterbrechungen, finanzielle Verluste, rechtliche oder regulatorische Konsequenzen, Sicherheitsrisiken und Rufschädigung berücksichtigen.
- **Methode der Prioritätensetzung**
  Es sollte ein einheitliches Bewertungs- oder Ranglistenverfahren verwendet werden, um die Vermögenswerte auf der Grundlage von Klassifizierung, Kritikalität und Geschäftswert zu priorisieren.
- **Eigentumszuweisung**
  Jeder Vermögenswert sollte einen Eigentümer haben, der für die Pflege genauer und aktueller Informationen verantwortlich ist.
- **Regelmäßige Überprüfung**
  Die Klassifizierung von Vermögenswerten und ihre Prioritäten sollten mindestens jährlich oder bei wesentlichen Änderungen (z. B. neue Systeme, Umstrukturierung des Unternehmens) überprüft werden.
- **Dokumentation und Beweise**
  - Das Bestandsverzeichnis sollte eine Klassifizierung, Priorisierungskriterien, zugewiesene Eigentümer und Nachweise für regelmäßige Überprüfungen enthalten.
  - Die Definitionen von primären und sekundären Vermögenswerten sollten klar dokumentiert werden.

ID.AM-07 Inventare von Daten und entsprechenden Metadaten für bestimmte Datentypen werden gepflegt

ID.AM-07.1 Daten, die die Organisation speichert und verwendet, werden identifiziert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle von der Organisation gespeicherten und verwendeten Daten eindeutig identifiziert werden. Dies unterstützt die ordnungsgemäße Datenverwaltung, den Schutz und die Anpassung an geschäftliche und gesetzliche Anforderungen.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Identifizierung der Daten**
  Alle Arten von Daten, unabhängig von Format, Speicherort oder System, sollten identifiziert und aufgezeichnet werden.
- **Klassifizierung der Daten**
  Die identifizierten Daten sollten anhand von Standardkategorien klassifiziert werden wie z. B.:
  - Öffentlich
  - Intern
  - Vertraulich
  - Eingeschränkt
- **Daten-zu-Vermögenswert-Zuordnung**
  Daten sollten mit den Vermögenswerten verknüpft werden, die sie speichern oder verarbeiten, einschließlich physischer Geräte, Systeme, Software und Anwendungen, die in den Inventaren von ID.AM-01 und ID.AM-02 aufgeführt sind.
- **Dokumentation und Pflege**
  Datentypen, Klassifizierungen und zugehörige Vermögenswerte sollten dokumentiert und regelmäßig aktualisiert werden, um Änderungen in der Umgebung zu berücksichtigen.

ID.AM-07.2 Inventare von Daten und zugehörigen Metadaten werden für bestimmte Datentypen gepflegt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Bestandsverzeichnisse über Daten und deren zugehörige Metadaten für alle Datentypen geführt werden, die durch Richtlinien oder Vorgaben ausdrücklich ausgewählt oder festgelegt sind (z. B. Kundendaten, Finanzinformationen oder Produktionsdaten). Dies unterstützt ein sicheres Datenmanagement, die Einhaltung regulatorischer Anforderungen sowie die betriebliche Integrität in IKT- und OT-Umgebungen.

Um dieses Ziel zu erreichen:

- **Definieren Sie ein Datenklassifizierungsschema**
  Es sollte ein Klassifizierungsschema erstellt werden, um Datentypen auf der Grundlage von Sensibilität und Verwendung zu kategorisieren. Dieses Schema sollte die Handhabung, den Schutz und die Aufbewahrung von Daten regeln.
- **Wenden Sie Sicherheitsmaßnahmen nach Klassifizierungsstufe an**
  Für jede Klassifizierungsstufe sollten geeignete Sicherheitskontrollen durchgeführt werden. Dazu können Verschlüsselung, rollenbasierte Zugriffskontrollen und maßgeschneiderte Richtlinien zur Datenaufbewahrung gehören.
- **Identifizieren und schützen Sie sensible Datentypen**
  Inventare sollten sensible Daten umfassen, wie zum Beispiel:
  - Persönlich identifizierbare Informationen (PII)
  - Finanz- und Gesundheitsinformationen
  - Vertrauliche Geschäftsdaten
  - Geistiges Eigentum
  - Behörden- und Personalakten

  OT-Umgebungen sollten auch betriebliche Daten enthalten, die für die Sicherheit und Zuverlässigkeit kritisch sind.
- **Verfolgen Sie Metadaten für jede Dateninstanz**
  Metadaten sollten gepflegt werden, um die Datenverwaltung zu unterstützen. Dazu gehören:
  - Beschreibende Metadaten (z. B. Titel, Autor, Schlüsselwörter)
  - Strukturelle Metadaten (z. B. Format, Schema)
  - Administrative Metadaten (z. B. Zugriffsrechte, Aufbewahrungspolitik)
  - Technische Metadaten (z. B. Kodierung, Prüfsumme)
- **Überwachen Sie die Herkunft und den Speicherort von Daten**
  Die Herkunft, Eigentumsverhältnisse und der Standort jeder Dateninstanz sollten dokumentiert werden. Dies hilft zu verstehen, wo und wie Daten gespeichert und verarbeitet werden, insbesondere in verteilten oder OT-Systemen.
- **Ermitteln und analysieren Sie kontinuierlich Ad-hoc-Daten**
  Es sollten Prozesse vorhanden sein, um neue Fälle sensibler Daten zu identifizieren, die in den ursprünglichen Inventaren nicht erfasst wurden. Dies hilft, Lücken in der Datenflusszuordnung zu schließen und unterstützt den laufenden Datenschutz.
- **Erwägen Sie die Verwendung des Ampelprotokolls (Traffic Light Protocol, TLP)**
  TLP sollte als Methode zur Klassifizierung und zum Austausch von cybersicherheitsrelevanten Daten in Betracht gezogen werden, insbesondere bei der Reaktion auf Vorfälle und bei Bedrohungsanalysen.

ID.AM-08 Systeme, Hardware, Software, Services und Daten werden während ihres gesamten Lebenszyklus verwaltet

ID.AM-08.2 Patches und Sicherheitsupdates für Betriebssysteme und kritische Systemkomponenten werden installiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Betriebssysteme und kritische Systemkomponenten sicher und auf dem neuesten Stand gehalten werden, indem Patches und Sicherheitsupdates zeitnah und kontrolliert installiert werden.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Rechtzeitige Updates**
  Patches und Sicherheitsupdates sollten so schnell wie möglich installiert werden, insbesondere bei kritischen Systemen.
- **Industrielle Systeme**
  Firmware-Updates für industrielle Vermögenswerte (z. B. SPS, HMI) sollten in den Patching-Prozess einbezogen werden.
- **Zentralisiertes Management**
  Ein zentralisiertes Patch-Management-System sollte zur Automatisierung und Rationalisierung der Patch-Verteilung eingesetzt werden.
- **Tests vor der Bereitstellung**
  - Patches sollten in einer kontrollierten Umgebung getestet werden, um Unterbrechungen zu vermeiden.
  - Eine Testumgebung sollte weitgehend die Produktionsumgebung widerspiegeln.
- **Schrittweise Einführung**
  - Gegebenenfalls sollten Testgruppen, Pilotanwender und schrittweise Einführungen eingesetzt werden.
  - Für den Fall, dass Probleme auftreten, sollte ein Rollback-Verfahren vorhanden sein.
- **Nur vertrauenswürdige Quellen**
  - Patches sollten nur von verifizierten, vertrauenswürdigen Quellen heruntergeladen werden.
  - Links in E-Mails oder Werbung sollten vermieden werden.
- **Minimaler Software-Footprint**
  Es sollten nur notwendige Anwendungen installiert werden. Diese sollten regelmäßig gepatcht und aktualisiert werden.
- **Sichere Update-Praktiken**
  - Automatische Updates sollten aktiviert werden, wenn eine Verbindung zu vertrauenswürdigen Netzwerken besteht.
  - Updates sollten nicht über nicht vertrauenswürdige Netzwerke (z. B. öffentliches Wi-Fi) durchgeführt werden.
- **Nur unterstützte Software**
  - Es sollten nur vom Hersteller unterstützte und aktuelle Softwareversionen verwendet werden.
  - Auslaufende Software (End-of-life, EOL) sollte so schnell wie möglich außer Betrieb genommen werden.
- **Regelmäßige Überprüfungen**
  Wenn automatische Aktualisierungen nicht möglich sind, sollte ein regelmäßiger Zeitplan (z. B. monatlich) festgelegt werden, um manuell nach Aktualisierungen zu suchen und diese zu installieren.
- **Aktualisierung von Überwachungstools**
  Tools, die über verfügbare Updates informieren, sollten so konfiguriert werden, dass sie alle installierten Anwendungen überwachen.

ID.AM-08.3 **Die Organisation setzt die Rechenschaftspflicht für alle geschäftskritischen Vermögenswerte während des gesamten Systemlebenszyklus durch, einschließlich Entfernung, Übertragung und Entsorgung.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Rechenschaftspflicht für alle geschäftskritischen Vermögenswerte während ihres gesamten Lebenszyklus zu gewährleisten, einschließlich Bereitstellung, Transport und Entsorgung, um das Risiko eines unbefugten Zugriffs, eines Datenlecks oder einer Betriebsunterbrechung in IKT- und OT-Umgebungen zu verringern.

Um dieses Ziel zu erreichen:

- **Sichern Sie Vermögenswerte vor der Bereitstellung**
  Systeme, Hardware, Software und Services sollten ordnungsgemäß konfiguriert und gesichert werden, bevor sie in Produktionsumgebungen eingeführt werden.
- **Identifizieren und entfernen Sie redundante Vermögenswerte**
  Redundante oder ungenutzte Systeme, Software und Services, die die Angriffsfläche vergrößern, sollten regelmäßig identifiziert und entfernt werden.
- **Überwachen und dokumentieren Sie die Bewegungen von Vermögenswerten**
  Die Bewegungen geschäftskritischer Vermögenswerte sollten nachverfolgt und dokumentiert werden, um die Rückverfolgbarkeit und Rechenschaftspflicht sicherzustellen.
- **Autorisieren Sie Transfers von Vermögenswerten**
  Geschäftskritische Vermögenswerte sollten nur mit ordnungsgemäßer Autorisierung in die Einrichtungen gelangen oder diese verlassen dürfen, insbesondere in OT-Umgebungen, in denen die Kontrolle der physischen Vermögenswerte entscheidend ist.
- **Entsorgen Sie Vermögenswerte sicher**
  Die Entsorgung von geschäftskritischen Vermögenswerten sollte auf sichere, verantwortungsvolle und überprüfbare Weise erfolgen, um Datenverluste oder eine unbefugte Wiederverwendung zu verhindern.
- **Aktualisieren Sie Inventare umgehend**
  Inventare von Vermögenswerten sollten aktualisiert werden, wenn Systeme, Hardware, Software oder Services verschoben, übertragen, entfernt oder außer Betrieb genommen werden.

ID.AM-08.4 **Die Organisation stellt sicher, dass die erforderlichen Maßnahmen getroffen werden, um den Verlust, den Missbrauch, die Beschädigung oder den Diebstahl von Vermögenswerten zu verhindern.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass geeignete Maßnahmen ergriffen werden, um den Verlust, den Missbrauch, die Beschädigung oder den Diebstahl von Vermögenswerten zu verhindern und darauf zu reagieren, um den Geschäftsbetrieb zu schützen und Sicherheitsrisiken in IKT- und OT-Umgebungen zu verringern.

Um dieses Ziel zu erreichen:

- **Wenden Sie physische Sicherheitsmaßnahmen an**
  Physische Schutzvorrichtungen wie Schlösser, Überwachungskameras und Alarmanlagen sollten eingesetzt werden, um Einrichtungen und kritische Vermögenswerte, einschließlich solcher in OT-Umgebungen, zu sichern.
- **Implementieren Sie technische Sicherheitsvorkehrungen**
  Technische Kontrollen wie Verschlüsselung, sichere Datenlöschung und regelmäßige Backups sollten angewendet werden, um Daten und Systeme vor unbefugtem Zugriff oder Verlust zu schützen.

- **Richten Sie organisatorische Kontrollen ein**
  Es sollten Richtlinien, Verfahren und Nutzungsvereinbarungen vorhanden sein, um Verantwortlichkeiten und Erwartungen zu definieren. Mobile Device Management (MDM) und andere Verwaltungstools sollten zur Verwaltung der Nutzung von Vermögenswerten eingesetzt werden.
- **Führen Sie regelmäßige Audits und Inventarkontrollen durch**
  Es sollten regelmäßige Audits und Inventarisierungen der Vermögenswerte durchgeführt werden, um sicherzustellen, dass alle Vermögenswerte erfasst und ordnungsgemäß verwaltet werden.
- **Beschränken Sie den Zugang zu sensiblen Vermögenswerten**
  Der Zugang zu kritischen Systemen, Daten und physischen Bereichen sollte ausschließlich autorisierten Mitarbeitern vorbehalten sein, insbesondere in Umgebungen, in denen die Betriebskontinuität von entscheidender Bedeutung ist.
- **Bieten Sie Mitarbeitern Schulungen und Sensibilisierungsmaßnahmen**
  Mitarbeiter sollten in Bezug auf Maßnahmen zum Schutz von Vermögenswerten geschult und dazu ermutigt werden, verdächtige Aktivitäten oder Vorfälle im Zusammenhang mit Missbrauch oder Verlust von Vermögenswerten zu melden.
- **Halten Sie einen angemessenen Versicherungsschutz aufrecht**
  Es sollten Versicherungspolicen vorhanden sein, um finanzielle Verluste aufgrund von Diebstahl, Beschädigung oder anderen Vorfällen zu mindern.

ID.AM-08.5 Die Organisation muss sicherstellen, dass Entsorgungsmaßnahmen genehmigt, nachverfolgt, dokumentiert und überprüft werden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Entsorgungsmaßnahmen, die Informationssysteme, Daten oder physische Vermögenswerte betreffen, ordnungsgemäß autorisiert, nachvollziehbar und verifizierbar sind, um Risiken zu verringern, die Einhaltung von Vorschriften zu gewährleisten und sensible Informationen zu schützen, insbesondere in operativen Technologieumgebungen (OT).

Um dieses Ziel zu erreichen, sollten folgende Schritte berücksichtigt werden:

- **Genehmigung**: Entsorgungsmaßnahmen sollten vor ihrer Durchführung von autorisierten Mitarbeitern überprüft und genehmigt werden. Dies gewährleistet die Übereinstimmung mit internen Richtlinien und externen Vorschriften.
- **Nachverfolgung**: Jede Entsorgungsmaßnahme sollte mit den wichtigsten Details protokolliert werden, einschließlich der Art des Vermögenswertes oder Mediums, der Entsorgungsmethode, des Datums und der beteiligten Personen.
- **Dokumentation**: Alle Schritte, von der Genehmigung bis zur Überprüfung, sollten klar dokumentiert werden. Dazu gehören Genehmigungsaufzeichnungen, Verfolgungsprotokolle und sonstige Belege.
- **Verifizierung**: Die Entsorgung sollte verifiziert werden, um sicherzustellen, dass sie korrekt durchgeführt wurde. Dies kann die Überprüfung umfassen, ob die Daten sicher gelöscht wurden oder ob die physische Vernichtung effektiv war.

Dieser strukturierte Ansatz trägt zur Wahrung der Verantwortlichkeit und Sicherheit bei, insbesondere in OT-Umgebungen, in denen eine unsachgemäße Entsorgung zu Betriebsunterbrechungen oder Sicherheitsrisiken führen kann.

ID.AM-08.6 **Die Organisation plant vorbeugende Wartungs- und Reparaturarbeiten an ihren kritischen Systemkomponenten gemäß genehmigten Prozessen und Tools, führt diese durch und dokumentiert sie.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass vorbeugende Wartung und Reparaturen an kritischen Systemkomponenten auf sichere und konsistente Weise geplant, durchgeführt und dokumentiert werden, um die Systemzuverlässigkeit aufrechtzuerhalten und Betriebsrisiken in IKT- und OT-Umgebungen zu verringern.

Um dieses Ziel zu erreichen:

- **Dokumentieren Sie Wartungsverfahren**
  Wartungsrichtlinien und -verfahren sollten klar definiert und in die Cybersicherheits- und Betriebspläne der Organisation aufgenommen werden. Die Aufsicht über diese Verfahren sollte Teil der Managementverantwortung sein.
- **Autorisieren Sie Wartungspersonal**
  Es sollte ein Verfahren zur Autorisierung von Einzelpersonen oder externen Dienstleistern, die Wartungsarbeiten durchführen, eingerichtet werden. Es sollte eine Liste der zugelassenen Personen oder Organisationen geführt und regelmäßig überprüft werden.
- **Planen und dokumentieren Sie Wartungsaktivitäten**
  Vorbeugende Wartungs- und Reparaturarbeiten sollten gemäß den organisatorischen Anforderungen und den Spezifikationen des Herstellers geplant, durchgeführt und dokumentiert werden. Die Aufzeichnungen sollten auf Vollständigkeit und Richtigkeit überprüft werden.
- **Überwachen Sie alle Wartungsaktivitäten**
  Alle Wartungsarbeiten, unabhängig davon, ob sie vor Ort oder aus der Ferne durchgeführt werden, sollten im Voraus genehmigt und während der Ausführung überwacht werden. Dazu gehört auch die Wartung der aus der Anlage entfernten Komponenten.
- **Gewährleisten Sie eine sichere und zuverlässige Wartung der OT-Systeme**
  Die Wartung von OT-Systemen sollte so geplant und durchgeführt werden, dass der Betrieb sicher bleibt, unnötige Ausfallzeiten vermieden werden und alle spezifischen Anweisungen oder Anforderungen der Gerätehersteller befolgt werden.

ID.AM-08.7 **Die Organisation soll die nicht autorisierte Entfernung von Wartungsgeräten, die kritische Systeminformationen der Organisation enthalten, verhindern.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die nicht autorisierte Entfernung von Wartungsgeräten zu verhindern, die kritische Systeminformationen enthalten können, und so das Risiko von Datenlecks oder -diebstahl zu verringern, insbesondere in Umgebungen der Betriebstechnologie (OT).

Um dieses Ziel zu erreichen, sollten die folgenden Maßnahmen ergriffen werden:

- **Verifizierung**: Wartungsgeräte sollten überprüft werden, um sicherzustellen, dass sie keine organisatorischen Informationen enthalten, bevor sie entfernt werden
- **Bereinigung oder Vernichtung**: Bei Vorhandensein sensibler Daten sollten die Geräte gemäß den genehmigten Verfahren bereinigt oder sicher vernichtet werden.
- **Verbleib innerhalb der Einrichtung**: Die Geräte sollten innerhalb der Einrichtung verbleiben, es sei denn, eine Entfernung ist unbedingt erforderlich.
- **Einholung einer Ausnahmegenehmigung**: Wenn eine Entfernung erforderlich ist, sollte eine ausdrückliche Genehmigung von dafür zuständigen Mitarbeitern oder Stellen eingeholt werden.

Wartungsausrüstung bezieht sich in diesem Zusammenhang auf Hardware, die vorübergehend für Wartungs- oder Diagnosezwecke verwendet wird, wie z. B. externe Laufwerke, temporäre Server oder spezielle OT/ICS-Tools, nicht jedoch auf reguläre Wartungswerktools, die unter die Kontrolle ID.AM-08.9 fallen.

ID.AM-08.8 Die Organisation soll Wartungstools für den Einsatz auf ihren kritischen Systemen vorab genehmigen, überwachen und durchsetzen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die für kritische Systeme verwendeten Wartungstools vorab genehmigt, überwacht und durchgesetzt werden, um die Systemintegrität, Sicherheit und Betriebskontinuität zu schützen. In OT-Umgebungen kann die unsachgemäße Verwendung von Tools physische Prozesse beeinträchtigen, so dass die Kontrolle der Toolzulassung und -verwendung für die Betriebssicherheit und Zuverlässigkeit unerlässlich ist.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Kritische Systeme identifizieren**: Systeme, die sich auf die Sicherheit, die Qualität, die Einhaltung von Vorschriften oder den betrieblichen Durchsatz auswirken, sollten als kritisch eingestuft werden. Metriken wie Mean Time to Repair (MTTR) und Mean Time Between Failures (MTBF) sollten diese Klassifizierung unterstützen.
- **Tools vorab genehmigen**: Nur geprüfte und genehmigte Wartungstools sollten für kritische Systeme zugelassen werden. Dazu gehören sowohl Hardware- als auch Software-Tools wie Diagnosegeräte, Packet-Sniffer und Laptops.
- **Die Nutzung überwachen**: Die Nutzung von Wartungstools auf kritischen Systemen sollte aktiv überwacht werden, um unbefugte oder unsichere Aktivitäten zu erkennen.
- **Kontrollen durchsetzen**: Es sollten Richtlinien und technische Kontrollen vorhanden sein, um die Verwendung nicht zugelassener Tools zu verhindern und die Einhaltung interner Verfahren sowie der geltenden Gesetze und Vorschriften zu gewährleisten.

ID.AM-08.9 Wartungstools und tragbare Speichergeräte werden bei ihrer Einbringung in die Einrichtung überprüft und durch Anti-Malware-Lösungen geschützt, die sie vor ihrer Verwendung in den Systemen der Organisation auf schädlichen Code scannen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Einschleusung von schädlichem Code in die Organisationssysteme zu verhindern, indem sichergestellt wird, dass alle Wartungstools und tragbaren Speichermedien vor der Verwendung überprüft und gescannt werden. In OT-Umgebungen kann die Einführung nicht verifizierter Tools oder Speichergeräte die Systemintegrität gefährden und kritische physische Abläufe stören.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Bei Einführung kontrollieren**: Wartungstools und tragbare Speichergeräte sollten bei Einführung in die Einrichtung kontrolliert werden, um unbefugte oder verdächtige Gegenstände zu erkennen.
- **Nach Malware scannen**: Alle Geräte sollten mit aktuellen Anti-Malware-Lösungen gescannt werden, bevor sie mit den Systemen der Organisation verbunden werden.
- **Dies gilt für alle Tooltypen**: Dazu gehören Software-Tools (z. B. Diagnosesoftware, Firmware-Updater, Konfigurationstools, Fernzugriffstools), tragbare Speicher (z. B. USB-Laufwerke, externe Festplatten, SD-Karten) und Hardware-Tools (z. B. Laptops, Tablets, tragbare Diagnosegeräte).
- **Zerstörungsfreie Bereinigung verwenden**: Bei neu erworbenen Geräten oder Geräten ohne vertrauenswürdige Kontrollkette sollten vor der ersten Verwendung zerstörungsfreie Bereinigungstechniken angewendet werden.
- **Konformität und Compliance sicherstellen**: Alle Maßnahmen sollten den internen Verfahren entsprechen und die geltenden Cybersicherheitsvorschriften und Branchenstandardseinhalten.

ID.AM-08.10 Die Organisation verifiziert die Sicherheitskontrollen nach Wartungs- oder Reparaturarbeiten/Patches und ergreift gegebenenfalls entsprechende Maßnahmen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Sicherheitskontrollen auch nach Wartungs-, Reparatur- oder Patching-Aktivitäten wirksam bleiben. In OT-Umgebungen können selbst kleine Konfigurationsänderungen erhebliche Auswirkungen auf die Sicherheit oder den Betrieb haben, so dass eine Verifizierung nach der Wartung von entscheidender Bedeutung ist.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Sicherheitskontrollen verifizieren**: Nach der Wartung sollten die Systeme überprüft werden, um sicherzustellen, dass keine Änderungen die Sicherheit beeinträchtigt haben. Dazu gehört die Überprüfung von Konfigurationen, Zugriffsberechtigungen und anderen sicherheitsrelevanten Einstellungen.
- **Aufzeichnungen aktualisieren**: Alle während der Wartung vorgenommenen Änderungen sollten dokumentiert werden, einschließlich der Aktualisierung von Sicherheitskontrollen oder der Einführung neuer Maßnahmen.
- **Probleme melden**: Wenn während der Verifizierung Sicherheitsbedenken festgestellt werden, sollten die Ergebnisse den relevanten Stakeholdern mitgeteilt werden, um eine Sensibilisierung und koordinierte Reaktion zu gewährleisten.
- **Korrekturmaßnahmen ergreifen**: Wenn sich die Kontrollen als unzureichend oder gefährdet erweisen, sollten Korrekturmaßnahmen ergriffen werden. Dazu kann die Neukonfiguration von Einstellungen, die Anwendung zusätzlicher Patches oder die Verstärkung bestehender Kontrollen gehören.
- **Konformität und Compliance sicherstellen**: Alle Verifizierungs- und Korrekturmaßnahmen sollten den internen Verfahren entsprechen und die geltenden Gesetzen, Vorschriften und Branchenstandards einhalten.

ID.AM-08.11 Fernwartungs- und Diagnoseaktivitäten an Vermögenswerten der Organisation werden vorab genehmigt und die Durchführung protokolliert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Fernwartungs- und Diagnosetätigkeiten autorisiert, nachvollziehbar und sicher sind. In OT-Umgebungen muss die Fernwartung streng kontrolliert werden, da sich unbefugte Änderungen direkt auf die Sicherheit und Stabilität der physischen Systeme auswirken können.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Aktivitäten vorab genehmigen**: Alle Fernwartungs- und Diagnosetätigkeiten sollten vor ihrer Durchführung überprüft und genehmigt werden.
- **Leistung protokollieren**: Jede Fernsitzung sollte detailliert protokolliert werden, einschließlich Zeit, Dauer, beteiligte Personen und durchgeführte Maßnahmen.
- **Protokollierungsverfahren festlegen**: Protokollierungs- und Überwachungsverfahren sollten dokumentiert, genehmigt, kommuniziert, angewandt und regelmäßig, idealerweise jährlich, überprüft werden.
- **Unbefugte Änderungen verhindern**: Es sollten technische und verfahrenstechnische Maßnahmen getroffen werden, um unbefugte Änderungen an Systemen, Konfigurationen, Anwendungen oder der Infrastruktur während des Fernzugriffs zu erkennen oder zu verhindern.
- **Konformität und Compliance sicherstellen**: Alle Aktivitäten sollten den internen Richtlinien entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

ID.AM-08.12 **Die Einrichtung von nicht lokalen Wartungs- und Diagnosesitzungen über Remote-Netzwerkverbindungen erfordert starke Authentifizierungsverfahren, und derartige Verbindungen werden beendet, sobald die nicht lokale Wartung abgeschlossen ist.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass nicht-lokale Wartungs- und Diagnosesitzungen sicher eingerichtet und ordnungsgemäß beendet werden, um unbefugten Zugriff oder verbleibende Verbindungen zu verhindern. In OT-Umgebungen sind ein sicherer Sitzungsaufbau und -abbau unerlässlich, um dauerhafte Zugriffspfade zu verhindern, die zur Störung des physischen Betriebs ausgenutzt werden könnten.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Eine starke Authentifizierung verwenden**: Fernsitzungen sollten durch starke Authentifikatoren geschützt werden, die Wiederholungsangriffen widerstehen. Wo immer möglich, sollte eine Multi-Faktor-Authentifizierung verwendet werden.
- **Kommunikationen schützen**: Es sollten kryptografische Mechanismen implementiert werden, um die Vertraulichkeit und Integrität der Fernwartungskommunikationen zu gewährleisten.
- **Sitzungen beenden**: Fernverbindungen sollten sofort nach Abschluss der Wartungsarbeiten beendet werden, um potenzielle Bedrohungen zu vermeiden.
- **Die Verbindungstrennung verifizieren**: Eine Verifizierung der Beendigung der Fernverbindung sollte verwendet werden, um zu bestätigen, dass die Sitzungen vollständig geschlossen wurden und nicht mehr zugänglich sind.
- **Konformität und Compliance sicherstellen**: Alle Fernzugriffsaktivitäten sollten den internen Sicherheitsverfahren entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

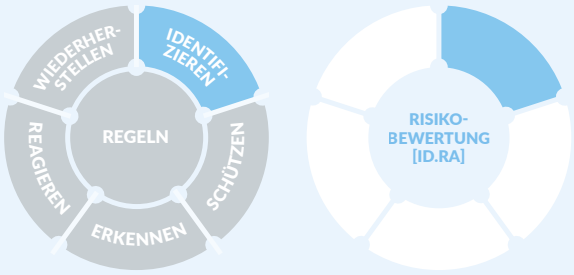
ID.AM-08.13 **Die Organisation verlangt, dass Fernwartungsdiagnosedienste von einem System aus durchgeführt werden, das ähnliche Sicherheitsmerkmale aufweist wie das entsprechende kritische System der Organisation.**

Implementierungshinweise

Mit dieser Kontrolle soll sichergestellt werden, dass Fernwartungs- und Diagnosedienste von Systemen aus durchgeführt werden, die über Sicherheitsmerkmale verfügen, die denen der kritischen Systeme der Organisation entsprechen. In OT-Umgebungen (Operational Technology) ist diese Abstimmung unerlässlich, um eine konsistente Sicherheitslage aufrechtzuerhalten, die Einführung von Schwachstellen zu verhindern und die Sicherheit, Zuverlässigkeit und Kontinuität des physischen Betriebs zu schützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Starke Authentifizierung verwenden**: Remote-Systeme sollten eine Multi-Faktor-Authentifizierung implementieren, um sicherzustellen, dass der Zugriff auf autorisierte Mitarbeiter beschränkt ist.
- **Aktivitätsprotokolle führen**: Detaillierte Protokolle aller Fernwartungsaktivitäten sollten geführt und regelmäßig überprüft werden, um Anomalien oder unbefugte Handlungen zu erkennen.
- **Tools und Verfahren aufeinander abstimmen**: Alle bei der Fernwartung eingesetzten Tools und Verfahren sollten mit den Organisationsrichtlinien übereinstimmen und in den entsprechenden Plänen für Cybersicherheit oder Informationssicherheit dokumentiert sein.
- **Sitzungen beenden**: Remote-Sitzungen sollten nach Abschluss der Wartungsarbeiten ordnungsgemäß beendet werden, um einen fortdauernden Zugriff zu verhindern.
- **Konformität und Compliance sicherstellen**: Remote-Systeme und -Aktivitäten sollten den internen Sicherheitsanforderungen entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.



Die Organisation kennt das Cybersicherheitsrisiko für die Organisation, Vermögenswerte und Personen

ID.RA-01 Schwachstellen in Anlagen werden identifiziert, validiert und dokumentiert

ID.RA-01.1 Bedrohungen und Schwachstellen werden in allen relevanten Anlagen, einschließlich Software, Netz- und Systemarchitekturen und Einrichtungen, die kritische Datenverarbeitungsanlagen beherbergen, identifiziert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, Organisationen bei der Minderung von Cybersicherheitsrisiken zu helfen, indem sie Bedrohungen und Schwachstellen in ihren kritischen Anlagen identifizieren. Dazu gehören Software, Netzwerke, Systeme und physische Standorte, die den wesentlichen Computerbetrieb unterstützen.

Um dieses Ziel zu unterstützen, sollten Organisationen:

- **Die Schlüsselkonzepte verstehen**
  - Eine **Sicherheitslücke** ist eine Schwachstelle in Hardware, Software oder Verfahren, die ausgenutzt werden kann.
  - Eine **Bedrohung** ist ein Ereignis oder ein Akteur, der versuchen könnte, eine Schwachstelle auszunutzen.
  - Ein **Risiko** ist die mögliche Auswirkung, wenn eine Bedrohung eine Sicherheitslücke erfolgreich ausnutzt.
- **Relevante Vermögenswerte identifizieren**
  Alle kritischen Systeme, Anwendungen, Netzwerke und Einrichtungen sollten aufgelistet und dokumentiert werden.
- **Auf Schwachstellen reagieren**
  - Organisationen sollten auf Schwachstellen reagieren, die von vertrauenswürdigen Quellen gemeldet werden (z. B. von Anbietern, Dienstleistern und Behörden).
  - Auf der Basisebene ist ein aktives Scannen ist nicht erforderlich, aber bekannte Schwachstellen sollten umgehend behoben werden.
- **Sich der Bedrohungen bewusst sein**
  Organisationen sollten sich über gängige, für ihren Sektor relevante Bedrohungen informieren (z. B. Phishing, Ransomware).

ID.RA-01.2 Es wird ein Prozess eingerichtet, um Schwachstellen der geschäftskritischen Systeme der Organisation kontinuierlich zu überwachen, zu identifizieren und zu dokumentieren.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Schwachstellen in geschäftskritischen Systemen kontinuierlich identifiziert, überwacht und dokumentiert werden, um eine rechtzeitige Risikominderung zu unterstützen und die betriebliche Resilienz aufrechtzuerhalten.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Schwachstellenscans einsetzen, wo dies sicher ist**
  Schwachstellenscans sollten auf IT- und OT-Systeme angewendet werden, wenn dies den Betrieb nicht stört und die Sicherheit nicht beeinträchtigt. In OT-Umgebungen sollten passive oder nicht-intrusive Methoden bevorzugt werden.
- **Tools für das Schwachstellenmanagement einsetzen**
  Tools sollten eingesetzt werden, um nicht gepatchte Software, Fehlkonfigurationen und veraltete Firmware sowohl in IT- als auch in OT-Vermögenswerten zu erkennen.
- **Architekturen auf Schwachstellen überprüfen**
  Netzwerk- und Systemarchitekturen, einschließlich Segmentierung, Fernzugriffspfade und ältere Komponenten, sollten auf Konstruktionsfehler überprüft werden, die OT-Systeme Cyber-Bedrohungen aussetzen könnten.
- **Quellen für Bedrohungsdaten überwachen**
  Öffentliche und private Quellen für Cyber-Bedrohungsdaten sollten auf Schwachstellen überwacht werden, die OT-Produkte, industrielle Kontrollsysteme (ICS) und herstellerspezifische Technologien betreffen.
- **Unternehmenseigene Software überprüfen**
  Personalisierte Anwendungen, einschließlich solcher, die in OT-Umgebungen verwendet werden (z. B. HMIs, SPS-Logik), sollten auf unsichere Codierungspraktiken und Standardkonfigurationen analysiert und getestet werden.
- **Betriebsverfahren bewerten**
  Prozesse und Verfahren, insbesondere solche, die Fernzugriff, Wartung und Notfallmaßnahmen betreffen, sollten auf ausnutzbare Schwachstellen überprüft werden, die die Integrität des OT-Systems beeinträchtigen könnten.

ID.RA-01.3 Die Organisation richtet einen dokumentierten Prozess ein , der eine kontinuierliche Überprüfung, Analyse und Behebung von Schwachstellen ermöglicht und gegebenenfalls den Informationsaustausch vorsieht, und behält diesen bei.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Schwachstellen kontinuierlich überprüft, analysiert und durch einen dokumentierten Prozess behoben werden, der gegebenenfalls auch den Informationsaustausch unterstützt.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Gewonnene Erkenntnisse und neue Bedrohungen einbeziehen**
  Der Prozess sollte auf der Grundlage von Vorfällen, technologischen Veränderungen und sich entwickelnden Bedrohungen, einschließlich solcher, die auf OT-Systeme und industrielle Protokolle abzielen, aktualisiert werden.
- **Interne Rückmeldungen und Metriken nutzen**
  Auditergebnisse, Leistungsindikatoren und Rückmeldungen von Bedienern sollten zur Optimierung des Schwachstellenmanagementprozesses genutzt werden, insbesondere wenn manuelle Prozesse üblich sind.
- **Software-Stücklisten (Software Bills of Materials, SBOMs) nutzen**
  SBOMs sollten verwendet werden, um anfällige Komponenten in IT- und OT-Software-Stacks, einschließlich eingebetteter Systeme und Firmware, zu identifizieren.
- **Quellen für Bedrohungsinformationen überwachen**
  Zuverlässige Quellen wie Herstellerhinweise, ICS-CERT und ENISA sollten hinsichtlich Schwachstellen überwacht werden, die OT-Produkte, Steuerungssysteme und Feldgeräte betreffen.
- **Prozesse und Verfahren überprüfen**
  Betriebsabläufe, insbesondere solche, die Fernzugriff, Wartung und sicherheitskritische Funktionen umfassen, sollten auf ausnutzbare Schwachstellen überprüft werden.
- **Mit Technik und Geschäftstätigkeit abstimmen**
  Behebungsmaßnahmen sollten in Abstimmung mit den OT- und Technikteams geplant werden, um ungeplante Ausfallzeiten oder Sicherheitsrisiken zu vermeiden.

ID.RA-01.4 Um sicherzustellen, dass der Betrieb der Organisation durch den Testprozess nicht beeinträchtigt wird, werden Leistungs-/Lasttests und Penetrationstests an den Systemen der Organisation mit Sorgfalt durchgeführt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Leistungs-/Lasttests und Penetrationstests sorgfältig durchgeführt werden, um eine Unterbrechung des Betriebs oder eine Gefährdung der Systemstabilität zu vermeiden, insbesondere in Umgebungen mit geschäfts- oder sicherheitskritischen Systemen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Testprogrammen erstellen und aufrechterhalten**
  Testprogramme für Leistungs-/Lasttests und Penetrationstests sollten auf die Größe, Komplexität und den Reifegrad der Organisation zugeschnitten sein, einschließlich OT-spezifischer Einschränkungen.
- **Kontrollierte Testumgebungen verwenden**
  Penetrationstests sollten nach Möglichkeit in isolierten oder kontrollierten Umgebungen durchgeführt werden, um unbeabsichtigte Auswirkungen auf aktive OT-Systeme zu vermeiden.
- **Qualifizierte ethische Hacker beauftragen**
  Erfahrene ethische Hacker sollten mit der Durchführung von Penetrationstests beauftragt werden, insbesondere in komplexen oder sensiblen OT-Umgebungen.
- **Sicherheitsmaßnahmen nach dem Test validieren**
  Nach dem Test sollten die Sicherheitskontrollen erneut validiert werden, um sicherzustellen, dass die Abwehrmaßnahmen weiterhin wirksam sind und keine unbeabsichtigten Änderungen vorgenommen wurden.

Abgrenzung zu ID.RA-01.5

Während sich ID.RA-01.4 auf Testaktivitäten wie Penetrations- und Lasttests konzentriert, die typischerweise geplant, selten und oft in kontrollierten Umgebungen durchgeführt werden, befasst sich ID.RA-01.5 mit der sicheren Durchführung von Schwachstellen-Scans, die häufiger und oft automatisiert durchgeführt werden und sorgfältig gemanagt werden müssen, um unbeabsichtigte Unterbrechungen in laufenden OT-Systemen zu vermeiden.

ID.RA-01.5 Das Scannen auf Schwachstellen beeinträchtigt die Systemfunktionen nicht.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Schwachstellenscans die Leistung geschäftskritischer Systeme nicht beeinträchtigen oder stören, insbesondere in Operational-Technology-Umgebungen (OT), in denen Systemstabilität und -verfügbarkeit kritisch sind.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Scans in Zeiten geringer Auslastung einplanen**
  Scans sollten in Zeiten geringer Auslastung oder in geplanten Wartungsfenstern durchgeführt werden, um die Auswirkungen auf den Betrieb zu minimieren.
- **Nicht-invasive Scanning-Tools verwenden**
  Tools sollten nach ihrer Fähigkeit ausgewählt werden, zu scannen, ohne die Systemressourcen zu überlasten oder den Echtzeitbetrieb zu stören.
- **Zuerst in Staging-Umgebungen testen**
  Die ersten Scans sollten in Nicht-Produktionsumgebungen getestet werden, um mögliche Probleme vor dem Einsatz in Live-Systemen zu erkennen.

- **Inkrementelles Scannen anwenden**
  Das Scannen sollte in kleinere, überschaubare Segmente unterteilt werden, um die Systemlast zu reduzieren und eine Überlastung kritischer Komponenten zu vermeiden.
- **Die Systemleistung während des Scans überwachen**
  Das Systemverhalten sollte während des Scans aktiv überwacht werden, um Leistungseinbußen oder Anomalien zu erkennen und darauf zu reagieren.

Abgrenzung zu ID.RA-01.4

Während sich ID.RA-01.4 auf Testaktivitäten wie Penetrations- und Lasttests konzentriert, die typischerweise geplant, selten und oft in kontrollierten Umgebungen durchgeführt werden, befasst sich ID.RA-01.5 mit der sicheren Durchführung von Schwachstellen-Scans, die häufiger und oft automatisiert durchgeführt werden und sorgfältig gemanagt werden müssen, um unbeabsichtigte Unterbrechungen in laufenden OT-Systemen zu vermeiden.

ID.RA-01.6 Schwachstellen werden in allen relevanten Vermögenswerten, einschließlich Software, Netz- und Systemarchitekturen und Einrichtungen, identifiziert und verwaltet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Schwachstellen systematisch identifiziert und in allen relevanten Bereichen verwaltet werden, einschließlich Software, Netz- und Systemarchitekturen und physischer Einrichtungen. Dies baut auf der Kontrolle ID.RA-01.1 auf, die sich auf die Ermittlung von Bedrohungen und Schwachstellen konzentriert, um die Risikominderung zu unterstützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Den Anwendungsbereich des Schwachstellenmanagements erweitern**
  Schwachstellenerkennung und -beseitigung sollten alle relevanten Vermögenswerte umfassen, einschließlich IT- und OT-Systeme, Anwendungen, Netzwerkdesigns und Einrichtungen, die kritische Abläufe unterstützen.
- **Einen dedizierten Prozess zum Schwachstellenmanagement pflegen**
  Ein strukturierter Prozess sollte vorhanden sein, um Schwachstellen kontinuierlich zu verfolgen, zu bewerten und zu mindern, unabhängig von Aktivitäten zur Bedrohungserkennung.
- **Zwischen Bedrohungsanalyse und Schwachstellenmanagement unterscheiden**
  Es sollten getrennte Prozesse oder Nachweise geführt werden, um zwischen der Identifizierung externer Bedrohungen (z. B. Bedrohungsakteure, Kampagnen) und dem Management interner Schwachstellen (z. B. ungepatchte Systeme, Fehlkonfigurationen) zu unterscheiden.
- **Mit dem allgemeinen Risikomanagement integrieren**
  Der Prozess des Schwachstellenmanagements sollte sich in das allgemeine Risikomanagement der Organisation einfügen und eine rechtzeitige Entscheidungsfindung unterstützen.
- **OT-spezifische Überlegungen sicherstellen**
  In OT-Umgebungen sollte das Schwachstellenmanagement Altsysteme, Herstellerabhängigkeiten und betriebliche Einschränkungen berücksichtigen, die die Patching- oder Scan-Optionen einschränken können.

ID.RA-02 Cyberbedrohungsinformationen werden von Foren und Quellen für den Informationsaustausch erhalten

ID.RA-02.1 Ein Programm zur Sensibilisierung für Bedrohungen und Schwachstellen, das eine Fähigkeit zum organisationsübergreifenden Informationsaustausch beinhaltet, wird implementiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Fähigkeit der Organisation zu stärken, Cyber-Bedrohungen zu antizipieren und auf sie zu reagieren, indem ein Programm zur Sensibilisierung für Bedrohungen und Schwachstellen eingeführt wird, das einen organisationsübergreifenden Informationsaustausch beinhaltet.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Taktiken von Bedrohungsakteuren und das Aufkommen von Schwachstellen überwachen**
  Cyber-Bedrohungsdaten sollten aktuelle Informationen über Bedrohungsakteure, ihre Taktiken, Techniken und Verfahren (TTPs) sowie über Schwachstellen in neuen Technologien (z. B. KI-gestützte Angriffe, Data Poisoning beim maschinellen Lernen) enthalten.
- **Eine kontinuierliche externe Zusammenarbeit aufbauen**
  Die Organisation sollte sich aktiv an Sicherheitsgruppen, Foren und Fachverbänden beteiligen, um Warnmeldungen, Hinweise und Erkenntnisse von Kollegen zu erhalten, die sowohl für IT- als auch für OT-Umgebungen relevant sind.
- **Informationsaustausch ermöglichen**
  Das Programm sollte den Austausch von nicht klassifizierten und gegebenenfalls klassifizierten Informationen über Schwachstellen und Vorfälle zwischen den Abteilungen und mit vertrauenswürdigen externen Partnern unterstützen.
- **OT-spezifische Sensibilisierung unterstützen**
  Bedrohungsinformationen sollten OT-spezifische Quellen (z. B. ICS-CERT, Herstellerhinweise) einbeziehen, um Schwachstellen in industriellen Kontrollsystemen, älteren Geräten und sektorspezifischen Technologien zu erkennen.
- **Zwischen Bedrohungsinformationen und Schwachstellenmanagement unterscheiden**
  Das Sensibilisierungsprogramm sollte die Schwachstellenmanagementprozesse ergänzen, sich jedoch von diesen unterscheiden, indem es sich auf externe Bedrohungsentwicklungen und strategische Erkenntnisse konzentriert.

ID.RA-02.2 Automatisierte Mechanismen werden implementiert, um Sicherheitswarnungen und -hinweise an relevante Stakeholder der Organisation weiterzuleiten.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Sicherheitswarnungen und -hinweise durch automatisierte Mechanismen umgehend und zuverlässig an die relevanten Stakeholder weitergeleitet werden, um eine rechtzeitige Wahrnehmung und Reaktion in der gesamten Organisation zu ermöglichen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Zentralisierte Sicherheitsplattformen implementieren**
  Lösungen wie SIEM (Security Information and Event Management), XDR (Extended Detection and Response), SOAR (Security Orchestration, Automation, and Response) oder UEBA (User and Entity Behaviour Analytics) sollten eingesetzt werden, um Warnmeldungen aus verschiedenen Quellen, einschließlich OT- und IT-Systemen, zu sammeln, zu analysieren und zu korrelieren.

- **Die Alarmverteilung automatisieren**
  Alarme sollten so konfiguriert werden, dass Stakeholder automatisch per E-Mail, über Messaging-Plattformen oder andere Kanäle benachrichtigt werden, um eine schnelle Verbreitung wichtiger Informationen zu gewährleisten.
- **Echtzeit-Dashboards einsetzen**
  Dashboards sollten implementiert werden, um einen kontinuierlichen Überblick über Sicherheitswarnungen und -hinweise zu bieten und so die Lageerkennung und Entscheidungsfindung zu unterstützen.
- **Mit Plattformen für die Reaktion auf Vorfälle integrieren**
  Automatisierte Mechanismen sollten die Verteilung von Warnmeldungen an Teams für die Reaktion auf Vorfälle unterstützen, um sicherzustellen, dass diese über die neuesten Informationen verfügen, um effektiv handeln zu können.
- **Externe Quellen für Bedrohungsdaten nutzen**
  Automatisierte Tools sollten Daten aus vertrauenswürdigen externen Quellen abrufen, um interne Warnmeldungen mit einem breiteren Bedrohungskontext, einschließlich OT-spezifischer Hinweise, anzureichern.

ID.RA-03 Interne und externe Bedrohungen für die Organisation sind identifiziert und erfasst

ID.RA-03.1 Bedrohungen werden in Bezug auf alle relevanten Vermögenswerten, einschließlich Software, Netz- und Systemarchitekturen und Einrichtungen, identifiziert und bewertet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Bedrohungen systematisch identifiziert und in Bezug auf alle relevanten Vermögenswerte bewertet werden, einschließlich Software, Netz- und Systemarchitekturen und physischer Einrichtungen. Dies baut auf ID.RA-01.1 auf, das die Grundlage für die Identifizierung von Bedrohungen und Schwachstellen bei kritischen Vermögenswerten bildet.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Identifizierung von Bedrohungen auf alle Vermögenswerte ausweiten**
  Bedrohungen sollten in Bezug auf alle relevanten Vermögenswerte bewertet werden, einschließlich IT- und OT-Systemen, Anwendungen, Netzwerkdesigns und physischen Einrichtungen, die kritische Vorgänge unterstützen.
- **Einen dedizierten Prozess zur Erfassung von Bedrohungsinformationen aufrechterhalten**
  Es sollte ein strukturierter Prozess vorhanden sein, um Bedrohungsinformationen aus internen und externen Quellen zu sammeln, zu analysieren und zu bewerten, einschließlich branchenspezifischer Hinweise und OT-fokussierter Bedrohungsfeeds.
- **Bedrohungsinformationen vom Schwachstellenmanagement trennen**
  Bedrohungsinformationen sollten getrennt vom Schwachstellenmanagement verwaltet werden, mit unterschiedlichen Prozessen und Nachweisen, um Klarheit und Fokus zu gewährleisten. Bedrohungen beziehen sich auf potenzielle Akteure oder Ereignisse, während Schwachstellen auf Schwächen hinweisen, die ausgenutzt werden könnten.
- **Mit der Risikoanalyse integrieren**
  Identifizierte Bedrohungen sollten mit bekannten Schwachstellen verknüpft und in einem zentralen Risikoregister erfasst werden, um die Priorisierung und die Planung von Abhilfemaßnahmen zu unterstützen, wie in ID.RA-01.1 beschrieben.
- **OT-spezifische Bedrohungen einbeziehen**
  Bedrohungsbewertungen sollten OT-spezifische Risiken wie die Gefährdung der Lieferkette, unbefugten Fernzugriff und die Ausnutzung von Altsystemen oder proprietären Protokollen berücksichtigen.

ID.RA-05 Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen werden genutzt, um das inhärente Risiko zu verstehen und eine Priorisierung der Risikobewältigung vorzunehmen

ID.RA-05.1 Die Organisation führt Risikobewertungen durch, bei denen das Risiko durch Bedrohungen, Schwachstellen und die Auswirkungen auf Geschäftsprozesse und Vermögenswerte bestimmt wird.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Risikobewertungen durchgeführt werden, indem Bedrohungen, Schwachstellen und ihre potenziellen Auswirkungen auf Geschäftsprozesse und Vermögenswerte bewertet werden. Dies unterstützt eine fundierte Entscheidungsfindung und eine wirksame Risikominderung.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Identifizierung von Bedrohungen und Schwachstellen**
  Die Bewertungen sollten Bedrohungen und Schwachstellen in Software, Netzwerk- und Systemarchitekturen sowie in Einrichtungen, in denen sich kritische IT-Ressourcen befinden, umfassen.
- **Bewertung der Auswirkungen auf das Geschäft**
  Die potenziellen Auswirkungen auf Geschäftsabläufe, Services und Vermögenswerte sollten analysiert werden, um den Schweregrad jedes Risikos zu bestimmen.
- **Einbeziehung menschliche Faktoren**
  Das menschliche Verhalten sollte bei der Entwicklung und Anwendung von Sicherheitsmaßnahmen berücksichtigt werden, insbesondere in Umgebungen der Betriebstechnologie (OT).
- **Dokumentation und Überprüfung**
  Risikobewertungen sollten dokumentiert, regelmäßig überprüft und aktualisiert werden, um Änderungen an Systemen, Abläufen oder der Bedrohungslage Rechnung zu tragen.

ID.RA-05.2 Die Organisation führt Risikobewertungen durch und dokumentiert diese, wobei das Risiko anhand von Bedrohungen, Schwachstellen, Auswirkungen auf Geschäftsprozesse und Vermögenswerte sowie der Wahrscheinlichkeit ihres Eintretens bestimmt wird.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Risikobewertungen nach einem strukturierten Ansatz durchgeführt und dokumentiert werden, der Bedrohungen, Schwachstellen, Auswirkungen auf das Geschäft und die Wahrscheinlichkeit berücksichtigt. Dies unterstützt eine fundierte Entscheidungsfindung und die Priorisierung von Cybersicherheitsmaßnahmen sowohl in IT- als auch in OT-Umgebungen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Interne und externe Bedrohungen einbeziehen**
  Risikobewertungen sollten Bedrohungen berücksichtigen, die sowohl von innerhalb der Organisation als auch von externen Akteuren ausgehen.
- **Anerkannte Risikoanalysemethoden anwenden**
  Qualitative und/oder quantitative Methoden – wie das MAPGOOD-Modell, ISO/IEC 27005 oder die CIS-Risikobewertungsmethode – sollten verwendet werden. Diese Methoden können durch Software-Tools für das Risikomanagement unterstützt werden.
- **Prioritäten nach Wahrscheinlichkeit und Auswirkung setzen**
  Die Zuweisung von Ressourcen und Investitionen in die Cybersicherheit sollte auf der Grundlage der geschätzten Wahrscheinlichkeit von Bedrohungen und der potenziellen Auswirkungen auf Geschäftsprozesse und kritische Vermögenswerte erfolgen.
- **OT-spezifischer Risikobetrachtungen sicherstellen**
  Risikobewertungen sollten OT-spezifische Faktoren wie Sicherheitsimplikationen, Systemverfügbarkeit, ältere Technologien und betriebliche Einschränkungen berücksichtigen.

ID.RA-05.3 Die Ergebnisse der Risikobewertung werden an die relevanten Stakeholder weitergegeben.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Ergebnisse der Risikobewertung den relevanten Stakeholdern wirksam mitgeteilt werden, um fundierte Entscheidungen und koordinierte Reaktionen innerhalb der Organisation zu ermöglichen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Einen Kommunikationsplan oder ein Kommunikationsverfahren festlegen**
  Ein dokumentierter Prozess sollte festlegen, wie, wann und an wen risikobezogene Informationen weitergegeben werden. Dabei sollten sowohl interne als auch externe Stakeholder einbezogen werden.
- **Eine zeitnahe und eindeutige Kommunikation sicherstellen**
  Risikoinformationen sollten unverzüglich und in einem leicht verständlichen Format weitergegeben werden, insbesondere an nicht-technische Stakeholder, die an operativen oder strategischen Entscheidungen beteiligt sind.
- **Kontaktinformationen der Stakeholder verifizieren**
  Die Kontaktinformationen der Stakeholder sollten mindestens einmal jährlich überprüft werden, um die Richtigkeit und Zuverlässigkeit der Kommunikation zu gewährleisten.
- **OT-spezifische Kommunikationsanforderungen unterstützen**
  Kommunikationsverfahren sollten OT-spezifische Rollen berücksichtigen, wie z. B. Ingenieurs-, Wartungs- und Betriebsteams, um sicherzustellen, dass diese relevante Risikoinformationen in Bezug auf Systemverfügbarkeit, Sicherheit und Kontinuität erhalten.

ID.RA-06 Risikobewältigungsmaßnahmen werden ausgewählt, nach Prioritäten geordnet, geplant, nachverfolgt und kommuniziert

ID.RA-06.1 Risikobewältigungsmaßnahmen werden ausgewählt, nach Prioritäten geordnet, geplant, nachverfolgt und kommuniziert

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Reaktionen auf Risiken klar identifiziert, nach Prioritäten geordnet, geplant, verfolgt und kommuniziert werden, um eine wirksame Risikominderung und eine fundierte Entscheidungsfindung in der gesamten Organisation zu unterstützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Risikoreaktionskriterien anwenden**
  Entscheidungen zur Akzeptanz, Übertragung, Minderung oder Vermeidung von Risiken sollten den Kriterien des Schwachstellenmanagements der Organisation entsprechen, wie in ID.RA-08.1 angegeben.
- **Kompensierende Kontrollen sorgfältig auswählen**
  Wenn direkte Risikominderung nicht möglich ist, sollten kompensierende Kontrollen nach denselben Kriterien ausgewählt werden, um eine konsistente Risikominderung zu gewährleisten.
- **Maßnahmen auf Basis der Risikobewertungsergebnisse ergreifen**
  Alle Entscheidungen zur Risikobewältigung sollten auf den Ergebnissen dokumentierter Risikobewertungen beruhen, um sicherzustellen, dass sie mit den tatsächlichen Bedrohungen, Schwachstellen und Auswirkungen auf das Geschäft übereinstimmen.
- **Den Fortschritt der Umsetzung verfolgen**
  Risikomaßnahmen sollten mithilfe strukturierter Tools wie einem Risikoregister, einem Maßnahmenplan und Meilensteinen oder detaillierten Risikoberichten verfolgt werden.

- **Nach Priorität kommunizieren**
  Geplante Risikomaßnahmen sollten den betroffenen Stakeholdern in der Reihenfolge ihrer Priorität mitgeteilt werden, um eine zeitnahe Sensibilisierung und Koordination sicherzustellen.
- **OT-spezifische Überlegungen einbeziehen**
  Risikoreaktionen in OT-Umgebungen sollten betriebliche Einschränkungen, Sicherheitsanforderungen und die Systemverfügbarkeit berücksichtigen, insbesondere bei der Planung von Abschwächungs- oder Ausgleichskontrollen.

ID.RA-08 Prozesse für den Empfang, die Analyse und die Reaktion auf die Offenlegung von Schwachstellen sind eingerichtet

ID.RA-08.1 **Die Organisation erstellt und implementiert einen Schwachstellenmanagementplan, um alle Arten von Schwachstellen zu identifizieren, zu analysieren, zu bewerten, zu mindern und zu kommunizieren, einschließlich in Form einer koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure, CVD) gemäß den geltenden rechtlichen Bestimmungen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Arten von Schwachstellen systematisch identifiziert, analysiert, bewertet, abgemildert und durch einen dokumentierten Schwachstellenmanagementplan kommuniziert werden. Dazu gehört auch die Behandlung von Aufdeckungen im Einklang mit den Praktiken der Coordinated Vulnerability Disclosure (CVD) und den geltenden rechtlichen Anforderungen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Einen umfassenden Plan zum Management von Schwachstellen erstellen**
  Der Plan sollte Schwachstellen aus internen Tests, externen Quellen wie Sicherheitsbulletins und Enthüllungen von Forschern, Anbietern, Partnern oder staatlichen Cybersicherheitsgremien abdecken.
- **Zuständigkeiten und die Überwachung der Umsetzung umsetzen**
  Es sollten klare Rollen für die Bearbeitung, Analyse und Reaktion auf aufgedeckte Schwachstellen definiert werden. Die Durchführung der Verfahren sollte überwacht werden, um eine rechtzeitige und wirksame Bearbeitung zu gewährleisten.
- **Die koordinierte Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure, CVD) unterstützen**
  Der Plan sollte Verfahren für die Entgegennahme von Schwachstellenmeldungen von externen Parteien und die Reaktion darauf enthalten. CVD-Praktiken sollten sich an den Leitlinien des ENISA-Rahmens für CVD orientieren, in dem rechtliche, technische und kommunikative Erwägungen dargelegt sind.
- **OT-spezifische Abdeckung sicherstellen**
  Der Plan sollte Schwachstellen in OT-Umgebungen, einschließlich Altsystemen, vom Hersteller verwalteten Komponenten und eingebetteter Firmware, abdecken, bei denen Patches oder Entschärfungen eine Koordination mit den technischen Teams erfordern können.

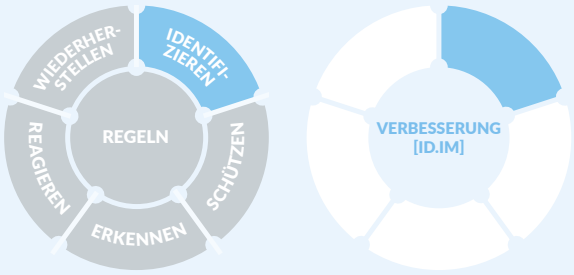
ID.RA-08.2 **Die Organisation implementiert automatisierte Mechanismen zur Verbreitung und Nachverfolgung von Abhilfemaßnahmen im Zusammenhang mit Schwachstelleninformationen, die die Erfassung von Schwachstellendaten automatisch verarbeiten, Informationen verbreiten, Abhilfemaßnahmen nachverfolgen, Berichterstattung und Rechenschaftspflicht umfassen und eine kontinuierliche Überwachung ermöglichen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Informationen über Schwachstellen automatisch gesammelt, verbreitet, nachverfolgt und durch einen dokumentierten und automatisierten Prozess zur Verwaltung von Sicherheitslücken bearbeitet werden. Dazu gehört auch die kontinuierliche Überwachung, Berichterstattung und Rechenschaftspflicht, um rechtzeitige und wirksame Abhilfemaßnahmen zu ermöglichen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Erfassung und Verteilung von Schwachstellendaten automatisieren**
  Schwachstelleninformationen sollten aus internen Quellen (z. B. Audits, OT/IT-Scans) und externen Quellen (z. B. ENISA-Hinweise, Bedrohungsinformationen, Anbieter-Bulletins) gesammelt werden. Diese Informationen sollten mit Hilfe von Dashboards, Warnmeldungen oder integrierten Kommunikationstools automatisch an die relevanten Stakeholder verteilt werden.
- **Abhilfemaßnahmen verfolgen und Fortschritte überwachen**
  Automatisierte Systeme sollten die Implementierung von Abhilfemaßnahmen wie Patches, Konfigurationsänderungen oder kompensierende Kontrollen verfolgen. Die Fortschritte sollten überwacht werden, um eine rechtzeitige Lösung zu gewährleisten.
- **Berichte erstellen und Rechenschaftspflicht sicherstellen**
  Es sollten regelmäßig Berichte erstellt werden, um Transparenz hinsichtlich des Schwachstellenstatus, der zugewiesenen Verantwortlichkeiten und des Fortschritts der Abhilfemaßnahmen zu gewährleisten. Diese Berichte sollten die Transparenz und die Aufsicht des Managements unterstützen.
- **Kontinuierliche Überwachung durch Automatisierung ermöglichen**
  Es sollten automatisierte Mechanismen vorhanden sein, um kontinuierlich nach neuen Schwachstellen zu suchen und sicherzustellen, dass die Workflows zur Behebung entsprechend aktualisiert werden.
- **Die Effektivität der Automatisierung bewerten**
  Die Effektivität der Automatisierung sollte regelmäßig bewertet werden, um Verbesserungen in Bezug auf Reaktionszeit, Effizienz und Sensibilisierung der Stakeholder zu ermitteln. Wenn die Ziele nicht erreicht werden, sollten Anpassungen vorgenommen werden.
- **OT-spezifische Abdeckung sicherstellen**
  Der Automatisierungsprozess sollte OT-Umgebungen umfassen und sich mit Altsystemen, vom Anbieter verwalteten Komponenten und eingebetteter Firmware befassen. Für die Behebung von Problemen in diesen Umgebungen kann eine Abstimmung mit den Ingenieurteams erforderlich sein.



Verbesserungen der organisatorischen Prozesse, Verfahren und Aktivitäten des Managements von Cybersicherheitsrisiken werden in allen CyFun®-Funktionen identifiziert.

ID.IM-02 Verbesserungen werden aus Sicherheitstests und Übungen ermittelt, einschließlich solcher, die in Abstimmung mit Lieferanten und relevanten Dritten durchgeführt werden.

ID.IM-02.1 Aus Sicherheitstests und -übungen, auch in Abstimmung mit Lieferanten und relevanten Drittparteien, werden Verbesserungen ermittelt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, durch die Durchführung von Sicherheitstests und Übungen – intern und in Zusammenarbeit mit Lieferanten und Drittparteien – Möglichkeiten zur Verbesserung der Sicherheit, der Reaktion auf Vorfälle und der Resilienz zu ermitteln. In OT-Umgebungen (Operational Technology) sind diese Aktivitäten unerlässlich, um auf Vorfälle vorbereitet zu sein, die den physischen Betrieb, die Sicherheit oder die Kontinuität der Services beeinträchtigen könnten.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Bereitschaft zur Reaktion auf Vorfälle bewerten**: Sicherheitstests wie Tabletop-Übungen, Simulationen, interne Überprüfungen und Audits sollten genutzt werden, um Verbesserungen bei den Verfahren zur Reaktion auf Vorfälle zu ermitteln.
- **Sich mit externen Parteien koordinieren**: Es sollten Übungen mit kritischen Dienstleistern und Produktlieferanten durchgeführt werden, um die Geschäftskontinuität, die Wiederherstellung im Katastrophenfall und die Reaktionsfähigkeit bei Vorfällen zu stärken.
- **Interne Stakeholder einbeziehen**: Die relevanten internen Stellen, einschließlich der Geschäftsleitung, der Rechtsabteilung und der Personalabteilung, sollten in die Übungen einbezogen werden, um eine umfassende Sensibilisierung und Anpassung der Organisation sicherzustellen.
- **Penetrationstests durchführen**: Systeme mit hohem Risiko sollten Penetrationstests unterzogen werden, um Schwachstellen zu ermitteln. Diese Tests sollten vorab von der Geschäftsführung genehmigt werden.
- **Notfallpläne testen**: Pläne für die Reaktion auf nicht autorisierte oder manipulierte Produkte oder Services sollten getestet und optimiert werden, um eine effektive Wiederherstellung zu gewährleisten.
- **Konformität und Compliance sicherstellen**: Alle Aktivitäten sollten den internen Richtlinien entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

ID.IM-03 Bei der Durchführung von betrieblichen Prozessen, Verfahren und Aktivitäten werden Verbesserungen festgestellt

ID.IM-03.1 **Die Organisation führt nach einem Vorfall Bewertungen durch, um die aus der Reaktion auf einen Vorfall und der Wiederherstellung gezogenen Lehren zu analysieren und folglich Prozesse/Verfahren/Technologien zu verbessern, um ihre Cyber-Resilienz zu erhöhen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Resilienz gegenüber Cyberangriffen zu erhöhen, indem aus Vorfällen gelernt wird. Nach jedem Vorfall sollte die Organisation analysieren, was passiert ist, wie es gehandhabt wurde und was an Prozessen, Verfahren oder Technologien verbessert werden kann.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Durchführung von Überprüfungen nach einem Vorfall**
  Nach jedem Vorfall sollte eine strukturierte Bewertung durchgeführt werden, an der alle Beteiligten beteiligt sind.
- **Nachdenken über die Schlüsselfragen**
  Die Überprüfung sollte untersuchen:
  - Was geschah und warum
  - Wie die Reaktion bewältigt wurde
  - Was gut funktionierte und was nicht
  - Welche Maßnahmen sollten ergriffen werden, um ein erneutes Auftreten zu verhindern
- **Dokumentation von gewonnenen Erkenntnissen**
  Die Ergebnisse der Überprüfung sollten dokumentiert und den zuständigen Teams mitgeteilt werden.
- **Aktualisierung von Richtlinien und Verfahren**
  Die Richtlinien, Prozesse und Verfahren zur Cybersicherheit sollten regelmäßig, mindestens jährlich, überprüft und aktualisiert werden, um die gewonnenen Erkenntnisse zu berücksichtigen.
- **Verbesserung von Tools und Fähigkeiten**
  Gegebenenfalls sollten Technologien und Reaktionsinstrumente auf der Grundlage der Erkenntnisse aus dem Vorfall angepasst oder aktualisiert werden.

ID.IM-03.2 Die Organisation bezieht die aus der Bearbeitung von Vorfällen gewonnenen Erkenntnisse in aktualisierte oder neue Prozesse und/oder Verfahren zur Bearbeitung von Vorfällen ein, die nach Überprüfung, Genehmigung und Testen durch entsprechende Schulungen ergänzt werden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Fähigkeiten der Organisation zur Bewältigung von Vorfällen zu verbessern, indem die aus früheren Vorfällen gewonnenen Erkenntnisse in aktualisierte oder neue Prozesse und Verfahren einfließen. In OT-Umgebungen (Operational Technology), in denen Vorfälle direkte Auswirkungen auf physische Systeme und die Betriebskontinuität haben können, trägt die Anwendung von Erkenntnissen aus der Praxis dazu bei, die Reaktionsfähigkeit zu verbessern und die Wahrscheinlichkeit wiederholter Ausfälle zu verringern.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Den gesamten Lebenszyklus eines Vorfalls abdecken**: Lehren sollten aus allen Phasen der Behandlung von Vorfällen gezogen werden, einschließlich Identifizierung, Kategorisierung, Priorisierung, Untersuchung, Lösung, Wiederherstellung, Abschluss und Überprüfung nach einem Vorfall.
- **Prozessoptimierung demonstrieren**: Aktualisierungen der Verfahren zur Behandlung von Vorfällen sollten die aus früheren Vorfällen gewonnenen Erkenntnisse widerspiegeln und klar dokumentiert werden.
- **Mit Lieferanten zusammenarbeiten**: Sitzungen über gewonnene Erkenntnisse sollten gemeinsam mit den wichtigsten Lieferanten durchgeführt werden, um die Koordination und Reaktion innerhalb der Lieferkette zu verbessern.
- **Leistungsmetriken verwenden**: Anhand von Kennzahlen sollte die Effektivität der Behandlung von Vorfällen im Laufe der Zeit verfolgt und bewertet werden, um Verbesserungen zu veranlassen.
- **Konformität und Compliance sicherstellen**: Alle Aktualisierungen für Prozesse und Verfahren sollten den internen Richtlinien entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

ID.IM-03.3 Die Organisation ermittelt Verbesserungen, die sich aus der Überwachung, den Messungen, den Bewertungen und den gewonnenen Erkenntnissen ergeben, und diese konsequent in verbesserte Prozesse/Verfahren/Technologien umsetzen, um ihre Cyber-Resilienz zu erhöhen (kontinuierliche Verbesserung).

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Cyber-Resilienz der Organisation zu erhöhen, indem Verbesserungen aus der Überwachung, den Messungen, den Bewertungen und den gewonnenen Erfahrungen ermittelt und in aktualisierte Prozesse, Verfahren oder Technologien umgesetzt werden. In OT-Umgebungen, in denen Systemzuverlässigkeit und -sicherheit eng mit der Cyberleistung verknüpft sind, trägt die kontinuierliche Verbesserung dazu bei, die betriebliche Integrität aufrechtzuerhalten und sich an die sich entwickelnden Bedrohungen anzupassen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Metriken zur Cyber-Resilienz nutzen**: Metriken sollten verwendet werden, um die Fähigkeit der Organisation zu bewerten, Cybervorfällen zu widerstehen und sich von ihnen zu erholen, um ein fundiertes Risikomanagement und eine fundierte Entscheidungsfindung zu unterstützen.
- **Wirksamkeitsmaßstäbe (Measures of Effectiveness, MOEs) anwenden**: MOE sollten verwendet werden, um die Effektivität verschiedener Cyber-Resilienz-Strategien zu bewerten und zu vergleichen und Investitions- oder Designentscheidungen zu treffen.
- **Zielgerichtete Metriken implementieren**: Die Metriken sollten sich auf Bereitschaft, Betriebskontinuität bei Angriffen, Schadensbegrenzung sowie Wiederherstellungs- und Wiederaufbaufähigkeiten beziehen.
- **Unabhängige Bewertungen durchführen**: Unabhängige Teams sollten mit der Durchführung von Bewertungen beauftragt werden und objektive Erkenntnisse über verbesserungswürdige Bereiche liefern.
- **Strukturierte Bewertungssysteme nutzen**: Bewertungsmethoden wie die SSM-CR (Situated Scoring Methodology for Cyber Resiliency) von MITRE sollten in Betracht gezogen werden, um eine strukturierte Bewertung und Priorisierung von Verbesserungen zu unterstützen.
- **Konformität und Compliance sicherstellen**: Alle Verbesserungen sollten den internen Richtlinien entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

ID.IM-03.4 Die Organisation arbeitet zusammen und tauscht Informationen über sicherheitsrelevante Vorfälle in ihrem kritischen System und Maßnahmen zur Schadensbegrenzung aus.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Cyber-Resilienz zu stärken, indem Informationen über Sicherheitsvorfälle und Abhilfemaßnahmen in Bezug auf kritische Systeme mit den benannten Partnern ausgetauscht werden. In OT-Umgebungen trägt ein rechtzeitiger und koordinierter Informationsaustausch dazu bei, die Ausbreitung von Bedrohungen zu verhindern, eine schnellere Wiederherstellung zu unterstützen und die kollektive Verteidigung über vernetzte Systeme zu verbessern.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Rollen und Befugnisse definieren**: Der Reaktionsplan für Vorfälle sollte die Rollen, Zuständigkeiten und Befugnisse für die Weitergabe von vorfallbezogenen Informationen an die benannten Partner klar umreißen.
- **Reaktionsteams schulen**: Die Notfallkräfte sollten regelmäßig in den Verfahren für die Kommunikation mit externen Partnern während und nach Vorfällen geschult werden.
- **Sich mit Partnern koordinieren**: Der Informationsaustausch sollte Einzelheiten zu Vorfällen, Abhilfemaßnahmen und gewonnenen Erkenntnissen umfassen, insbesondere mit Lieferanten und Dienstleistern, die am Betrieb kritischer Systeme beteiligt sind.
- **Auf vertrauenswürdige Anleitungen verweisen**: Relevante Praktiken sollten sich auf vertrauenswürdige Quellen stützen, wie z. B. die ENISA/CERT-EU Security Guidance 22-001, die empfohlene Abhilfemaßnahmen gegen kritische Bedrohungen enthält.
- **Konformität und Compliance sicherstellen**: Alle Aktivitäten zur Zusammenarbeit und Teilung sollten den internen Richtlinien entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

ID.IM-03.5 Die Wirksamkeit von Schutztechnologien ist den relevanten Interessengruppen mitzuteilen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Wirksamkeit der Schutztechnologien den relevanten Interessengruppen klar mitgeteilt wird. In OT-Umgebungen, in denen Schutz-Tools wichtige physische Systeme schützen, unterstützt eine sinnvolle Kommunikation fundierte Entscheidungen, Risikobewusstsein und die Abstimmung zwischen technischen und nicht-technischen Teams.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Kommunikation auf die Interessengruppen zuschneiden**: Die Informationen sollten an die Bedürfnisse der verschiedenen Zielgruppen angepasst werden. Technische Teams benötigen möglicherweise detaillierte Protokolle, während Führungskräfte Zusammenfassungen auf hoher Ebene in Verbindung mit dem Geschäftsrisiko benötigen.
- **Über technische Metriken hinausgehen**: Die Kommunikation sollte nicht nur Daten enthalten (z. B. abgewehrte Bedrohungen, erkannte Vorfälle), sondern auch Einblicke in die Risikolage, neue Trends und empfohlene Maßnahmen.
- **Alle relevanten Rollen einbeziehen**: Beteiligte wie CISOs, IT-Sicherheitsteams, Compliance-Beauftragte, interne Auditoren und Führungskräfte sollten die Informationen erhalten, die sie für ihre Aufgaben benötigen.
- **Leistung überwachen und melden**: Die Leistung von Schutztechnologien (z. B. Virenschutz, Firewalls, Intrusion Prevention, Endpoint Detection, Data Loss Prevention) sollte kontinuierlich überwacht und gemeldet werden.
- **Kontinuierliche Verbesserung unterstützen**: Die Kommunikation sollte dazu beitragen, Lücken zu erkennen, strategische Entscheidungen zu treffen und eine Kultur der Transparenz und Resilienz zu fördern.
- **Konformität und Compliance sicherstellen**: Alle Kommunikationspraktiken sollten den internen Richtlinien entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

ID.IM-03.6 Die Organisation setzt, soweit durchführbar, automatisierte Mechanismen ein, um den Prozess des Informationsaustausches und der Zusammenarbeit zu erleichtern.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Effizienz, Genauigkeit und Sicherheit des Informationsaustauschs und der Zusammenarbeit zu verbessern, indem automatisierte Mechanismen eingesetzt werden, wo dies möglich ist. In OT-Umgebungen trägt die Automatisierung dazu bei, manuelle Fehler zu reduzieren, Zugriffskontrollen durchzusetzen und zeitnahe Entscheidungen über vernetzte Systeme hinweg zu unterstützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Zugangsberechtigungen abgleichen**: Automatisierte Tools sollten überprüfen, ob die Zugriffsrechte der Partner für den Informationsaustausch mit der Sensibilität der Informationen übereinstimmen. Unstimmigkeiten sollten markiert werden, bevor die gemeinsame Nutzung erfolgt.
- **Durchsetzung von Richtlinien automatisieren**: Die Systeme sollten automatisch bewerten, ob Informationen auf der Grundlage ihrer Klassifizierung und der Zugriffsrechte des Empfängers freigegeben werden können. Diese Überprüfungen sollten in Identitäts- und Zugriffsmanagementsysteme (IAM) integriert werden, um aktuelle Berechtigungsdaten zu gewährleisten.
- **Suche und Abrufe kontrollieren**: Such- und Abruftools sollten Zugriffsbeschränkungen mit Hilfe von Metadaten-Tagging und Klassifizierung durchsetzen, um sicherzustellen, dass Nutzer nur auf autorisierte Informationen zugreifen können.
- **Aktivitäten überwachen und auditieren**: Eine automatische Protokollierung und Überwachung sollte alle Aktionen zum Informationsaustausch verfolgen. Die Protokolle sollten regelmäßig überprüft werden, um unbefugte Zugriffe oder Richtlinienverstöße zu erkennen.
- **Benutzerfreundlichkeit und Schulung fördern**: Automatisierte Tools sollten benutzerfreundlich sein, um eine korrekte Nutzung zu fördern. Es sollten Schulungen angeboten werden, um sicherzustellen, dass die Nutzer wissen, wie sie diese Instrumente effektiv und verantwortungsvoll nutzen können.
- **Konformität und Compliance sicherstellen**: Alle automatisierten Mechanismen sollten den internen Richtlinien entsprechen und die geltenden Gesetze, Vorschriften und Branchenstandards einhalten.

ID.IM-03.7 Die Organisation implementiert unabhängige Teams, um ihre Prozesse, bewährten Verfahren und technologischen Lösungen zum Schutz kritischer Systeme und Vermögenswerte zu bewerten.

Implementierungshinweise

Ziel dieser Kontrolle ist es, den Schutz kritischer Systeme und Vermögenswerte zu verstärken, indem eine objektive Bewertung der organisatorischen Prozesse, Praktiken und Technologien gewährleistet wird. Im Bereich der Betriebstechnologie (OT) helfen unabhängige Evaluierungen dabei, Schwachstellen zu erkennen, Voreingenommenheit zu verringern und eine kontinuierliche Verbesserung der Widerstandsfähigkeit und Sicherheit von Systemen zu unterstützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Unabhängige Teams einbinden**
  Zu den unabhängigen Bewertern sollten interne Mitarbeiter gehören, die nicht in die Entwicklung oder den Betrieb des Systems involviert sind, sowie externe Experten, die keine finanziellen oder betrieblichen Verbindungen zu dem System haben.
- **Unparteilichkeit sicherstellen**
  Die Bewerter sollten frei von Interessenkonflikten sein. Die Bewertungsrollen sollten abwechselnd besetzt werden, um eine Verzerrung durch Vertrautheit zu vermeiden. Unabhängigkeit und Qualifikation sollten dokumentiert werden.

- **Umfang und Kriterien klar und deutlich definieren**
  Die Bewertungsziele, der Umfang und die Bewertungskriterien sollten im Voraus vereinbart werden, um eine unzulässige Beeinflussung durch die Stakeholder zu verhindern.
- **Unabhängige Berichtswege einrichten**
  Die Bewertungsergebnisse sollten direkt an das Senior Management oder ein Aufsichtsgremium weitergeleitet werden, ohne die für die überprüften Systeme zuständigen Teams zu informieren.
- **Die Wirksamkeit der Bewertung regelmäßig überprüfen**
  Die Unabhängigkeit und Leistung der Bewertungsteams sollte regelmäßig überprüft werden, um Objektivität und Relevanz zu gewährleisten.

ID.IM-03.8 Die Organisation stellt sicher, dass der Sicherheitsplan für ihre kritischen Systeme die Überprüfung, das Testen und die kontinuierliche Verbesserung der Sicherheitsschutzverfahren erleichtert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass der Sicherheitsplan der Organisation für kritische Systeme die regelmäßige Überprüfung, das Testen und die kontinuierliche Verbesserung der Schutzmaßnahmen unterstützt. In OT-Umgebungen (Operational Technology) hilft dies, die Systemintegrität aufrechtzuerhalten, sich an sich entwickelnde Bedrohungen anzupassen und sich mit umfassenderen Risikomanagementmaßnahmen abzustimmen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Einen Sicherheitsplan entwickeln und pflegen**
  Ein dokumentierter Plan sollte beschreiben, wie kritische Systeme vor Sicherheitsbedrohungen geschützt werden. Er sollte sich vom Risikobehandlungsplan unterscheiden, aber auf diesen abgestimmt sein.
- **Sich auf operative und technische Kontrollen konzentrieren**
  Der Plan sollte definierte Sicherheitsziele, zugewiesene Verantwortlichkeiten, Sicherheitsarchitektur, Kontrollmaßnahmen und Verfahren zur Überwachung, Prüfung und Bewertung der Kontrollen enthalten.
- **Regelmäßige Überprüfungen und Tests ermöglichen**
  Der Plan sollte geplante Überprüfungen, Schwachstellenbewertungen und Penetrationstests unterstützen, um die Wirksamkeit der Sicherheitsmaßnahmen zu bewerten.
- **Kontinuierliche Verbesserungen unterstützen**
  Aktualisierungen sollten auf gewonnenen Erkenntnissen, Bedrohungsinformationen, Auditergebnissen und Veränderungen in der Bedrohungslandschaft basieren.
- **Mit dem Risikomanagement integrieren**
  Der Plan sollte mit den Risikobehandlungs- und Governance-Prozessen der Organisation abgestimmt sein, um Konsistenz und Verantwortlichkeit sicherzustellen.
- **Den Plan auf dem neuesten Stand halten**
  Der Plan sollte regelmäßig überprüft und aktualisiert werden, um Systemänderungen, neue Bedrohungen und sich ändernde betriebliche Anforderungen zu berücksichtigen.

ID.IM-03.9 Die Organisation führt spezialisierte Bewertungen durch, einschließlich eingehender Überwachung, Schwachstellen-Scans, Tests auf böswillige Benutzer, Bewertung von Insider-Bedrohungen, Leistungs-/Lasttests sowie Verifikations- und Validierungstests für die kritischen Systeme der Organisation.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Sicherheitslage kritischer Systeme zu verbessern, indem spezielle Bewertungen durchgeführt werden, die Schwachstellen aufdecken, die Leistung bewerten und die Abwehrmaßnahmen gegen interne und externe Bedrohungen testen. In OT-Umgebungen (Operational Technology) tragen diese Bewertungen zur Validierung von Schutzmaßnahmen und zur kontinuierlichen Verbesserung bei.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Spezialisierte Bewertungen durchführen**
  Die Bewertungen sollten eine eingehende Überwachung, Schwachstellenscans, Tests auf schädliche Nutzer, Bewertungen der Insider-Bedrohung, Leistungs-/Belastungstests sowie Verifizierungs- und Validierungstests umfassen.
- **An akkreditierte Anbieter auslagern**
  Spezialisierte Bewertungen können ausgelagert werden, vorzugsweise an akkreditierte Organisationen. Die Akkreditierung sollte nach anerkannten Standards erfolgen, wie z. B.:
  - CREST für Penetrationstests und Schwachstellenbewertungen
  - ISO/IEC 17025 für Prüflaboratorien
    Die Akkreditierung sollte durch anerkannte Stellen wie CREST, nationale Akkreditierungsbehörden (z. B. BELAC) oder branchenspezifische Stellen (z. B. PCI Security Standards Council) erfolgen. Dadurch wird sichergestellt, dass die Bewertungen mit fachlicher Kompetenz, unparteiisch und im Einklang mit bewährten Verfahren durchgeführt werden.
- **Ergebnisse in Abhilfemaßnahmen integrieren**
  Bei Bewertungen festgestellte Schwachstellen sollten durch festgelegte Abhilfemaßnahmen behoben werden, wie in der Kontrolle ID.IM-03.3 beschrieben.
- **Die Bereitschaft und Reifegradbewertung unterstützen**
  Die Bewertungsergebnisse sollten Aufschluss über die organisatorische Bereitschaft und Leistungsniveaus (z. B. CyFun®-Reifegrad) geben und als Leitfaden für gezielte Verbesserungen dienen.

ID.IM-04 Pläne zur Reaktion auf Vorfälle und andere Cybersicherheitspläne, die sich auf den Betrieb auswirken, werden erstellt, kommuniziert, gepflegt und verbessert

ID.IM-04.1 Notfall- und Kontinuitätspläne werden erstellt, kommuniziert, gepflegt, getestet, validiert und verbessert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Resilienz der Organisation zu gewährleisten, indem Notfall- und Kontinuitätspläne erstellt, aufrechterhalten und verbessert werden, die eine wirksame Reaktion auf und Wiederherstellung nach Störungen ermöglichen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Umfassende Pläne erstellen**
  Die Pläne sollten Folgendes beinhalten:
  - **Plan für die Reaktion auf Vorfälle**
  - **Business Continuity Plans (BCP)**
  - **Notfallwiederherstellungsplan (Disaster Recovery Plan, DRP)**
    Dieser sollte sich mit Betriebsunterbrechungen, Datenverletzungen und geschäftskritischen Ausfällen befassen.
- **Klare Plan-Inhalt definieren**
  Die Pläne sollten Folgendes beinhalten:
  - Kontakt- und Kommunikationsdaten
  - Rollen, Zuständigkeiten und Befugnisse (gemäß GV.RR-02.1)
  - Verfahren für gängige Szenarien
  - Kriterien für Prioritätensetzung, Eskalation und Entscheidungsfindung
    Die IRP sollten die Erkennung, Eindämmung, Reaktion und Wiederherstellung nach Cybervorfällen abdecken.
- **Kommunizieren und schulen**
  Die Pläne sollten an alle betroffenen Mitarbeiter weitergegeben werden. Es sollte ein Krisenmanagementteam mit Vertretern der wichtigsten Abteilungen (z. B. IT, Recht, HR, PR) eingerichtet und für das Handeln in Krisenfällen geschult werden.
- **Pläne pflegen und überprüfen**
  Pläne sollten mindestens einmal jährlich oder nach größeren Änderungen oder Vorfällen überprüft werden. Die Aktualisierungen sollten die gewonnenen Erkenntnisse und die sich entwickelnden Risiken widerspiegeln.
- **Regelmäßig testen und validieren**
  Die Pläne sollten anhand realistischer Szenarien getestet werden. Die Validierung soll bestätigen, dass die Verfahren wie vorgesehen funktionieren und den betrieblichen Anforderungen entsprechen. Die Ergebnisse sollten dokumentiert werden.
- **Kontinuierlich verbessern**
  Das Feedback aus Tests, Vorfällen und Überprüfungen sollte zu Verbesserungen führen. Verbesserungen sollten je nach Risiko und Auswirkung priorisiert werden, um die Kontinuität der wesentlichen Funktionen zu gewährleisten.
- Siehe auch: Richtlinienvorlagen auf www.cyfun.eu

ID.IM-04.2 Die Organisation koordiniert die Entwicklung und das Testen von Plänen zur Reaktion auf Vorfälle und anderen Cybersicherheitsplänen, die sich auf den Betrieb auswirken, mit den Stakeholdern, um sicherzustellen, dass diese Pläne mit den allgemeinen Organisationszielen übereinstimmen und die Widerstandsfähigkeit verbessern.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Notfallpläne und andere Cybersicherheitspläne, die sich auf den Betrieb auswirken, mit den Unternehmenszielen in Einklang stehen und durch koordinierte Entwicklung und Tests mit den relevanten Stakeholdern die Widerstandsfähigkeit verbessern.

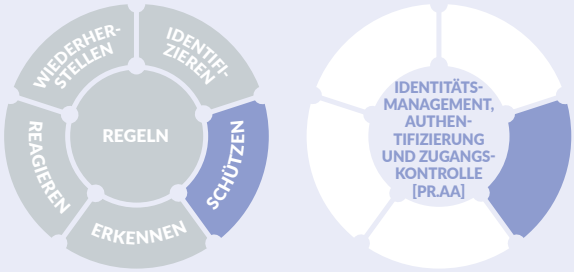
Um dieses Ziel zu erreichen, sollte die Organisation:

- **Pläne regelmäßig überprüfen und aktualisieren**
  Die Pläne sollten überprüft und aktualisiert werden, um den sich entwickelnden Bedrohungen, organisatorischen Veränderungen und betrieblichen Erfordernissen Rechnung zu tragen.
- **Stakeholder frühzeitig einbeziehen**
  Die Stakeholder, einschließlich interner Teams, Lieferanten und relevanter Dritter, sollten frühzeitig in den Planungsprozess einbezogen werden, um die Abstimmung und Relevanz sicherzustellen.
- **Laufende Kommunikation aufrechterhalten**
  Stakeholder sollten über die Fortschritte, Aktualisierungen und Änderungen des Plans auf dem Laufenden gehalten werden, um das gemeinsame Verständnis und die Bereitschaft zu erhalten.
- **Testaktivitäten koordinieren**
  Die Prüfung der Pläne sollte mit den Stakeholdern koordiniert werden, um die Wirksamkeit zu überprüfen, die Rollen zu klären und die Reaktionsfähigkeit der Zusammenarbeit zu stärken.


Username
Password
Protected
Balance
5.367.50 $

SCHÜTZEN

Schützen



Der Zugang zu physischen und logischen Vermögenswerten ist auf autorisierte Benutzer, Dienste und Hardware beschränkt und wird entsprechend dem bewerteten Risiko eines unbefugten Zugangs verwaltet

PR.AA-01 Identitäten und Berechtigungsnachweise für autorisierte Benutzer, Dienste und Hardware werden von der Organisation verwaltet

PR.AA-01.1 Identitäten und Berechtigungsnachweise für autorisierte Benutzer, Services und Hardware werden von der Organisation verwaltet

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Identitäten und Berechtigungsnachweise für autorisierte Benutzer, Services und Hardware ordnungsgemäß verwaltet werden, um unbefugten Zugriff zu verhindern und einen sicheren Betrieb sowohl in IKT- als auch in OT-Umgebungen zu unterstützen.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Zugriffsanträge und Autorisierung
  - Der Zugriff sollte förmlich beantragt, dokumentiert und von den System- oder Dateneigentümern genehmigt werden.
  - Die Zugriffsrechte sollten dem Grundsatz des geringsten Privilegs folgen.
- Identitäts- und Berechtigungsmanagement
  - Es sollten individuelle Benutzerkonten verwendet werden; die gemeinsame Nutzung von Passwörtern sollte vermieden werden.
  - Die Standardpasswörter sollten vor der Aktivierung der Systeme geändert werden.
  - Nicht genutzte Konten sollten sofort deaktiviert werden.
  - Administratorkonten sollten begrenzt sein, regelmäßig überprüft und nicht für tägliche Aufgaben verwendet werden.
- Passwort-Richtlinie
  - Es sollten strenge Passwortregeln durchgesetzt werden.
  - Passwörter sollten regelmäßig oder sofort nach einer vermuteten Kompromittierung geändert werden.
  - Es sollte eine formelle Passwort-Richtlinie vorhanden sein (siehe auch: CyFun® Toolbox auf www.cyfun.eu).
  - Rechte und Privilegien sollten über Benutzergruppen vergeben werden.

- **Geräte- und Hardware-Identität**
  - Jedes autorisierte Gerät sollte eine eindeutige Kennung haben (z. B. MAC-Adresse, Seriennummer).
  - Die Geräte sollten physisch gekennzeichnet werden, um die Inventarisierung und Wartung zu unterstützen.
- **Gemeinsamer Zugang zu PLCs/HMIs (OT-spezifische Maßnahmen)**
  - Wenn individuelle Konten nicht realisierbar sind, sollte das Prinzip der geringsten Privilegien trotzdem gelten.
  - Ein sicherer Jump-Server oder ein HMI-Frontend sollte verwendet werden, um den Zugriff zu kontrollieren, Aktivitäten zu protokollieren und Authentifizierungsebenen hinzuzufügen.
- **Sicherer Fernzugriff**
  - Die technischen Anforderungen für den Fernzugriff sollten klar definiert und dokumentiert werden.
  - Es sollten sichere Methoden wie VPNs, verschlüsselte Protokolle (z. B. SSH, TLS) und Multi-Faktor-Authentifizierung (MFA – siehe auch PR.AA-03.2) verwendet werden.
  - Der Fernzugriff sollte überwacht und protokolliert werden.

PR.AA-01.2 Identitäten und Berechtigungsnachweise für autorisierte Benutzer, Services und Hardware werden, soweit möglich, durch automatisierte Mechanismen verwaltet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko des Missbrauchs von Berechtigungsnachweisen und des unbefugten Zugriffs durch die Automatisierung von Verwaltungsprozessen für Identitäten und Berechtigungsnachweise zu verringern und so Konsistenz, Skalierbarkeit und Sicherheit in IT- und OT-Umgebungen zu gewährleisten.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Verwaltung von Berechtigungsnachweisen automatisieren**
  Automatisierte Systeme sollten für die Ausstellung, Überprüfung, den Entzug und die Kontrolle von Berechtigungsnachweisen für Benutzer, Services und Hardware eingesetzt werden. Dies reduziert manuelle Fehler und verbessert die betriebliche Effizienz.
- **Starke Authentifizierungsmechanismen implementieren**
  In Übereinstimmung mit der Kontrolle PR.AA-03.2 ist MFA für alle Fernzugriffe auf die Netzwerke der Organisation erforderlich. Bei der Multifaktor-Authentifizierung (MFA) sollten mindestens zwei unabhängige Faktoren verwendet werden:
  - *Wissen* (z. B. Passwort oder PIN)
  - *Besitz* (z. B. Token oder Smartphone)
  - *Inhärenz* (z. B. Fingerabdruck- oder Gesichtserkennung)

  Diese Faktoren sollten unabhängig voneinander sein, um zu gewährleisten, dass eine Beeinträchtigung des einen die anderen nicht beeinflusst.
- **Kryptografische und Token-basierte Lösungen nutzen**
  Digitale Zertifikate und Identitäts-Token sollten zur Authentifizierung von Benutzern, Geräten und Services verwendet werden, insbesondere in OT-Umgebungen, in denen die manuelle Handhabung von Anmeldeinformationen unpraktisch sein kann.
- **Eine OT-spezifische Integration sicherstellen**
  Identitäts- und Zugriffsmanagementlösungen sollten OT-Systeme, einschließlich älterer Geräte und vom Anbieter verwalteter Komponenten, mit minimaler Unterbrechung des Betriebs unterstützen.
  Wenn individuelle Benutzerkonten nicht möglich sind (z. B. gemeinsamer Zugang zu PLCs oder HMI), sollte der Zugang über sichere Jump-Server mit Protokollierung und zusätzlichen Authentifizierungsebenen erfolgen. Der Fernzugriff auf OT-Systeme sollte über sichere Protokolle (z. B. VPN, SSH, TLS) erfolgen, zeitlich begrenzt sein (Just-in-Time) und vollständig überwacht werden.

PR.AA-01.3 **Die Berechtigungsnachweise des Systems werden nach einer bestimmten Zeit der Inaktivität deaktiviert, es sei denn, dies würde den sicheren Betrieb (kritischer) Prozesse gefährden.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Berechtigungsnachweise des Systems nach einer bestimmten Zeit der Inaktivität deaktiviert werden, es sei denn, dies würde den sicheren Betrieb kritischer Prozesse gefährden. Dies trägt dazu bei, das Risiko eines unbefugten Zugriffs zu verringern und gleichzeitig die Betriebskontinuität zu wahren.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Dienstkonten für automatisierte Vorgänge verwenden**
  Dienstkonten sollten zum Ausführen von Anwendungen, Diensten oder automatisierten Aufgaben verwendet werden. Diese Konten sollten mit minimalen Berechtigungen konfiguriert, von Benutzerkonten isoliert und separat überwacht werden, um die Nachvollziehbarkeit und sichere Automatisierung zu unterstützen.
- **Das Prinzip der geringsten Privilegien anwenden**
  Dienstkonten sollten nur über die für ihre Funktion erforderlichen Berechtigungen verfügen. Dies schränkt potenziellen Missbrauch ein und unterstützt den sicheren Betrieb sowohl in IT- als auch in OT-Umgebungen.
- **Aktivitäten von Dienstkonten überwachen und auditieren**
  Von Dienstkonten durchgeführte Maßnahmen sollten protokolliert und regelmäßig überprüft werden. Dies verbessert die Rückverfolgbarkeit und hilft, Anomalien oder Missbrauch aufzudecken.
- **Richtlinien zur Inaktivität von Berechtigungsnachweise implementieren**
  Berechtigungsnachweise für das System, einschließlich derjenigen für Dienst- und Benutzerkonten, sollten nach einer festgelegten Zeit der Inaktivität automatisch deaktiviert werden. Ausnahmen sollten dokumentiert und begründet werden, insbesondere in OT-Umgebungen, in denen ein kontinuierlicher Betrieb kritisch ist.
- **Formelle Zugriffsverfahren für externe Parteien festlegen**
  Der externe Zugriff sollte einem definierten Prozess folgen, einschließlich rollenbasierter Zugriffsebenen, Autorisierungsschritten, Identitätsverifizierung und Sensibilisierungsschulungen. Es sollten Überwachungs- und Widerrufsmechanismen vorhanden sein, um Zugriffsverletzungen zu verwalten.
- **OT-spezifische Überlegungen sicherstellen**
  In OT-Umgebungen sollten die Richtlinien zur Deaktivierung von Berechtigungsnachweisen die Anforderungen an die Systembetriebszeit, vom Anbieter verwaltete Komponenten und Altsysteme berücksichtigen. Zur Vermeidung von Betriebsunterbrechungen kann eine Koordinierung mit den Ingenieurteams erforderlich sein.

PR.AA-01.4 **Für Transaktionen innerhalb der kritischen Systeme der Organisation setzt die Organisation, soweit angemessen und durchführbar, Multi-Faktor-Authentifizierung (MFA), kryptographische Zertifikate, Identitäts-Tokens, kryptographische Schlüssel und andere Berechtigungsnachweise ein.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass starke Authentifizierungsmechanismen für Transaktionen innerhalb kritischer Systeme angewendet werden. Dazu gehört der Einsatz von Multi-Faktor-Authentifizierung (MFA – PR.AA-03.2), kryptografischen Berechtigungsnachweisen und anderen sicheren Methoden zum Schutz sensibler Vorgänge und des Datenaustauschs.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Starke Authentifizierung für kritische Transaktionen verwenden**
  Transaktionen, bei denen es um den Zugriff auf sensible Daten, Änderungen an der Systemkonfiguration, die Ausführung von Befehlen, die Authentifizierung von Benutzern/Geräten oder die Datenübertragung zwischen Systemen geht, sollten nach Möglichkeit durch MFA, Identitäts-Token, kryptografische Schlüssel oder Zertifikate geschützt werden.

- **Kontextbezogene und verhaltensbasierte Authentifizierung verwenden**
  Eine starke Authentifizierung sollte kontextbezogene Überprüfungen (z. B. Standort, Zeit, Gerät) und verhaltensbasierte Biometrie (z. B. Tippmuster) umfassen, um Anomalien zu erkennen und die Sicherheit zu erhöhen.
- **MFA mit Single Sign-On (SSO) kombinieren**
  MFA sollte in SSO-Lösungen integriert werden, um den Zugriff zu optimieren und gleichzeitig einen robusten Schutz für interne und externe kritische Systeme zu gewährleisten.
- **Kryptographische Berechtigungsnachweise sicher verwalten**
  Kryptographische Zertifikate, Identitäts-Token und Schlüssel sollten sicher ausgestellt, gespeichert, rotiert und widerrufen werden. Dies unterstützt die sichere Implementierung von starken Authentifizierungsmechanismen, die von dieser Kontrolle gefordert werden, und ergänzt PR.AA-03.2, das MFA für den Fernzugriff vorschreibt.
- **OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollten Authentifizierungsmethoden an Systembeschränkungen, Altgeräte und Anforderungen an die Betriebskontinuität angepasst werden. Zur Umsetzung praktikabler Lösungen kann eine Koordinierung mit den Ingenieurteams erforderlich sein.

PR.AA-01.5 „Die kritischen Systeme der Organisation werden auf eine atypische Nutzung von Systemzugangsdaten überwacht. Berechtigungsnachweise, die mit einem erheblichen Risiko verbunden sind, werden deaktiviert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, eine anormale oder risikoreiche Verwendung von Berechtigungsnachweisen in kritischen Systemen zu erkennen und darauf zu reagieren, um unbefugten Zugriff, Insider-Bedrohungen und auf Berechtigungsnachweisen basierende Angriffe zu verhindern.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Eine auffällige Nutzung von Berechtigungsnachweisen erkennen**
  Systeme sollten auf Abweichungen vom normalen Nutzungsverhalten von Berechtigungsnachweisen überwacht werden, wie z. B. ungewöhnliche Anmeldezeiten, Zugriffe von unbekannten Standorten, Nutzung unbekannter Systeme, gleichzeitige Anmeldungen von weit entfernten Standorten oder plötzlicher Zugriff auf sensible Daten.
- **Fehlgeschlagene Anmeldeversuche begrenzen und darauf reagieren**
  Es sollte ein Schwellenwert für fehlgeschlagene Anmeldeversuche durchgesetzt werden. Konten sollten nach wiederholten Fehlern automatisch gesperrt werden und so lange unzugänglich bleiben, bis eine festgelegte Sperrfrist abläuft oder ein autorisierter Administrator sie zurücksetzt.
- **Den Lebenszyklus von Berechtigungsnachweisen verwalten**
  Die Ausstellung, Verwendung und Sperrung von Berechtigungsnachweisen sollte nach Möglichkeit automatisiert werden. Es sollte ein aktueller Bestand an aktiven Berechtigungsnachweisen geführt werden, und nicht genutzte oder verwaiste Konten sollten regelmäßig überprüft und deaktiviert werden.
- **Ereignisse überwachen und korrelieren**
  SIEM-Tools (Security Information and Event Management) oder gleichwertige Lösungen sollten in Betracht gezogen werden, um Anomalien zu erkennen und Ereignisse systemübergreifend zu korrelieren. Es sollte ein Behavioural Baselining durchgeführt werden, um Abweichungen von der typischen Nutzung festzustellen.
- **Hochriskante Berechtigungsnachweise automatisch deaktivieren**
  Berechtigungsnachweise, die mit bestätigten oder hochriskanten anomalen Aktivitäten in Verbindung stehen, sollten unverzüglich deaktiviert werden. Die Sicherheitsteams sollten zur Untersuchung und Reaktion benachrichtigt werden. Alle Maßnahmen sollten für Audit- und forensische Zwecke protokolliert werden.
- **Benutzer sensibilisieren**
  Die Benutzer sollten im Umgang mit sicheren Berechtigungsnachweisen geschult werden und dazu angehalten werden, verdächtige Aktivitäten oder Anomalien im Zugangsverhalten zu melden.

PR.AA-02 Identitäten werden geprüft und an Berechtigungsnachweise gebunden, basierend auf dem Kontext der Interaktionen

PR.AA-02.1 Die Organisation implementiert dokumentierte Verfahren zur Überprüfung der Identität von Personen, bevor sie Berechtigungsnachweise ausstellt, die den Zugang zu den Systemen der Organisation ermöglichen.

Implementierungshinweise

Ziel dieser Kontrolle, die auf GV.RR-04.1 aufbaut, ist es, sicherzustellen, dass nur verifizierten Personen Berechtigungsnachweise gewährt werden, um so das Risiko von Identitätsbetrug, unbefugtem Zugang und Insider-Bedrohungen zu verringern.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Dokumentierte Verfahren zur Identitätsüberprüfung einführen**
  Es sollte ein formelles Verfahren zur Identitätsüberprüfung vor der Ausstellung von Ausweisen entwickelt und genehmigt werden. Dieser Prozess sollte die Verantwortlichkeit, Rückverfolgbarkeit und Rechenschaftspflicht sicherstellen.
- **Die Identität anhand vertrauenswürdiger Quellen verifizieren**
  Die Identitätsüberprüfung sollte sich auf offizielle Dokumente wie staatliche Ausweise, Reisepässe oder Führerscheine stützen. Für das Remote- oder digitale Onboarding sollten die Praktiken mit den ENISA's Remote Identity Proofing Good Practices übereinstimmen.
- **Identitätsbetrug und -missbrauch verhindern**
  Die Verfahren sollten Kontrollen zur Aufdeckung und Verhinderung von Identitätsdiebstahl oder -nachahmung umfassen. Dies hilft dabei, das Risiko von finanziellen Verlusten, Rufschädigung und unbefugtem Zugriff zu verringern.
- **Eine OT-relevante Anpassung sicherstellen**
  Identitätsprüfungsprozesse sollten an OT-Umgebungen angepasst werden, insbesondere wenn Techniker von Drittanbietern oder Mitarbeiter von Lieferanten Zugriff auf kritische Systeme benötigen.

PR.AA-02.2 Die Organisation stellt sicher, dass für jeden authentifizierten Benutzer, jedes Gerät und jeden Prozess, der mit den kritischen Systemen der Organisation interagiert, eindeutige Berechtigungsnachweise verwendet werden. Diese Berechtigungsnachweise müssen verifiziert werden, und die eindeutigen Kennungen müssen bei Systeminteraktionen erfasst werden. Ausnahmen können für den Zugang in Notfällen („Break-Glass"-Verfahren) gemacht werden, sofern dieser Zugang streng kontrolliert, protokolliert und überprüft wird.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass jeder Benutzer, jedes Gerät und jeder Prozess, der/das mit kritischen Systemen interagiert, eindeutig identifizierbar und authentifiziert ist. Dies unterstützt die Rechenschaftspflicht, die Rückverfolgbarkeit und den sicheren Zugang und ermöglicht gleichzeitig kontrollierte Ausnahmen in Notfällen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Eindeutige Berechtigungsnachweise zuweisen**
  Jeder Benutzer, jedes Gerät und jeder automatisierte Prozess sollte über eigene, eindeutige Berechtigungsnachweise verfügen. Gemeinsame Konten sollten vermieden werden. Alle Berechtigungsnachweise sollten verifiziert werden, bevor der Zugang gewährt wird.

- **Eine starke Authentifizierung implementieren**
  Die Multi-Faktor-Authentifizierung (MFA – PR.AA-03.2) muss, wo immer möglich, eingesetzt werden. Die Authentifizierungsmechanismen sollten gegen Replay-Angriffe und die Wiederverwendung von Berechtigungsnachweisen resistent sein. Diese Praktiken stehen im Einklang mit den ENISA-Leitlinien für sichere Benutzerauthentifizierung, die eine mehrschichtige und kontextbezogene Authentifizierung für kritische Systeme empfehlen.
- **Verfahren zur Verwaltung von Berechtigungsnachweisen durchsetzen**
  Passwortrichtlinien und die regelmäßige Änderung von Berechtigungsnachweisen sollten durchgesetzt werden. Die Berechtigungsnachweise sollten regelmäßig überprüft und aktualisiert werden, insbesondere nach einem Rollenwechsel oder dem Ausscheiden eines Mitarbeiters. Dies unterstützt die in den technischen NIS2-Implementierungsleitlinien der ENISA dargelegten Grundsätze, die ein sicheres Identitätslebenszyklusmanagement betonen.
- **Zugangskontrolle und -überwachung anwenden**
  Der Zugang sollte nach dem Prinzip des geringsten Privilegs erfolgen. Protokolle und Auditpfade sollten kontinuierlich überwacht werden, um Anomalien zu erkennen. Verdächtige Aktivitäten sollte umgehend untersucht werden.
- **Den Notfallzugang kontrollieren („Break-Glass“)**
  Der Notfallzugang sollte ausschließlich über festgelegte Break-Glass-Konten gewährt werden. Diese Konten sollten streng kontrolliert, zeitlich begrenzt, vollständig protokolliert und nach der Nutzung überprüft werden. Für jeden Fall sollten eine Begründung und eine Genehmigung erforderlich sein.
- **Bewusstsein und Schulung der Benutzer fördern**
  Das Personal sollte hinsichtlich der Bedeutung der Verwendung individueller Berechtigungsnachweise und der Meldung verdächtiger Zugriffe geschult werden. Das Bewusstsein sollte auch für die Risiken der gemeinsamen Nutzung und des Missbrauchs von Berechtigungsnachweisen geschärft werden.
- **Eine OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollten eindeutige Berechtigungsnachweise so implementiert werden, dass betriebliche Einschränkungen und Systembeschränkungen berücksichtigt werden. Eine Abstimmung mit den Ingenieurteams kann erforderlich sein.

PR.AA-03 Benutzer, Dienste und Hardware sind authentifiziert

PR.AA-03.1 Alle von der Organisation verwendeten drahtlosen Zugangspunkte, einschließlich derer, die Gastzugang bieten, werden sicher konfiguriert, verwaltet und überwacht, um unbefugten Zugang zu verhindern und die Netzintegrität zu gewährleisten.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle drahtlosen Zugangspunkte, einschließlich derjenigen für Gäste, sicher konfiguriert, verwaltet und überwacht werden, um unbefugten Zugriff zu verhindern und die Netzwerkintegrität zu schützen.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Allgemeine drahtlose Sicherheit**
  - Die Standard-Anmeldeinformationen für die Verwaltung sollten unmittelbar nach der Installation geändert werden.
  - Das SSID-Broadcasting sollte deaktiviert werden, es sei denn, es ist betrieblich notwendig.
  - Es sollten starke Verschlüsselungsprotokolle (z. B. WPA2 oder WPA3 mit AES) verwendet werden.
  - Der physische Zugang zu drahtlosen Zugangspunkten sollte eingeschränkt werden.
  - Firmware sollte regelmäßig aktualisiert werden, um bekannte Schwachstellen zu beheben.
  - Drahtlose Netzwerke sollten auf nicht autorisierte Zugangspunkte und verdächtige Aktivitäten überwacht werden.

- **Sicherheit des Gast-WLANs**
  - Gastnetzwerke sollten von internen Systemen durch VLANs oder separate SSIDs isoliert werden.
  - Für Gastnetzwerke sollten Bandbreiten- und Zugangsbeschränkungen angewendet werden.
  - Ungeschützte Portale sollten zur Anzeige von Nutzungsbedingungen und zur optionalen Protokollierung des Gastzugangs verwendet werden.
  - Sensible Daten sollten nicht über Gastnetzwerke gespeichert oder übertragen werden.
  - Wenn möglich, sollte das Gast-WLAN bei Nichtbenutzung oder außerhalb der Geschäftszeiten deaktiviert werden.
- **Endpunkt und Benutzerpraktiken**
  - Geräte, die sich mit drahtlosen Netzwerken verbinden, sollten die Sicherheitsrichtlinien für Endpunkte einhalten.
  - VPNs sollten verwendet werden, wenn eine Verbindung zu unbekannten oder ungesicherten Netzen hergestellt werden soll.
  - Für WLAN-Berechtigungsnachweise sollten Passwortrichtlinien gelten, die Komplexität und regelmäßige Aktualisierungen vorschreiben.

PR.AA-03.2 Für den Fernzugriff auf die Netzwerke der Organisation ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Netzwerke der Organisation zu schützen, indem für alle Fernzugriffe eine Multi-Faktor-Authentifizierung (MFA) verlangt wird, um so das Risiko eines unbefugten Zugriffs und von Angriffen mit Zugangsdaten zu verringern.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Allgemeine MFA-Durchsetzung**
  - MFA sollte auf allen Systemen mit Internetzugang durchgesetzt werden, einschließlich E-Mail, VPNs, RDP, Cloud-Services und Webportale.
  - Der gesamte Fernzugriff, einschließlich des Zugriffs von Drittanbietern und Subunternehmern, sollte MFA erfordern.
- **Auswahl der MFA-Technologie**
  - MFA-Methoden sollten auf der Grundlage von Sicherheitsstärke, Phishing-Resistenz und betrieblicher Eignung ausgewählt werden.
  - Zu den gängigen Optionen gehören:
    - Hardware TOTP (Time-based One-Time Password) Token – sicher, begrenzter Phishing-Schutz
    - Authenticator-Apps (Software TOTP) – weit verbreitet, mäßige Sicherheit
    - Passkeys – passwortlos, benutzerfreundlich, kryptographisch sicher
    - FIDO2 (plattform- oder hardwarebasiert – Fast Identity Online 2) – starke kryptografische Authentifizierung
    - Push-basierte Apps – praktisch, aber möglicherweise anfällig für Push-Müdigkeit
  - SMS- und E-Mail-basierte MFA sollte aufgrund von Sicherheitsmängeln vermieden werden.
- **Unterstützende Sicherheitsmaßnahmen**
  - Neben MFA sollten auch strenge Passwortrichtlinien durchgesetzt werden.
  - Die Benutzer sollten geschult werden, sich ausdrücklich von Sitzungen abzumelden.
  - Anti-Malware-Tools und -Plattformen sollten auf dem neuesten Stand gehalten werden.
  - Es sollten regelmäßig Schulungen zum Thema Phishing durchgeführt werden.
- **OT-spezifische MFA-Überlegungen** (*siehe auch PR.AA-01.1*)
  - **Gemeinsamer Zugriff auf PLCs/HMIs**
    - Wenn individuelle Konten nicht realisierbar sind, sollte das Prinzip der geringsten Privilegien angewendet werden.
    - Zur Zugriffskontrolle, Protokollierung von Aktivitäten und Hinzufügen einer Authentifizierungsebene sollte ein sicherer Jump-Server oder ein HMI-Frontend verwendet werden.

- **Sicherer Fernzugriff auf OT-Systeme**
  - Die technischen und verfahrenstechnischen Anforderungen für den Fernzugriff sollten klar definiert werden.
  - Es sollten sichere Protokolle (z. B. VPN, SSH, TLS) verwendet werden.
  - MFA sollte für alle OT-Fernzugänge, insbesondere für Drittanbieter, durchgesetzt werden.
  - Just-in-Time-Zugangskontrollen (JIT) sollten verwendet werden, um vorübergehenden, zeitlich begrenzten Zugang zu gewähren.
  - Alle Fernzugänge sollten protokolliert und überwacht werden.
- **Integration und Kompatibilität**
  - Die MFA-Lösung sollte sowohl mit IT- als auch mit OT-Systemen kompatibel sein.
  - Die Integration sollte in OT-Umgebungen getestet werden, um Unterbrechungen zu vermeiden.
  - Wo eine direkte Integration nicht möglich ist, sollten sichere Zwischenplattformen (z. B. Jump-Server) verwendet werden.

PR.AA-03.3 Die Organisation definiert, dokumentiert und implementiert Nutzungsbeschränkungen, Verbindungsanforderungen und Autorisierungsverfahren für den Fernzugriff auf ihre kritischen Systeme. Diese Kontrollen stellen sicher, dass nur zugelassene Benutzer über sichere Methoden eine Verbindung herstellen können und der Zugang auf das für ihre Rolle erforderliche Maß beschränkt ist.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass der Fernzugriff auf kritische Systeme durch definierte Nutzungsbeschränkungen, sichere Verbindungsmethoden und formelle Genehmigungsverfahren streng kontrolliert wird. Dies hilft, unbefugten Zugriff zu verhindern und die Anfälligkeit für Cyber-Bedrohungen zu verringern.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Nutzungsbeschränkungen festlegen**
  Identifizieren Sie, welche Systeme kritisch sind (z. B. OT-Systeme, Produktionsserver, Finanzdatenbanken). Legen Sie fest, wer per Fernzugriff auf sie zugreifen darf (z. B. bestimmte Rollen, Drittanbieter). Den Zugriff auf genehmigte Zeiträume beschränken und ihn auf die Systeme und Funktionen begrenzen, die für die Rolle des Benutzers erforderlich sind.
- **Sichere Verbindungsanforderungen festlegen**
  Der Fernzugriff sollte über sichere Methoden wie VPNs mit starker Verschlüsselung, TLS/SSH oder Jump-Server für OT-Umgebungen hergestellt werden. Jeder Fernzugriff sollte durch Multi-Faktor-Authentifizierung (MFA) gemäß PR.AA-03.2 geschützt sein. Geräte, die für den Fernzugriff verwendet werden, sollten die Anforderungen an die Endgerätesicherheit erfüllen (z. B. Antivirus, Patching).
- **Den Zugriff dokumentieren und genehmigen**
  Eine Richtlinie für den Fernzugriff sollte Antrags- und Genehmigungsverfahren, Rollen und technische Anforderungen definieren. Es sollte ein Register der Fernbenutzer geführt werden, das den Zugriffsbereich, die Genehmigungsdaten und die Überprüfungsfristen enthält.
- **Den Zugriff überwachen und überprüfen**
  Alle Fernzugriffe sollten protokolliert werden, wobei die Identität des Benutzers, die Uhrzeit, die Dauer und die Systeme, auf die zugegriffen wurde, erfasst werden sollten. Die Protokolle sollten regelmäßig auf Anomalien überprüft werden. Die Fernzugriffsberechtigungen und -konfigurationen sollten regelmäßig überprüft werden.
- **OT-spezifische Kontrollen anwenden**
  Bei OT-Systemen sollte der Zugriff über sichere Front-End-Schnittstellen oder Jump-Server erfolgen. Wenn gemeinsame Konten erforderlich sind (z. B. für SPS oder HMI), sollte der Zugriff protokolliert, zeitlich begrenzt und durch MFA auf Jump-Server-Ebene geschützt werden und dem Prinzip der geringsten Berechtigung folgen.
- **Sich an den ENISA-Leitlinien orientieren**
  Diese Vorgehensweisen stehen im Einklang mit den technischen Umsetzungsleitlinien der ENISA zu NIS2, die Richtlinien für einen sicheren Fernzugriff, starke Authentifizierung und eine kontinuierliche Überwachung als Teil des Managements von Cybersicherheitsrisiken für kritische Systeme empfehlen.

PR.AA-03.4 Der Fernzugriff auf die kritischen Systeme der Organisation wird überwacht und kryptographische Mechanismen werden implementiert, wenn dies notwendig ist.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass der Fernzugriff auf kritische Systeme nicht nur eingeschränkt und genehmigt wird (wie in PR.AA-03.3 definiert), sondern auch aktiv überwacht und durch kryptographische Mechanismen geschützt wird, um unbefugten Zugriff und Datenkompromittierung zu verhindern.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Fernzugriffsaktivitäten überwachen**
  Alle Fernzugriffssitzungen sollten protokolliert werden, wobei die Identität des Benutzers, die Uhrzeit, die Dauer und die aufgerufenen Systeme erfasst werden sollten. Überwachungstools sollten ungewöhnliche oder nicht autorisierte Zugriffsmuster erkennen und die Sicherheitsteams in Echtzeit alarmieren. Die Protokolle sollten regelmäßig überprüft und gemäß den Richtlinien aufbewahrt werden.
- **Kryptografische Schutzmaßnahmen anwenden**
  Fernverbindungen sollten starke Verschlüsselungsprotokolle wie TLS (Transport Layer Security), SSH (Secure Shell) oder IPsec verwenden. Daten, die während Fernsitzungen übertragen werden, sollten während der Übertragung verschlüsselt werden. Wird auf sensible Daten zugegriffen, sollte eine Ende-zu-Ende-Verschlüsselung in Betracht gezogen werden.
- **Die Zugriffsregeln aus PR.AA-03.3 durchsetzen**
  Die Überwachungs- und Verschlüsselungseinstellungen sollten die in PR.AA-03.3 definierten Zugriffsbeschränkungen widerspiegeln. Beispielsweise sollten Warnmeldungen bei Zugriffen außerhalb der Geschäftszeiten oder bei Versuchen, auf nicht autorisierte Systeme zuzugreifen, ausgelöst werden. Jeder Zugang sollte anhand dokumentierter Genehmigungen verifiziert werden.
- **Kontinuierliche Verbesserung unterstützen**
  Überwachungsdaten sollten verwendet werden, um Zugriffsrichtlinien zu verbessern, Lücken in der Durchsetzung zu identifizieren und die Reaktion auf Vorfälle zu unterstützen. Die kryptografischen Standards sollten regelmäßig überprüft werden, um sicherzustellen, dass sie den aktuellen bewährten Verfahren entsprechen.
- **Eine OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollten Überwachung und Verschlüsselung so implementiert werden, dass Systembeschränkungen und die Betriebskontinuität berücksichtigt werden. Zur zentralen Steuerung und Protokollierung sollten Jump-Server oder sichere Gateways eingesetzt werden.
- **Sich an den ENISA-Leitlinien orientieren**
  Diese Vorgehensweisen stehen im Einklang mit den technischen Umsetzungsleitlinien der ENISA zu NIS2, die einen sicheren Fernzugriff, die Verschlüsselung der Kommunikation und eine kontinuierliche Überwachung als Teil eines wirksamen Managements von Cybersicherheitsrisiken für kritische Systeme empfehlen.

PR.AA-03.5 Die Sicherheit von Verbindungen mit externen Systemen wird verifiziert und durch dokumentierte Vereinbarungen geregelt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Verbindungen mit externen Systemen durch verifiziert Sicherheitskontrollen gesichert sind und durch dokumentierte Vereinbarungen geregelt werden. Dadurch wird das Risiko eines unbefugten Zugriffs, eines Datenlecks und einer Beeinträchtigung der Lieferkette verringert.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Alle externen Interaktionen kontrollieren und dokumentieren**
  Alle Interaktionen zwischen internen Systemen und externen Parteien (z. B. Anbietern, Partnern, Cloud-Diensten) sollten identifiziert, kontrolliert und dokumentiert werden, um Rückverfolgbarkeit und Verantwortlichkeit zu gewährleisten.

- **Sicherheitskontrollen externer Parteien verifizieren**
  Bevor eine Verbindung hergestellt wird, sollte die Sicherheitslage des externen Anbieters durch Bewertungen Dritter, Audits, Zertifizierungen (z. B. CyFun®) oder technische Unterlagen wie M154 verifiziert werden. In diesen Dokumenten sollten Sicherheitsarchitektur, Zugangskontrollen, Verschlüsselung und Überwachung beschrieben werden.
- **Dokumentierte Vereinbarungen treffen**
  In formellen Vereinbarungen (z. B. Verträge, SLAs, DPAs) sollten Sicherheitsanforderungen, Rollen und Verantwortlichkeiten, Datenaustauschprotokolle, Verfahren zur Reaktion auf Zwischenfälle und Kündigungsbedingungen festgelegt werden.
- **Anforderungen an die Zugangskontrolle festlegen**
  Die Vereinbarungen sollten technische Beschränkungen wie IP-Whitelisting, rollenbasierte Zugangskontrolle, Regeln für den Umgang mit Daten und Verschlüsselungsanforderungen für Daten bei der Übertragung und im Ruhezustand enthalten.
- **Externe Verbindungen überwachen und überprüfen**
  Alle externen Verbindungen sollten kontinuierlich auf Anomalien oder Richtlinienverstöße überwacht werden. Die Vereinbarungen und technischen Unterlagen (z. B. M154) sollten regelmäßig überprüft und bei Bedarf aktualisiert werden. Jede Änderung in der Sicherheitslage des externen Systems sollte eine Neubewertung auslösen.
- **OT-spezifische Überlegungen sicherstellen**
  In OT-Umgebungen sollte der externe Zugang über sichere Gateways oder Jump-Server geleitet werden. Ein gemeinsamer Zugriff (z. B. für vom Anbieter verwaltete SPS) sollte protokolliert, zeitlich begrenzt und durch eine starke Authentifizierung geschützt werden.
- **Sich an den ENISA-Leitlinien orientieren**
  Diese Praktiken stehen im Einklang mit den technischen Umsetzungsleitlinien der ENISA für Maßnahmen zum Management von Cybersicherheitsrisiken, in denen empfohlen wird, die Sicherheit Dritter zu verifizieren, die Verantwortlichkeiten durch Verträge zu formalisieren und externe Abhängigkeiten kontinuierlich zu überwachen.

PR.AA-04 Identitätsbestätigungen werden geschützt, übermittelt und verifiziert

PR.AA-04.1 Identitätsbestätigungen sollen geschützt, übermittelt und verifiziert werden

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Identitätsbestätigungen – Behauptungen über die Identität eines Benutzers, Geräts oder Prozesses – vor Manipulationen geschützt, sicher übertragen und zuverlässig verifiziert werden, bevor der Zugriff auf kritische Systeme oder Daten gewährt wird.

Definition: Eine Identitätsbestätigung ist eine digitale Erklärung, die während der Authentifizierung verwendet wird und die Identität eines Benutzers, Geräts oder Prozesses bestätigt. Sie enthält in der Regel Informationen wie den Identitätsanbieter, die Authentifizierungsmethode und die Gültigkeitsdauer und wird verwendet, um Zugang zu Systemen oder Diensten zu gewähren.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Identitätsbestätigungen schützen**
  Identitätsbestätigungen sollten vor Manipulationen, Diebstahl oder Missbrauch geschützt werden. Es sollten eine starke Verschlüsselung (z. B. TLS 1.2 oder höher) und digitale Signaturen verwendet werden. Identitätsanbieter sollten die eIDAS-Verordnung einhalten (z. B. itsme®, SPID, FranceConnect). Diese Praktiken stehen im Einklang mit den ENISA-Leitlinien für digitale Identität und Vertrauensdienste.
- **Identitätsbestätigungen sicher übermitteln**
  Identitätsdaten sollten mit sicheren Protokollen wie SAML 2.0 oder OpenID Connect übertragen werden. Die Exposition von Token in URLs sollte vermieden werden; es sollten HTTP-Header oder POST-Methoden verwendet werden. Für die grenzüberschreitende Identitätsföderation sollten eIDAS-Knoten verwendet werden, um eine sichere Interoperabilität zwischen den EU-Mitgliedstaaten zu gewährleisten.

- **Überprüfung der Identitätsbestätigungen**
  Alle Bestätigungen sollten validiert werden, bevor Zugriff gewährt wird. Dazu gehören die Verifizierung digitaler Signaturen mit Hilfe vertrauenswürdiger Zertifizierungsstellen, die in der EU Trusted List (EUTL) aufgeführt sind, die Überprüfung von Token-Ansprüchen (Aussteller, Zielgruppe, Ablaufdatum) und die Validierung anhand von eIDAS-Metadaten. Für die Ausgabe und Verifizierung von Identitätsnachweisen sollten Qualified Trust Service Providers (QTSPs) herangezogen werden.
- **Sicherstellung der OT-spezifischen Machbarkeit**
  In OT-Umgebungen sollten Identitätsbestätigungen in sichere Zugangsgateways oder Jump-Server integriert werden. Wo eine direkte Integration nicht möglich ist, sollte die Identitätsverifizierung auf der Schnittstellenebene erfolgen, wobei eine Protokollierung und Überwachung vorgesehen ist.
- **Anpassung an die ENISA-Leitlinien**
  Diese Praktiken werden durch die technischen NIS2-Implementierungsleitlinien der ENISA und ihre Arbeit an sicheren digitalen Identitätsrahmen im Rahmen der eIDAS- und der europäischen Verordnung zur digitalen Identität unterstützt.

PR.AA-05 Zugriffsberechtigungen, Berechtigungen und Autorisierungen werden in einer Richtlinie definiert, verwaltet, durchgesetzt und überprüft und berücksichtigen die Prinzipien der geringsten Rechte und der Aufgabentrennung

PR.AA-05.1 Zugriffsberechtigungen, -rechte und -autorisierungen werden definiert, verwaltet, durchgesetzt und überprüft.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Zugriffsberechtigungen, Rechte und Autorisierungen klar definiert, ordnungsgemäß verwaltet, konsequent durchgesetzt und regelmäßig überprüft werden, um Systeme und Daten vor unbefugtem Zugriff zu schützen.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Definition und Verwaltung des Zugangs**
  - Es sollten Zugriffslisten für Systeme (z. B. Dateien, Server, Software, Datenbanken) erstellt und regelmäßig überprüft werden.
  - Die Überprüfungen sollten durch Tools wie die Active Directory-Analyse unterstützt werden.
  - Die Verfahren zur Verwaltung von Genehmigungen sollten dokumentiert und bei Bedarf aktualisiert werden.
- **Überprüfung und Entzug des Zugangs**
  - Logische und physische Zugriffsrechte sollten regelmäßig und immer dann überprüft werden, wenn sich Rollen ändern oder Personen die Organisation verlassen.
  - Unnötige Privilegien sollten sofort entzogen werden.
- **Praktiken für Benutzerkonten**
  - Jeder Benutzer, einschließlich Subunternehmer, sollte ein eigenes Konto haben, um die Rechenschaft zu gewährleisten.
  - Soweit technisch machbar, sollten geeignete Authentifizierungsmaßnahmen angewandt werden.
  - Gastkonten sollten auf die erforderlichen Mindestrechte beschränkt sein (z. B. nur Internetzugang).
  - Wo es angebracht ist, sollte Single Sign-On (SSO) verwendet werden.
- **Autorisierungskriterien**
  Bei Autorisierungsentscheidungen sollten Merkmale wie Geolokalisierung, Zugriffszeitpunkt und Sicherheitsstatus des anfragenden Geräts berücksichtigt werden.

- **OT-spezifische Überlegungen**
  - In Umgebungen, in denen individuelle Konten technisch nicht realisierbar sind – wie z. B. bei gemeinsamem Zugriff auf SPS oder HMI – sollte der Zugriff auf wesentliche Funktionen beschränkt und durch sichere Methoden wie einen Jump-Server oder ein HMI-Frontend erzwungen werden, das Aktivitäten protokolliert, den Zugriff nach Rolle oder Zeit einschränkt und eine zusätzliche Authentifizierungsebene (z. B. Badge oder PIN) zufügt.
  - Die Authentifizierungsmethoden sollten auf die Fähigkeiten der OT-Systeme abgestimmt sein.
  - Der Zugang zu OT-Systemen sollte nach Möglichkeit protokolliert und überwacht werden.

PR.AA-05.2 Es ist festzulegen, wer Zugang zu den geschäftskritischen Informationen und Technologien der Organisation benötigt und wie der Zugang gewährt werden kann.

Implementierungshinweise

Ziel dieser Kontrolle ist es, zu bestimmen, wer Zugang zu den geschäftskritischen Informationen und Technologien der Organisation benötigt, und die sicheren Mittel zu definieren, mit denen dieser Zugang gewährt wird.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Zugangsbestimmung und -beschränkung**
  - Die Zugriffsrechte sollten auf die Personen beschränkt werden, die sie zur Erfüllung ihrer Aufgaben benötigen.
  - Ein Null-Vertrauensmodell sollte sowohl für IT- als auch für OT-Umgebungen in Betracht gezogen werden, wobei vor der Gewährung des Zugangs eine Verifizierung erforderlich ist.
- **Zugangsmittel**
  - Die Zugriffsmethoden sollten sichere Mechanismen wie Schlüssel, Passwörter, Codes oder administrative Berechtigungen umfassen.
  - Diese Methoden sollten verwaltet und überwacht werden, um Missbrauch zu verhindern.
- **Cyber-Gesundheit von Endpunkten**
  - Geräte wie Laptops, Smartphones und Tablets sollten Sicherheitsstandards erfüllen, bevor sie mit dem Produktionsnetzwerk verbunden werden.
  - Der Zustand des Endpunkts sollte durch Überprüfung von Folgendem verifiziert werden:
    - Aktuelle Antiviren-Software
    - Abwesenheit von Malware
    - Installation der neuesten Sicherheitspatches
  - Nur regelkonforme Geräte sollten Zugriff auf kritische Systeme und Daten erhalten.
- **OT-spezifische Überlegungen**
  - In OT-Umgebungen sollte der Zugang zu Kontrollsystemen auf die notwendigen Mitarbeiter beschränkt sein.
  - Sichere Zugriffsmethoden (z. B. Jump-Server, rollenbasierte Einschränkungen) sollten verwendet werden, wenn individuelle Konten nicht realisierbar sind.
- **Referenz**
  Praktische Hilfsmittel und Vorlagen finden Sie in der Vorlage für Zugangsrichtlinien in der CyFun® Toolbox auf www.cyfun.eu

PR.AA-05.3 Zugriffsrechte, Privilegien und Berechtigungen sind auf die Systeme und spezifischen Informationen beschränkt, die für die Erfüllung der Aufgaben erforderlich sind (Grundsatz des geringsten Privilegs).

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Zugriffsrechte, Privilegien und Berechtigungen gemäß dem Prinzip der geringsten Privilegien auf die Systeme und spezifischen Informationen beschränkt sind, die zur Erfüllung der zugewiesenen Aufgaben erforderlich sind.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Anwendung des Prinzips der geringsten Privilegien**
  - Die Zugriffsrechte sollten auf das für Benutzer, Systeme und Services erforderliche Minimum beschränkt werden.
  - Konten sollten mit wenigen Berechtigungen beginnen und nur in begründeten Fällen erweitert werden.
  - Der Just-in-Time-Zugang sollte genutzt werden, um die Dauer erhöhter Privilegien zu begrenzen.
- **Definition und Verwaltung von Berechtigungen**
  - Die Zugriffsrechte sollten auf der Grundlage von Rollen und Verantwortlichkeiten klar definiert werden.
  - Es sollte ein Verzeichnis der Konten und ihrer Berechtigungen geführt und auf dem neuesten Stand gehalten werden.
  - Für Subunternehmer und Drittparteien sollten getrennte Konten verwendet werden, um die Rückverfolgbarkeit zu gewährleisten.
- **Durchsetzung von Zugangskontrollen**
  - Wo es möglich ist, sollten rollen- oder attributbasierte Zugangskontrollmodelle implementiert werden.
  - Internet-Zugangspunkte und externe Verbindungen sollten auf das unbedingt Notwendige beschränkt werden.
- **Sicherung von Systemen**
  Systeme sollten so gesichert werden, dass sie die Zugriffskontrolle unterstützen, und zwar durch:
  - Deaktivierung ungenutzter Ports und Services
  - Einschränkung von Bluetooth, wo es nicht benötigt wird
  - Begrenzung von Legacy-Protokollen wie FTP, sofern diese nicht sicher konfiguriert sind
- **Überprüfung und Anpassung des Zugangs**
  - Die Zugriffsrechte sollten regelmäßig überprüft und aufgrund von Rollenänderungen, Projektabschluss oder Sicherheitsbewertungen angepasst werden.
  - Der Zugang sollte sofort widerrufen werden, wenn er nicht mehr benötigt wird.
- **OT-spezifische Überlegungen**
  In OT-Umgebungen sollte die Zugangskontrolle weiter dem Prinzip der geringsten Rechte folgen. Wo technische Beschränkungen bestehen, sollten die zuvor definierten OT-Zugangskontrollmaßnahmen (siehe PR.AA-01.1 und PR.AA-05.1) angewendet werden, um einen sicheren und nachvollziehbaren Zugang zu gewährleisten.

PR.AA-05.4 Niemand hat Verwaltungsrechte für alltägliche Aufgaben.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Nutzung administrativer Rechte für routinemäßige, alltägliche Aufgaben zu verhindern und so das Risiko des Missbrauchs oder der Ausnutzung durch Angreifer zu verringern.

Um sicherzustellen, dass dieses Ziel erreicht wird, sollte die Organisation Folgendes berücksichtigen:

- **Kontentrennung und Privilegienverwaltung**
  - Administrative und allgemeine Benutzerkonten sollten strikt getrennt werden.
  - Dedizierte Administratorkonten sollten nur für die Systemverwaltung und administrative Aufgaben verwendet werden.
  - Benutzerkonten sollten keine administrativen Berechtigungen haben.
- **Zugangsbeschränkungen und Sicherheitsmaßnahmen**
  - Für jedes System sollten eindeutige lokale Administratorkennwörter erstellt werden.
  - Nicht genutzte Konten sollten umgehend deaktiviert werden.
  - Das Surfen im Internet von administrativen Konten aus sollte verboten werden, um die Anfälligkeit für webbasierte Bedrohungen zu verringern.
- **OT-spezifische Überlegungen**
  - In OT-Umgebungen sollte der administrative Zugriff auf die notwendigen Mitarbeiter und die erforderlichen Funktionen beschränkt werden.
  - Wo ein gemeinsamer Zugriff erforderlich ist, sollten sichere Zugriffsmethoden (z. B. Jump-Server, Sitzungsprotokollierung) verwendet werden, um die Rechenschaftspflicht durchzusetzen und das Risiko zu verringern.

PR.AA-05.5 **Sofern dies technisch, betrieblich und wirtschaftlich machbar ist – ohne die Systemintegrität, Sicherheit oder Compliance zu beeinträchtigen –, werden automatisierte Mechanismen zur Verwaltung von Benutzerkonten auf kritischen IKT- und OT-Systemen implementiert. Die Durchführbarkeit wird auf der Grundlage der Systemkapazitäten, des Integrationspotenzials, der Risikobewertung und der geschäftlichen Auswirkungen bestimmt.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Benutzerkonten auf kritischen IKT- und OT-Systemen durch automatisierte Mechanismen – soweit dies technisch, betrieblich und wirtschaftlich machbar ist – sicher, effizient und konsistent verwaltet werden, ohne die Systemintegrität, Sicherheit oder Compliance zu beeinträchtigen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Durchführbarkeit von Automatisierung bewerten**
  Die Durchführbarkeit sollte auf den Systemkapazitäten, dem Integrationspotenzial, der Risikobewertung und der geschäftlichen Auswirkungen basieren.
  - Bei **IKT-Systemen** hängt die Durchführbarkeit von der Verfügbarkeit von Automatisierungswerkzeugen, APIs oder Integrationsoptionen sowie vom Fehlen größerer technischer oder finanzieller Hindernisse ab.
  - Bei **OT-Systemen** hängt die Durchführbarkeit vom Alter des Systems, den Einschränkungen des Anbieters, den Sicherheitsanforderungen und dem Risiko einer Unterbrechung des kritischen Betriebs ab.
  - Bei der allgemeinen Durchführbarkeit sollten die technische Leistungsfähigkeit, die Betriebssicherheit, die Kostenwirksamkeit und die Einhaltung der Sicherheits- und Regulierungsstandards berücksichtigt werden.
- **Das Lebenszyklusmanagement von Konten automatisieren**
  Automatisierte Mechanismen sollten die Erstellung, Änderung und Löschung von Konten auf der Grundlage vordefinierter Regeln verwalten. Dadurch wird sichergestellt, dass nur befugte Benutzer Zugang haben und dass Konten umgehend gelöscht werden, wenn sie nicht mehr benötigt werden.
- **Inaktive oder nicht autorisierte Konten deaktivieren**
  Konten sollten automatisch deaktiviert werden, wenn Benutzer die Organisation verlassen oder keinen Zugang mehr benötigen. Dadurch wird das Risiko eines unbefugten Zugriffs auf kritische Systeme verringert.
- **Kontoaktivitäten überwachen und melden**
  Automatisierte Tools sollten die Kontonutzung kontinuierlich überwachen und Berichte erstellen, um ungewöhnliche oder unzulässige Aktivitäten zu erkennen. Bei verdächtigem Verhalten sollten Warnmeldungen ausgelöst werden.
- **Benachrichtigung bei wichtigen Ereignissen senden**
  Automatisierte Benachrichtigungen sollten Administratoren über wichtige Ereignisse wie die Erstellung, Änderung oder Löschung von Konten informieren, um eine rechtzeitige Kontrolle zu ermöglichen.
- **Audit-Trails zur Einhaltung von Vorschriften führen**
  Alle kontobezogenen Aktivitäten sollten automatisch protokolliert werden, um die Einhaltung von internen Richtlinien und externen Vorschriften zu unterstützen.
- **OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollte die Automatisierung nur dort implementiert werden, wo sie die Sicherheit oder Betriebskontinuität nicht beeinträchtigt. Wo eine direkte Automatisierung nicht möglich ist, sollte die Kontoverwaltung über sichere Schnittstellenschichten oder Jump-Server erfolgen.
- **Sich an den ENISA-Leitlinien orientieren**
  Diese Praktiken werden von den technischen NIS2-Implementierungsleitlinien der ENISA und ihrer Arbeit zum sicheren Zugangsmanagement in kritischen Infrastrukturumgebungen unterstützt.

PR.AA-05.6 Bei der Verwaltung von Zugriffsrechten wird eine Aufgabentrennung (SoD) gewährleistet.

Implementierungshinweise

Das Ziel dieser Kontrolle ist es, sicherzustellen, dass keine einzelne Person die volle Kontrolle über kritische Systeme oder Prozesse hat, indem die Trennung der Aufgaben (Separation of Duties - SoD) durchgesetzt wird. Dies sollte das Risiko von Fehlern, Betrug und Missbrauch von Zugangsrechten verringern.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Aufgabentrennung definieren**
  Die Zuständigkeiten sollten so verteilt werden, dass die wichtigsten Aufgaben von verschiedenen Personen wahrgenommen werden.
  SoD sollte Folgendes umfassen:
  - Operative und systemunterstützende Aufgaben sollten unterschiedlichen Personen zugewiesen werden.
  - Systemunterstützende Aufgaben sollten eine Aufsicht oder ein Vier-Augen-Prinzip erfordern.
  - Eine einzelne Person sollte nicht ein und dieselbe Transaktion veranlassen und genehmigen.
  - Zugangskontroll- und Auditfunktionen sollten von separaten Rollen wahrgenommen werden.
- **Zugriffsrechte angemessen verwalten**
  - Die rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC) sollte für die Zuweisung von Berechtigungen auf der Grundlage von Jobrollen verwendet werden.
  - Der Grundsatz des geringsten Privilegs sollte angewandt werden, um den Zugang auf das absolut Notwendige zu beschränken.
  - Die Zugriffsrechte sollten regelmäßig überprüft werden, insbesondere für kritische Systeme und Rollen mit hohem Risiko.
  - Für Verwaltungs- und Prüfungsfunktionen sollten nach Möglichkeit getrennte Tools oder Konten verwendet werden.
- **Kontrollen für Systemadministratoren anwenden**
  - Die administrativen Zuständigkeiten sollten aufgeteilt werden, um eine vollständige Kontrolle durch eine einzige Person zu verhindern.
  - Administratoren sollten getrennte Konten für reguläre und privilegierte Aufgaben verwenden.
  - Alle administrativen Maßnahmen sollten protokolliert und von einer unabhängigen Stelle überprüft werden.
  - Administratoren, die den Zugang verwalten, sollten nicht für die Prüfung dieses Zugangs verantwortlich sein.
- **Die Durchführbarkeit in OT-Umgebungen sicherstellen**
  - In OT-Systemen sollte SoD an betriebliche und sicherheitstechnische Zwänge angepasst werden.
  - Wenn eine vollständige Trennung nicht möglich ist, sollten kompensierende Kontrollen wie eine doppelte Genehmigung, Protokollierung und externe Überprüfung implementiert werden.
- **Sich an den ENISA-Leitlinien orientieren**
  Diese Praktiken stehen im Einklang mit den ENISA-Sicherheitsmaßnahmen für Betreiber grundlegender Services, die die Bedeutung der Aufgabentrennung (Separation of Duties, SoD) und der rollenbasierten Zugangskontrolle (Role-Based Access Control, RBAC) bei der Verringerung von zugangsbezogenen Risiken in IKT- und OT-Umgebungen hervorheben.

PR.AA-05.7 Privilegierte Benutzer werden verwaltet und überwacht.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko eines unbefugten Zugriffs, von Datenschutzverletzungen und Betriebsunterbrechungen zu verringern, indem sichergestellt wird, dass privilegierte Benutzer, die über einen erweiterten Zugriff auf kritische Systeme verfügen, einer strengen Verwaltung und ständigen Überwachung unterworfen sind.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Privilegierte Aktivitäten überwachen**
  Aktivitäten privilegierter Benutzer sollten routinemäßig oder kontinuierlich protokolliert und überprüft werden, auch wenn sie von Personen durchgeführt werden, die nicht unabhängig vom Prozess sind.
- **Sensible Daten schützen**
  Die Überwachung soll verhindern, dass privilegierte Benutzer sensible Informationen und Systemkonfigurationen preisgeben oder missbrauchen.
- **Missbrauch von Privilegien verhindern**
  Privilegierte Konten sollten so verwaltet werden, dass unbefugte Änderungen, die Ausweitung von Privilegien oder die Umgehung von Sicherheitskontrollen vermieden werden.
- **Verdächtige Verhaltensweisen erkennen**
  Verhaltensanomalien und unbefugte Handlungen sollten durch automatische Protokollierungs- und Warnmechanismen erkannt werden.
- **Die Reaktion auf Vorfälle unterstützen**
  Die Überwachungsdaten sollten zur Untersuchung von und Reaktion auf Sicherheitsvorfälle mit privilegierten Konten verwendet werden.
- **Zugriffsrechte proaktiv verwalten**
  Zugriffsrechte sollten klar definiert, regelmäßig überprüft und auf der Grundlage von Rollenänderungen, betrieblichen Anforderungen oder Risikobewertungen angepasst werden.
- **OT-spezifische Durchführbarkeit sicherstellen**
  In OT-Umgebungen sollte der privilegierte Zugriff unter Berücksichtigung der Systemstabilität und -sicherheit verwaltet werden. Wo eine vollständige Überwachung nicht möglich ist, sollten kompensierende Kontrollen wie die Protokollierung[1] auf Schnittstellenebene oder eine externe Überprüfung implementiert werden.
- **Mit den ENISA-Leitlinien übereinstimmen**
  Diese Praktiken stimmen mit den technischen Umsetzungsleitlinien der ENISA zu NIS2 überein, in denen die Bedeutung der privilegierten Zugriffskontrolle und -überwachung für die Sicherung wesentlicher Services und kritischer Infrastrukturen hervorgehoben wird.

PR.AA-05.8 Kontennutzungsbeschränkungen für bestimmte Zeiträume und Orte werden in der Sicherheitszugangsrichtlinie der Organisation berücksichtigt und entsprechend angewendet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko eines unbefugten Zugriffs zu verringern, indem sichergestellt wird, dass die Kontonutzung je nach Zeit, Standort, Gerät und Benutzerkontext eingeschränkt wird. Diese Beschränkungen sollten in den Sicherheitszugangsrichtlinien der Organisation festgelegt und in allen IKT- und OT-Umgebungen einheitlich angewendet werden.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Zeitlich begrenzte Beschränkungen anwenden**
  - Der Zugang zu den Systemen sollte auf bestimmte Arbeitszeiten beschränkt werden, um die Exposition außerhalb der Arbeitszeiten zu verringern.
  - Die Nutzungsdauer für bestimmte Konten sollte begrenzt werden, um übermäßige oder unbeaufsichtigte Sitzungen zu verhindern.
- **Standortbasierte Beschränkungen anwenden**
  - Geofencing sollte eingesetzt werden, um den Zugriff nur von vertrauenswürdigen geografischen Standorten aus zu ermöglichen.
  - Die IP-Adressfilterung sollte den Zugang auf bekannte und genehmigte Netzbereiche beschränken.

1 Protokollierung auf Schnittstellenebene bedeutet, dass aufgezeichnet wird, was Benutzer an dem Punkt tun, an dem sie sich mit einem System verbinden, z. B. über ein Fernzugriffstool, einen Jump Server oder ein sicheres Gateway, ohne dass eine direkte Protokollierung im System selbst erforderlich ist (z. B. mit Splunk®). Dies hilft bei der Überwachung privilegierter Aktivitäten in Umgebungen, in denen eine direkte Systemprotokollierung nicht möglich ist, wie z. B. in OT-Systemen.

- **Gerätebasierte Beschränkungen anwenden**
  - Der Zugang sollte nur von verwalteten Geräten aus gestattet werden, die den Sicherheitsrichtlinien der Organistaion entsprechen.
  - Nicht verwaltete Geräte sollten eingeschränkt werden oder nur begrenzten Zugriff erhalten (z. B. nur Lesezugriff oder kein Zugriff auf sensible Daten).
- **Nutzerbasierte Beschränkungen anwenden**
  - Role-Based Access Control (RBAC) sollte sicherstellen, dass Benutzer nur auf Systeme und Daten zugreifen, die für ihre Arbeit relevant sind.
  - Richtlinien für den bedingten Zugang sollten in Hochrisikoszenarien eine zusätzliche Verfizierung (z. B. Multi-Faktor-Authentifizierung) erfordern.
  - Continuous Adaptive Risk and Trust Assessment (CARTA) sollte in Betracht gezogen werden, um das Vertrauen von Benutzern und Geräten dynamisch zu bewerten. Dieser Ansatz steht im Einklang mit dem Zero-Trust-Prinzip, bei dem kein implizites Vertrauen für einen Benutzer oder ein Gerät vorausgesetzt wird, auch nicht innerhalb des Netzes.
- **OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollten die Beschränkungen an die Betriebs- und Sicherheitsanforderungen angepasst werden. Wo technische Beschränkungen bestehen, sollten kompensierende Kontrollen wie physische Zugangsbeschränkungen oder überwachte Jump-Server implementiert werden.
- **Sich an den ENISA-Leitlinien ausrichten**
  Diese Vorgehensweisen stehen im Einklang mit den technischen Umsetzungsleitlinien der ENISA zu NIS2, die kontextbezogene Zugriffskontrollen als Teil eines wirksamen Managements von Cybersicherheitsrisiken unterstützen.

PR.AA-05.9 Privilegierte Benutzer werden verwaltet, überwacht und auditiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass privilegierte Benutzerkonten, d. h. solche mit erweitertem Zugriff auf kritische Systeme, streng kontrolliert, kontinuierlich überwacht und unabhängig auditiert werden. Dies sollte das Risiko des Missbrauchs verringern, die Rechenschaftspflicht sicherstellen und kritische Umgebungen der Informationstechnologie (IT), der Betriebstechnologie (OT) und des Internets der Dinge (IoT) schützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Starkes Privileged Access Management durchsetzen**
  Privilegierte Konten sollten klar definierte Rollen und einen begrenzten Zugriffsbereich haben und regelmäßigen Zugriffsüberprüfungen unterliegen.
- **Kontinuierliche Überwachung einführen**
  Alle Aktivitäten privilegierter Benutzer sollten protokolliert und kontinuierlich überwacht werden, wobei nach Möglichkeit automatisierte Tools eingesetzt werden sollten, um die Rückverfolgbarkeit und die Reaktion auf Vorfälle zu unterstützen.
- **Unabhängige Audits durchführen**
  - Audits sollten in regelmäßigen Abständen von Personen durchgeführt werden, die vom Zugangsmanagementprozess unabhängig sind.
  - Audits sollten:
    - Verifizieren, ob privilegierter Zugriff gemäß den Richtlinien gewährt wird.
    - Bestätigen, dass die Überwachungs- und Protokollierungsmechanismen korrekt funktionieren.
    - Missbrauch, Richtlinienverstöße oder Abweichungen identifizieren.
    - Dokumentierte Ergebnisse wie Auditberichte oder Pläne für Abhilfemaßnahmen erstellen.
- **Das Vier-Augen-Prinzip anwenden**
  Keine einzelne Person sollte in der Lage sein, privilegierten Zugang zu gewähren, zu ändern oder zu widerrufen, ohne dass eine andere befugte Person dies beaufsichtigt oder genehmigt.
- **Zwischen Überwachung und Audit unterscheiden**
  - Die tägliche Überwachung der Einhaltung der Vorschriften sollte sich auf betriebliche Aspekte (z. B. Warnmeldungen, Anomalien) konzentrieren.
  - Regelmäßige Audits sollten die allgemeine Effektivität und Integrität des Prozesses zur Verwaltung des privilegierten Zugangs bewerten.

- **OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollten privilegierte Zugriffskontrollen an betriebliche und sicherheitstechnische Einschränkungen angepasst werden. Wo ein vollständiges Audit nicht möglich ist, sollten kompensierende Kontrollen wie die Protokollierung auf Schnittstellenebene oder eine externe Überprüfung durchgeführt werden.
- **Sich an den ENISA-Leitlinien ausrichten**
  Diese Praktiken sollten mit den ENISA-Leitlinien für die technische Umsetzung von NIS2 übereinstimmen, in denen die Bedeutung der Kontrolle des privilegierten Zugangs, der Überwachung und von Audits für die Sicherung wesentlicher Services und kritischer Infrastrukturen hervorgehoben wird.

PR.AA-06 Der physische Zugang zu Vermögenswerten wird risikoadäquat verwaltet, überwacht und durchgesetzt

PR.AA-06.1 Der physische Zugang zu allen Einrichtungen der Organisation, einschließlich kritischer Bereiche, soll risikobasiert verwaltet, überwacht und durchgesetzt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass der physische Zugang zu allen Ressourcen der Organisation, insbesondere in kritischen Bereichen, risikobasiert verwaltet, überwacht und durchgesetzt wird, um unbefugte Zugriffe zu verhindern und sensible Systeme zu schützen.

Um dieses Ziel zu unterstützen, sollten die folgenden Maßnahmen angewendet werden:

- **Maßnahmen zur Zugangskontrolle**
  - Schlüssel, Badges und Alarmcodes sollten streng verwaltet werden.
  - Die Zugangsdaten der Mitarbeiter sollten unmittelbar nach dem Ausscheiden aus der Organisation eingezogen werden.
  - Die Alarmcodes sollten regelmäßig geändert werden.
  - Externe Dienstleister (z. B. Reinigungskräfte) sollten nur dann Zugang erhalten, wenn dies erforderlich ist und dieser sollte:
    - Durch technische Kontrollen zeitlich begrenzt sein
    - Für Rückverfolgbarkeit elektronisch protokolliert sein
- **Physische Sicherheitsverbesserungen**
  - Kritische Zonen sollten durch physische Kontrollen geschützt werden, z. B:
    - Überwachungskameras
    - Sicherheitspersonal
    - Verschlossene Türen und Tore
    - Alarmanlagen
  - Diese Kontrollen sollten strategisch platziert werden, um den Zugang zu überwachen und zu beschränken.
- **Schutz des Netzwerkzugriffs**
  Interne Netzwerkanschlüsse (z. B. Ethernet) sollten nicht in ungesicherten Bereichen wie Wartezimmern, Korridoren oder Empfangsbereichen offen liegen.
- **OT-spezifische Überlegungen**
  - Der physische Zugang zu OT-Umgebungen (z. B. Kontrollräume, Schränke, Feldgeräte) sollte auf befugte Mitarbeiter beschränkt sein.
  - Der Zugang sollte protokolliert und überwacht werden, und wenn möglich, sollten physische Barrieren eingesetzt werden.
- **Referenz**
  Praktische Hilfsmittel und Vorlagen finden Sie in der Zugangsrichtlinien in der CyFun® Toolbox auf www.cyfun.eu.

PR.AA-06.2 **Physikalische Zugangskontrollen sollen spezielle Verfahren für Notfallsituationen beinhalten, die einen kontinuierlichen Schutz kritischer und nicht-kritischer Vermögenswerte während solcher Ereignisse gewährleisten.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass physische Zugangskontrollen in Notfällen wirksam und anpassungsfähig bleiben. Dazu gehört die Aufrechterhaltung der Sicherheit kritischer und nicht-kritischer Vermögenswerte bei gleichzeitiger Ermöglichung eines sicheren, autorisierten und nachvollziehbaren Zugangs für Notfallmaßnahmen, Wiederherstellung oder Eindämmung – insbesondere in Umgebungen, in denen physische und betriebliche Sicherheit eng miteinander verbunden sind, wie z. B. bei Systemen der Betriebstechnologie (OT) und des Internets der Dinge (IoT).

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Notfallszenarien definieren**
  Notfallverfahren sollten eine Reihe von Ereignissen abdecken, darunter:
  - Umwelt- und Sicherheitsvorfälle (z. B. Feuer, Überschwemmung, medizinische Notfälle, Evakuierungen)
  - Infrastrukturausfälle (z. B. Stromausfälle, Systemstörungen)
  - Sicherheitsvorfälle (z. B. Einbrüche, Versagen der Zugangskontrolle)
  - Cybersecurity-Ereignisse (z. B. Ransomware, Datenschutzverletzungen, Insider-Bedrohungen)
- **Über Zugangsverfahren für Notfälle verfügen**
  Der Zugang für Notfälle sollte:
  - Protokolliert sein: Halten Sie fest, wer wann und warum auf welche Daten zugegriffen hat.
  - Überwacht sein: Verwenden Sie Überwachungs- oder Zugangskontrollsysteme, um Aktivitäten zu verfolgen.
  - Überprüft sein: Führen Sie nachträgliche Überprüfungen durch, um die ordnungsgemäße Verwendung zu verifizieren und Missbrauch zu erkennen.
- **Die Notfallbereitschaft durch physische Kontrollen unterstützen**
  - Es sollten aktuelle Listen der befugten Personen mit Zugangsrechten für Notfälle geführt werden.
  - Es sollten Identitätsnachweise (z. B. Zugangsausweise) verwendet und Sicherheitszonen festgelegt werden.
  - Für Besucher oder Zeitarbeitskräfte sollten Begleitpersonen eingesetzt werden.
  - Es sollten physische Barrieren wie Zäune, Schleusen, Drehkreuze und personell besetzte Kontrollpunkte eingerichtet werden.
  - Es sollten Überwachungssysteme eingesetzt werden, um die Ein- und Ausgänge zu kontrollieren.
- **Zusätzliche Sicherheitsvorkehrungen anwenden**
  - Ausweissysteme mit differenzierten Zugangsstufen für verschiedene Zonen sollten in Betracht gezogen werden.
  - Der physische Zugang zu Servern und Netzkomponenten sollte nur befugten Mitarbeitern vorbehalten sein.
  - Jeder Zugang zu kritischen Infrastrukturen sollte protokolliert und regelmäßig überprüft werden.
  - Führen und Überprüfen – Die Aufzeichnungen über den Zugang von Besuchern sollten geführt und überprüft werden. Falls erforderlich, sollten Korrekturmaßnahmen ergriffen werden.
- **OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollten die Verfahren für den physischen Zugang angepasst werden, um eine Störung der Sicherheit oder der Betriebskontinuität zu vermeiden. Der Zugang für Notfälle sollte so gestaltet sein, dass sowohl eine schnelle Reaktion als auch der Schutz von Vermögenswerten möglich ist.
- **Sich an den ENISA-Leitlinien orientieren**
  Diese Praktiken stehen im Einklang mit den ENISA-Leitlinien für die technische Umsetzung von NIS2, in denen die Bedeutung von physischen und logischen Zugangskontrollen für die Aufrechterhaltung der Resilienz in Notfällen hervorgehoben wird.

PR.AA-06.3 Kritische Bereiche sollen über die für allgemeine Einrichtungen geltenden Maßnahmen hinaus mit zusätzlichen physischen Zugangskontrollen ausgestattet sein.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko des unbefugten physischen Zugangs zu Bereichen, die für die Betriebskontinuität, die Datenintegrität und die Sicherheit von Mitarbeitern und Ausrüstung wichtig sind, zu verringern, indem strengere Zugangsmaßnahmen als in den allgemeinen Anlagenbereichen angewandt werden.

Um dieses Ziel zu erreichen, sollten die folgenden Maßnahmen angewendet werden:

- **Bei der Klassifizierung von Vermögenswerten sollten kritische Bereiche identifiziert werden. Dazu gehören in der Regel:**
  - Umgebungen für Produktion und Betriebstechnik (OT)
  - Serverräume und Rechenzentren
  - Büros der Finanz- und Personalabteilung
  - Kontrollräume
  - Standorte, an denen sensible oder klassifizierte Informationen aufbewahrt werden
- **Die folgenden verbesserten physischen Zugangskontrollen sollten in Betracht gezogen werden:**
  - Zwei-Faktor-Authentifizierung (z. B. Ausweis + Biometrie)
  - Kontinuierliche Überwachung (z. B. CCTV, Bewegungsmelder)
  - Zugangsprotokollierung mit regelmäßiger Überprüfung
  - Sicherheitspersonal vor Ort oder auf Patrouille
  - Alarmsysteme mit Echtzeitwarnungen
  - Verfahren zur Besucherverwaltung
  - Vorabgenehmigung und Begleitung
  - Zeitlich begrenzter Zugang
  - Besucherprotokolle
- **Stellen Sie die Konsistenz mit umfassenderen Richtlinien für den physischen Zugang sicher, darunter:**
  - PR.AA-06.1 – Risikobasierte Zugangskontrolle
  - PR.AA-06.2 – Zugangsverfahren für Notfälle
  - PR.AA-06.4 – Physischer Schutz von Vermögenswerten
- **Passen Sie die Kontrollen an die Kritikalität der einzelnen Zonen an und integrieren Sie sie in die Gesamtstrategie für die physische Sicherheit.**

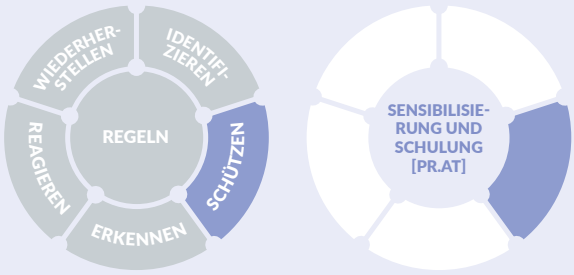
PR.AA-06.4 **Vermögenswerte, die sich in kritischen Zonen befinden, sollen physisch gegen unbefugten Zugang, Beschädigung oder Störung geschützt werden.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, wesentliche Vermögenswerte, die sich in kritischen Zonen befinden, durch maßgeschneiderte physische Schutzmaßnahmen vor nicht autorisiertem Zugang, Beschädigung oder Störung zu schützen, unabhängig davon, ob dies absichtlich oder zufällig geschieht.

Um dieses Ziel zu erreichen, sollten folgende Maßnahmen berücksichtigt werden:

- Vermögenswerte in kritischen Zonen sollten je nach ihrer Kritikalität und ihrem Risikoprofil physisch geschützt werden. Zu diesen Vermögenswerten können gehören:
  - Server und Kontrollsysteme
  - Strominfrastruktur und Verkabelung
  - Sensible Datenbestände
  - Komponenten der Operationellen Technologie (OT)
- Die Schutzmaßnahmen sollten Folgendes umfassen:
  - Physische Barrieren und Abschirmungen:
  - Verschlossene Gehäuse, sichere Schränke oder Käfige für empfindliche Geräte
  - Manipulationssichere Siegel zur Erkennung von nicht autorisiertem Zugriff
  - Umgebungsschutzmaßnahmen (z. B. Brandbekämpfung, Temperaturregelung)
  - Schutz der Infrastruktur:
    - Sicherung von Strom- und Netzwerkverkabelung, Zugangsschnittstellen und Geräten
    - Redundante und räumlich getrennte Stromversorgungssysteme für kritische Vorgänge
  - Zugangskontrolle und Überwachung:
    - Begleitung von Gästen, Anbietern und Dritten zu jeder Zeit
    - Führen und regelmäßiges Überprüfen von Zugangsprotokollen
- Die Kontrollen sollten auf die damit verbundenen Anforderungen abgestimmt sein, einschließlich:
  - PR.AA-06.1 – Risikobasierte Zugangskontrolle
  - PR.AA-06.2 – Zugangsverfahren für Notfälle
  - PR.AA-06.3 - Verbesserte Zugangskontrollen für kritische Zonen
- Der Schutz sollte proaktiv erfolgen, bereits bei der Klassifizierung von Vermögenswerten und der Planung von Einrichtungen eingeleitet und in die umfassendere Strategie der physischen Sicherheit integriert werden.



Die Mitarbeiter der Organisation werden für die Cybersicherheit sensibilisiert und geschult, damit sie ihre Aufgaben im Bereich der Cybersicherheit wahrnehmen können

PR.AT-01 Die Mitarbeiter werden sensibilisiert und geschult, damit sie über das Wissen und die Fähigkeiten verfügen, allgemeine Aufgaben unter Berücksichtigung der Cybersicherheitsrisiken auszuführen.

PR.AT-01.1 Die Organisation führt ein Programm zur Sensibilisierung und Schulung im Bereich Cybersicherheit ein und hält dieses aufrecht, um sicherzustellen, dass alle Mitarbeiter verstehen, wie sie ihre Aufgaben sicher und verantwortungsbewusst ausführen können.

Implementierungshinweise

Ziel der Kontrolle PR.AT-01.1 ist es, sicherzustellen, dass jeder in der Organisation versteht, wie man sicher arbeitet, indem regelmäßige, klare und praktische Schulungen zur Cybersicherheit angeboten werden, die das menschliche Risiko reduzieren und sicheres Verhalten sowohl in IT- als auch in OT-Umgebungen unterstützen.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Grundlegende Schulungen sollten für alle angeboten werden**
  Schulungen zum Thema Cybersicherheit sollten für alle Mitarbeiter, Subunternehmer, Partner und Lieferanten angeboten werden, einschließlich derjenigen, die in Operational-Technology-Umgebungen (OT) tätig sind.
- **Die Schulung sollte gängige Bedrohungen abdecken**
  Themen wie Phishing, schwache Passwörter, Social Engineering und OT-spezifische Risiken (z. B. USB-Missbrauch, Bedrohungen durch Fernzugriff) sollten einbezogen werden.
- **Die Schulung sollte früh beginnen und regelmäßig wiederholt werden**
  Die Schulung sollte während des Onboardings erfolgen und mindestens einmal jährlich aufgefrischt werden. Laufende Aktualisierungen und Erinnerungen sollten die Schlüsselbotschaften verstärken.
- **Mehrere Kanäle sollten genutzt werden**
  Das Bewusstsein sollte durch strukturierte Veranstaltungen, Kampagnen, Poster, Newsletter und interaktive Tools geschärft werden.
- **Die Folgen der Nichteinhaltung sollten erläutert werden**
  Die Auswirkungen eines Verstoßes gegen die Cybersicherheitsrichtlinien sollten sowohl für den Einzelnen als auch für die Organisation klar kommuniziert werden.
- **Die Schulungen sollten mit den Richtlinien und Best Practices abgestimmt sein**
  Die Inhalte sollten die internen Cybersicherheitsrichtlinien, erwarteten Verhaltensweisen und Schutzmaßnahmen widerspiegeln. Anerkannte Rahmenwerke wie ENISAs AR-in-a-Box sollten die Programmgestaltung leiten.
- **Auf OT-spezifische Risiken sollte eingegangen werden**
  Die Schulung sollte auf die besonderen Verantwortlichkeiten und Risiken der Mitarbeiter zugeschnitten sein, die mit industriellen Steuerungssystemen und anderen OT-Anlagen arbeiten.
- **Die Inhalte sollten auf dem neuesten Stand gehalten werden**
  Die Schulungsunterlagen sollten regelmäßig überprüft und aktualisiert werden, um neue Bedrohungen und aus Vorfällen gewonnene Erkenntnisse zu berücksichtigen.

PR.AT-01.2 **Die Organisation nimmt die Sensibilisierung für Insider-Bedrohungen und die Meldung solcher Vorfälle in ihre Cybersicherheitsschulungen auf, um den Mitarbeitern zu helfen, potenzielle interne Risiken zu erkennen und darauf zu reagieren.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Mitarbeiter darin geschult sind, potenzielle Insider-Bedrohungen zu erkennen und zu melden, um so das Risiko interner Cybersicherheitsvorfälle zu verringern.
Diese Kontrolle baut auf den allgemeinen Erkenntnissen aus PR.AT-01.1 auf, indem sie spezifische Bedrohungsszenarien und Reaktionsmaßnahmen einführt.

Bei der Implementierung sollten diese Punkte berücksichtigt werden:

- Zu den Schulungen sollte gehören, wie man Verhaltensanzeichen von Insider-Bedrohungen erkennt, z. B. ungewöhnliche Zugriffsmuster, das Horten von Daten oder plötzliche Verhaltensänderungen.
- Die Organisation sollte Insider-Bedrohungen klar definieren (z. B. schädliche, fahrlässige oder gefährdete Insider, einschließlich Mitarbeiter und Subunternehmer).
- Die Mitarbeiter sollten darin geschult werden, wie und wo verdächtige Aktivitäten zu melden sind und warum eine rechtzeitige Meldung wichtig ist.
- Es sollten reale Fallstudien oder Simulationen verwendet werden, um die Auswirkungen von Insider-Bedrohungen aufzuzeigen und den Lernprozess zu verstärken.
- Die Sensibilisierung für Insider-Bedrohungen sollte Teil der regelmäßigen Sicherheitsschulungen und des Onboardings aller Mitarbeiter sein.
- Mitarbeiter, die Zugang zu sensiblen Daten oder Systemen haben, sollten eine spezielle Schulung erhalten, die sich auf ihre spezifischen Aufgaben konzentriert.
- Die Schulung funktionsübergreifender Teams sollte sowohl mit IT-Sicherheits- als auch mit OT-Betriebskenntnissen durchgeführt werden (Cross-Training).
- Jährliche Auffrischungsschulungen sollten dazu dienen, Schlüsselbotschaften zu bekräftigen und Aktualisierungen einzuführen.
- Die Organisation sollte eine Sicherheitskultur fördern, in der sich die Mitarbeiter sicher fühlen, Bedenken zu melden, ohne Vergeltungsmaßnahmen befürchten zu müssen.

PR.AT-01.3 **Die Mitarbeiter erhalten Schulungen, um ihre spezifischen Rollen, Verantwortlichkeiten und Prioritäten während eines Cybersicherheits- oder Informationssicherheitsvorfalls zu verstehen, einschließlich der Schritte, die sie befolgen müssen, um effektiv reagieren zu können.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Mitarbeiter ihre spezifischen Rollen, Verantwortlichkeiten und Prioritäten während eines Cybersicherheits- oder Informationssicherheitsvorfalls verstehen, damit sie effektiv und in Abstimmung mit den Vorfallreaktions- und Notfallplänen der Organisation reagieren können.
Diese Kontrolle baut auf der bedrohungsspezifischen Sensibilisierung aus PR.AT-01.2 auf, indem sie rollenbasierte Schulungen und die Bereitschaft zur Reaktion auf Vorfälle einführt.

Bei der Implementierung sollte Folgendes berücksichtigt werden:

- Die Schulungen sollten auf die verschiedenen Rollen (z. B. IT, HR, Führungskräfte) zugeschnitten sein, damit jede Gruppe ihre spezifischen Verantwortlichkeiten während eines Vorfalls versteht.
- Die Mitarbeiter sollten mit ihren Zielen, den Prioritäten für die Wiederherstellung und der richtigen Reihenfolge der Maßnahmen während eines Vorfalls vertraut sein.

- Tabletop-Übungen oder simulierte Übungen sollten genutzt werden, um die Reaktion auf Vorfälle in einer realistischen, aber kontrollierten Umgebung zu üben.
- Es sollte eine klare Dokumentation erstellt werden, in der die Aufgaben und Zuständigkeiten der einzelnen Rollen während eines Vorfalls beschrieben sind.
- In der Schulung sollte erklärt werden, wie die Reaktion auf einen Vorfall mit der Notfallplanung zusammenhängt, damit die Mitarbeiter wissen, wann und wie sie Notfallmaßnahmen aktivieren müssen (siehe auch ID.IM-04.1).
- Es sollten regelmäßige Auffrischungssitzungen stattfinden, um das Wissen auf dem neuesten Stand zu halten und die Bereitschaft zu stärken.

PR.AT-01.4 Die Organisation bewertet, ob ihre Schulungen zum Bewusstsein für Cybersicherheit das Wissen, das Verhalten und die Bereitschaft in der gesamten Organisation wirksam verbessern.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Schulungen zum Thema Cybersicherheit zu messbaren Verbesserungen hinsichtlich des Wissensstands der Mitarbeiter, ihres Sicherheitsbewusstseins und ihrer Bereitschaft, auf Cyberbedrohungen auf allen Ebenen der Organisation zu reagieren, führen. Diese Kontrolle baut auf der bedrohungsspezifischen Sensibilisierung aus PR.AT-01.2 und der rollenbasierten Schulung aus PR.AT-01.3 auf, indem sie einen strukturierten Ansatz zur Messung der Auswirkungen von Sensibilisierungsmaßnahmen einführt.

Bei der Implementierung sollte Folgendes berücksichtigt werden:

- Die Organisation sollte bewerten, ob Schulungen zur Sensibilisierung für alle relevanten Mitarbeiter zugänglich sind und ob sie deren Verhalten, Bewusstsein und Einstellung in Bezug auf Cybersicherheit wirksam beeinflussen.
- Wenn die Organisation über keine Erfahrung mit Bewertungen verfügt, sollte sie die Verwendung bestehender bewerteter Rahmenwerke oder Tools in Betracht ziehen, wie beispielsweise AR-in-a-Box von ENISA, das Leitlinien zur Festlegung von Zielen, zur Auswahl von KPIs und zur Messung der Auswirkungen enthält.
- Wenn die Organisation intern eine Bewertungsmethode entwickelt, sollte sie sich mit bewährten Verfahren und evidenzbasierten Ansätzen zur Bewertung von Sensibilisierungsprogrammen befassen.
- Die Bewertungsmethoden sollten eine Mischung aus Folgendem enthalten:
  - Bewertungen vor und nach der Schulung oder Tests.
  - Simulierte Phishing- oder Social-Engineering-Tests.
  - Umfragen zur Messung von Veränderungen in Bezug auf Sensibilisierung, Vertrauen und Verhalten.
  - Feedback von Teilnehmern und Ausbildern.
- Die Organisation sollte die gemachten Erfahrungen dokumentieren und die Ergebnisse zur Verbesserung künftiger Schulungsmaßnahmen nutzen.

PR.AT-02 Personen in speziellen Funktionen werden sensibilisiert und geschult, so dass sie über das Wissen und die Fähigkeiten verfügen, relevante Aufgaben unter Berücksichtigung von Cybersicherheitsrisiken auszuführen

PR.AT-02.1 **Die Mitglieder der Führungsgremien können nachweisen, dass sie eine Schulung absolviert haben, die ihnen fundierte Kenntnisse über Informations- und Cybersicherheit sowie Risikomanagement vermittelt, sodass sie Informations- und Cybersicherheitsrisiken und deren Folgen bewerten und unter Berücksichtigung ihrer Rollen, Verantwortlichkeiten und Befugnisse die erforderlichen Maßnahmen zur Risikominderung vorschlagen können.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Mitglieder der Führungsgremien in der Lage sind, fundierte Entscheidungen über Cybersicherheitsrisiken und Strategien zur Risikominderung zu treffen, indem sie ein grundlegendes Verständnis der Informationssicherheit, der Cyberbedrohungen und der Grundsätze des Risikomanagements entwickeln, die für ihre Führungsrolle relevant sind.

Um dieses Ziel zu erreichen, sollten folgende Praktiken berücksichtigt werden:

- Die Schulung sollte die Führungskräfte in die Lage versetzen, Cybersicherheitsrisiken zu bewerten, ihre potenziellen Auswirkungen zu verstehen und geeignete Abhilfemaßnahmen vorzuschlagen, die ihren Verantwortlichkeiten und Befugnissen entsprechen.
- Die Schulungsinhalte sollten Folgendes berücksichtigen:
  - Kernkonzepte der Informations- und Cybersicherheit
  - Risikoidentifizierung, -bewertung und -minderung
  - Strategische Entscheidungsfindung im Kontext von Cyber-Bedrohungen
  - Erkennung potenzieller Sicherheitslücken und Verantwortlichkeiten
- Die Schulungen sollten auf die Führungsrollen zugeschnitten sein, wobei die Leitlinien der Agentur der Europäischen Union für Cybersicherheit (ENISA) zu den Rollenprofilen, einschließlich der Titel, Aufgaben, Fähigkeiten und Kompetenzen (Ref. European Cybersecurity Skills Framework Role Profiles) angewendet werden.
- Jährliche Auffrischungssitzungen sollten in Betracht gezogen werden, um bestehende Praktiken zu stärken und neue Entwicklungen im Bereich der Cybersicherheit und des Risikomanagements einzuführen.

PR.AT-02.2 **Personen in spezialisierten Funktionen erhalten vor der Gewährung von Berechtigungen eine Sensibilisierung und Schulung, damit sie über die erforderlichen Kenntnisse und Fähigkeiten verfügen, um relevante Aufgaben unter Berücksichtigung der Cybersicherheitsrisiken auszuführen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Personen in speziellen Funktionen vor der Gewährung privilegierter Zugriffsrechte eine Schulung zum Thema Cybersicherheit erhalten, damit sie ihre Aufgaben mit einem umfassenden Verständnis der Cybersicherheitsrisiken ausführen können.

Um dieses Ziel zu erreichen, sollte die Organisation:

- Die spezialisierten Rollen innerhalb der Organisation, die zusätzliche Cybersicherheitsschulungen benötigen (z. B. physisches und Cybersicherheitspersonal, Finanzpersonal, Personen in Führungspositionen und alle, die Zugang zu geschäftskritischen Daten haben), sollten formell festgelegt werden.

- Alle Personen in speziellen Funktionen, einschließlich Subunternehmern, Partnern, Lieferanten und anderen Drittparteien, sollten rollenbasiert für das Thema Cybersicherheit sensibilisiert und geschult werden.
- Es sollte sichergestellt werden, dass die Schulung durchgeführt wird, bevor der Zugang gewährt wird, und dass sie auf die spezifischen Risiken und Verantwortlichkeiten der jeweiligen Rolle zugeschnitten ist.
- Einzelpersonen sollten regelmäßig hinsichtlich ihres Verständnisses von Cybersicherheitspraktiken durch Tests, Simulationen oder praktische Bewertungen, die für ihre Rolle relevant sind, beurteilt und geprüft werden.
- Jährliche Auffrischungen in Betracht ziehen, um bestehende Praktiken zu verstärken und neue Praktiken einzuführen.
- Sowohl die Informationstechnologie (IT) als auch die Betriebstechnologie (OT) sollten einbezogen werden, insbesondere bei Aufgaben, die mit industriellen Systemen oder kritischen Infrastrukturen zu tun haben.

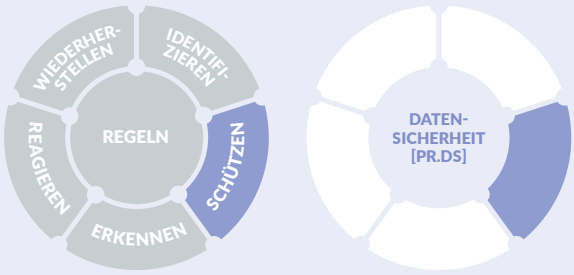
PR.AT-02.3 Privilegierte Benutzer werden vor der Vergabe von Privilegien qualifiziert und können nachweisen, dass sie ihre Rollen, Verantwortlichkeiten und Befugnisse verstehen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Personen, denen privilegierter Zugriff gewährt wird, sei es in IT- oder OT-Umgebungen, nachweislich kompetent sind und sich der mit ihrer Rolle verbundenen Verantwortlichkeiten, Risiken und Befugnisgrenzen im Bereich der Cybersicherheit voll bewusst sind. Dies verringert die Wahrscheinlichkeit eines versehentlichen Missbrauchs oder der Ausnutzung erhöhter Privilegien, insbesondere in kritischen Systemen, bei denen die Betriebskontinuität und Sicherheit auf dem Spiel stehen.

Um sicherzustellen, dass dieses Ziel erreicht wird, sollte die Organisation Folgendes berücksichtigen:

- Privilegierte Benutzer sollten in verschiedenen Aspekten geschult werden, um sicherzustellen, dass sie ihre erhöhten Zugriffsrechte auf sichere und verantwortungsvolle Weise nutzen. Die folgenden Schulungsthemen könnten in Betracht gezogen werden:
  - Sicherheitsbewusstsein: Es ist von entscheidender Bedeutung, dass privilegierte Benutzer sich der Sicherheitsrisiken bewusst sind, die mit ihren erhöhten Zugriffsrechten verbunden sind. Dazu gehört auch Wissen über Phishing, Malware und andere Cyber-Bedrohungen.
  - Zugriffsverwaltung: Die Benutzer sollten wissen, wie sie ihre Zugriffsrechte ordnungsgemäß verwalten können, einschließlich der Verwendung von sicheren Passwörtern, Multi-Faktor-Authentifizierung und der Beschränkung des Zugriffs auf das, was für ihre Rolle erforderlich ist.
  - Einhaltung von Gesetzen und Vorschriften: Es ist wichtig, dass privilegierte Nutzer die relevanten Gesetze und Vorschriften kennen, wie z. B. GDPR, NIS2, DORA usw., und wissen, wie sie sich auf ihre Arbeit auswirken.
  - Reaktion auf Vorfälle: Schulungen zur Reaktion auf Sicherheitsvorfälle sind unerlässlich. Dazu gehört auch, verdächtige Aktivitäten zu erkennen und zu wissen, wie und an wen man sie melden muss.
  - Best Practices in der Datenverwaltung: Die Benutzer sollten darin geschult werden, wie sie sensible Daten sicher speichern, verarbeiten und übertragen können.
  - Ethik und Verantwortung: Es ist wichtig, dass sich privilegierte Benutzer ihrer ethischen Verantwortung und der möglichen Folgen eines Missbrauchs ihrer Zugangsrechte bewusst sind.
- Privilegierte Benutzer sollten in regelmäßigen Abständen bewertet und auf ihr Verständnis der Cybersicherheitspraktiken für ihre spezielle Rolle geprüft werden.
- Jährliche Auffrischungen in Betracht ziehen, um bestehende Praktiken zu verstärken und neue Praktiken einzuführen.



Daten werden im Einklang mit der Risikostrategie der Organisation verwaltet, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen

PR.DS-01 Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten im Ruhezustand sind geschützt

PR.DS-01.1 Die Organisation implementiert Software-, Firmware- und Informationsintegritätsprüfungen, um unbefugte Änderungen an ihren kritischen Systemkomponenten während der Lagerung, des Transports, der Inbetriebnahme und bei Bedarf zu erkennen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Integrität und Vertrauenswürdigkeit kritischer Systemkomponenten wie Software, Firmware und Konfigurationsdaten zu gewährleisten, indem unbefugte Änderungen aufgespürt werden, die die Betriebssicherheit, Zuverlässigkeit oder Gefahrenabwehr in allen Phasen des Lebenszyklus, einschließlich Lagerung, Transport und Inbetriebnahme, beeinträchtigen könnten.

Um die Integrität der Daten im Ruhezustand wirksam zu schützen, sollte die Organisation ein mehrstufiges Kontrollsystem einführen, das unbefugte Änderungen an gespeicherten Daten, Software und Systemkomponenten erkennt und verhindert.

Die folgenden Vorgehensweisen sollten in Betracht gezogen werden:

- Anwendung kryptographischer Integritätsmechanismen
  - Verwenden Sie kryptografische Hashes (z. B. SHA-256), digitale Signaturen oder andere kryptografische Mechanismen (z. B. Message Authentication Codes (MACs)), um die Integrität gespeicherter Daten und wichtiger Dateien zu überprüfen.
  - Integritätswerte sollten zum Zeitpunkt der Speicherung erzeugt und vor dem Zugriff oder der Ausführung überprüft werden.
- Implementierung automatisierter Integritätsüberwachung
  - Setzen Sie Tools zur Überwachung der Dateiintegrität (FIM) ein, um Änderungen an kritischen Systemdateien, Konfigurationen und Anwendungen kontinuierlich zu verfolgen.
  - Bei unbefugten oder unerwarteten Änderungen sollten Warnmeldungen generiert werden, und die Protokolle sollten zu Prüf- und Untersuchungszwecken aufbewahrt werden.
- Überprüfung der Integrität von Software und Firmware
  - Stellen Sie sicher, dass die auf den Systemen gespeicherte Software und Firmware vor der Ausführung durch Signaturüberprüfung oder sichere Boot-Mechanismen validiert wird.
  - Die Validierung der Integrität sollte Teil des Systemstartprozesses sein und durch technische Kontrollen durchgesetzt werden.
- Durchsetzung von Änderungskontrolle und Zugriffsbeschränkungen
  - Beschränken Sie den Schreibzugriff auf kritische Daten und Systemkomponenten durch rollenbasierte Zugriffskontrollen (RBAC) und das Prinzip der geringsten Privilegien.
  - Alle Änderungen an Data-at-Rest sollten formellen Änderungsmanagementverfahren unterliegen und zur Nachvollziehbarkeit protokolliert werden.

- **Schutz der Integrität von Backups**
  - Backups sollten Mechanismen zur Überprüfung der Integrität enthalten (z. B. Prüfsummen oder digitale Signaturen), um sicherzustellen, dass sie nicht manipuliert wurden.
  - Es sollten regelmäßige Testwiederherstellungen durchgeführt werden, um die Integrität und Verwendbarkeit der Backup-Daten zu bestätigen.

PR.DS-01.2 Die Organisation setzt, soweit möglich, automatisierte Tools ein, um bei der Integritätsverifizierung festgestellte Unstimmigkeiten zu melden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Unstimmigkeiten in der System- oder Datenintegrität automatisch erkannt und gemeldet werden, um eine rechtzeitige Reaktion zu ermöglichen und das Risiko unentdeckter Manipulationen zu verringern, insbesondere in Umgebungen, in denen die Kontinuität des Betriebs und die Sicherheit entscheidend sind.

Um dieses Ziel zu erreichen, sollte die Organisation:
- Soweit möglich automatisierte Tools implementieren, um die Integrität kritischer Daten und Systeme kontinuierlich zu verifizieren.
- Sicherstellen, dass diese Tools Verstöße gegen die Integrität unverzüglich melden, wenn Unstimmigkeiten festgestellt werden.
- Warnmeldungen konfigurieren, um relevante Mitarbeiter wie Systemadministratoren, Geschäftsinhaber und Informationssicherheitsbeauftragte zu benachrichtigen, um eine schnelle Untersuchung und Reaktion zu ermöglichen.
- Zentral verwaltete Lösungen zur Integritätsverifizierung einsetzen, um die Überwachung und Berichterstattung sowohl in IT- (Informationstechnologie) als auch in OT- (Betriebstechnologie) Umgebungen zu optimieren.
- Die Leitlinien der ENISA befolgen, wie beispielsweise die Technischen Umsetzungsleitlinien zu NIS2 (ENISA, 2025), in denen bewährte Verfahren für die automatisierte Integritätsüberwachung und die Reaktion auf Vorfälle beschrieben werden.

PR.DS-01.3 Die Organisation definiert und implementiert automatisierte Reaktionen auf festgestellte Integritätsverletzungen unter Verwendung vordefinierter Schutzmaßnahmen, die in einem angemessenen Verhältnis zur Schwere und den Auswirkungen der Verletzung stehen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Auswirkungen von Integritätsverletzungen zu minimieren, indem zeitnahe, verhältnismäßige und automatisierte Reaktionen ermöglicht werden, die dazu beitragen, Bedrohungen einzudämmen, die Systemstabilität zu erhalten und forensische Analysen zu unterstützen, insbesondere in Umgebungen, in denen ein manuelles Eingreifen verzögert oder unpraktisch sein kann.

Um dieses Ziel zu erreichen, sollten die folgenden Leitlinien berücksichtigt werden:
- Schweregrade und Reaktionsmaßnahmen sollten definiert werden, wobei Integritätsverletzungen kategorisiert (z. B. geringe, mittlere, starke Auswirkungen) und mit geeigneten automatischen Schutzmaßnahmen verknüpft werden sollten.
- Warnungen und Benachrichtigungen sollten automatisch ausgelöst werden, wenn Integritätsverletzungen festgestellt werden, und in SOAR-Plattformen (Security Orchestration, Automation, and Response) integriert werden, um die Bearbeitung von Vorfällen zu optimieren.
- Betroffene Komponenten sollten unter Quarantäne gestellt oder isoliert werden, z. B. kompromittierte Dateien, Anwendungen oder Systeme, um weiteren Schaden zu verhindern.

- Alle Ereignisse sollten protokolliert und auditierbar sein, einschließlich festgestellter Verstöße und automatisierter Maßnahmen, um forensische Untersuchungen und Compliance-Berichte zu unterstützen.
- Wo immer möglich, sollte eine leichte Automatisierung eingesetzt werden, beispielsweise:
  - Blockieren bestimmter Prozesse oder Benutzer
  - Zurückkehren zu einer bekannten, guten Konfiguration
  - Vorübergehende Deaktivierung der betroffenen Dienste
- Die Reaktionsmechanismen sollten regelmäßig in kontrollierten Umgebungen getestet und angepasst werden, um ihre Wirksamkeit zu gewährleisten und unnötige Störungen zu vermeiden.
- Die Leitlinien der Agentur der Europäischen Union für Cybersicherheit (ENISA) in den „Implementierungsleitlinien zu Sicherheitsmaßnahmen“ (zur öffentlichen Konsultation, Dokument Nr. ENISA/2024/IGSM) sollten konsultiert werden.

PR.DS-01.4 Die Organisation definiert und setzt klare Richtlinien und praktische Sicherheitsvorkehrungen zur Verwaltung und Einschränkung der Nutzung tragbarer Speichermedien um, um das Risiko von Datenlecks, unbefugtem Zugriff und der Einschleusung von Malware zu verringern.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko von Datenlecks, unbefugtem Zugriff und der Einschleusung von Malware zu verringern, indem klare Richtlinien und Sicherheitsvorkehrungen für die Verwendung tragbarer Speichermedien definiert und durchgesetzt werden.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Richtlinien definieren und kommunizieren**
  - Es sollte eine dokumentierte Richtlinie über die zulässige Verwendung von tragbaren Speichermedien (z. B. USB-Laufwerke, SD-Karten, externe Festplatten) festgelegt werden.
  - Die Richtlinie sollte beim Onboarding vermittelt und durch regelmäßige Schulungen zum Sicherheitsbewusstsein verstärkt werden.
- **Die Geräteverwendung kontrollieren**
  - Es sollten nur von der Organisation zugelassene tragbare Speichermedien zugelassen werden.
  - Es sollte ein Inventar der zugelassenen Geräte geführt und mit bestimmten Benutzern oder Abteilungen verknüpft werden.
- **Praktische Schutzmaßnahmen anwenden**
  - **Zugangskontrolle**: Die Geräte sollten eine Benutzerauthentifizierung erfordern (z. B. Passwortschutz).
  - **Verschlüsselung**: Daten auf tragbaren Geräten sollten mit hardware-verschlüsselten Laufwerken oder Software-Tools wie BitLocker To Go oder VeraCrypt verschlüsselt werden.
  - **Read-Only-Modus**: Die Geräte, die zur Verteilung (z. B. von Software-Updates) verwendet werden, sollten als schreibgeschützt konfiguriert werden.
  - **Malware-Scans**: Die Geräte sollten vor und nach der Nutzung auf Malware gescannt werden.
  - **Physische Sicherheit**: Die Geräte sollten sicher aufbewahrt werden (z. B. in verschlossenen Schubladen oder Schränken), wenn sie nicht in Gebrauch sind.
- **Die Nutzung überwachen und protokollieren**
  - Auf verwalteten Systemen sollten USB-Geräteverbindungen und Dateiübertragungen mithilfe von Endpunkt-Verwaltungstools protokolliert werden.
  - Die Protokolle sollten regelmäßig überprüft werden, um unbefugte Nutzung oder Anomalien festzustellen.
- **Beispiele**
  - Ein Außendiensttechniker sollte einen vom Unternehmen bereitgestellten, verschlüsselten USB-Stick verwenden, um Daten von Fernsensoren zu erfassen. Das Laufwerk sollte vor und nach der Benutzung gescannt werden, und die Daten sollten nach der Rückkehr auf einen sicheren Server hochgeladen werden.
  - Ein Marketingteam sollte einen schreibgeschützten USB-Stick verwenden, um auf einer Messe Werbematerialien zu verteilen und so zu verhindern, dass Daten auf das Gerät zurückkopiert werden.

PR.DS-01.5 Die Organisation erlaubt die Verwendung von Wechseldatenträgern nur, wenn dies unbedingt erforderlich ist, und ergreift technische Maßnahmen, um die automatische Ausführung von Dateien von diesen Geräten zu verhindern.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Angriffsfläche in Betriebs- und IT-Umgebungen zu minimieren, indem die Verwendung von Wechseldatenträgern streng begrenzt und die automatische Ausführung potenziell schädlicher Dateien verhindert wird.

Um das Risiko von Malware-Infektionen und Datenlecks durch Wechselmedien (z. B. USB-Sticks, externe Laufwerke) zu verringern, sollte die Organisation:

- Die Nutzung nur im Bedarfsfall zulassen
  - Die Organisation sollte in ihren Richtlinien festlegen, dass Wechseldatenträger nur dann verwendet werden sollten, wenn keine sicherere Alternative zur Verfügung steht (z. B. sichere Dateiübertragung).
  - Es sollten technische Tools eingesetzt werden, um den Zugang zu USB-Anschlüssen einzuschränken oder vor der Nutzung eine Genehmigung zu verlangen.
- Autorun und automatische Ausführung deaktivieren
  - Alle Systeme sollten so konfiguriert werden, dass Autorun- und Autoplay-Funktionen deaktiviert werden, damit Dateien auf Wechselmedien nicht automatisch ausgeführt werden.
  - Dadurch soll verhindert werden, dass Malware ohne Zutun des Benutzers ausgeführt wird.
- Sicherheitstools zur Zugriffskontrolle verwenden
  Die Organisation sollte Endpunktschutz-Tools verwenden, um:
  - Den USB-Zugriff zu blockieren oder zu limitieren.
  - Nur zugelassene Geräte zu erlauben.
  - Die Genehmigung des Administrators für neue Geräte zu verlangen.
- Die Nutzung überwachen und überprüfen
  Die Organisation sollte die Nutzung von Wechseldatenträgern überwachen, indem sie Geräteverbindungen über Endpunktschutz-Tools oder Betriebssystemprotokolle protokolliert. In OT-Umgebungen sollten manuelle Protokollierung oder kontrollierte Zugriffsverfahren verwendet werden. Die Protokolle sollten regelmäßig überprüft werden, um unbefugte Zugriffe oder Richtlinienverstöße zu erkennen.
- Beispiel: Ein Finanzteam sollte verschlüsselte, vom Unternehmen zugelassene USB-Laufwerke verwenden, um sensible Berichte zu übertragen. Diese Laufwerke sollten vor der Benutzung gescannt werden, Autorun sollte auf allen Systemen deaktiviert werden, und der Zugriff sollte protokolliert und überprüft werden.

Klärung des Unterschieds zu PR.DS-01.4

- PR.DS-01.4 konzentriert sich auf die Festlegung von Regeln und Verfahren für die Verwendung von Wechseldatenträgern (z. B. wer sie verwenden darf, Verschlüsselung, physischer Schutz).
- PR.DS-01.5 konzentriert sich auf die technische Durchsetzung dieser Regeln – wie Systeme konfiguriert werden sollten, um Risiken zu reduzieren.

PR.DS-01.6 Die Organisation schützt die Vertraulichkeit ihrer kritischen Vermögenswerte im Ruhezustand.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass sensible Betriebs- und Geschäftsdaten, die auf Systemen, Servern oder Geräten gespeichert sind, vor nicht autorisiertem Zugriff geschützt bleiben, selbst wenn die physische oder logische Sicherheit beeinträchtigt ist.

In OT-Umgebungen, in denen Altsysteme und gemeinsam genutzte Infrastrukturen weit verbreitet sind, ist der Schutz ruhender Daten von entscheidender Bedeutung, um zu verhindern, dass Konfigurationsdateien, Prozessdaten oder Berechtigungsnachweise offengelegt werden, die zur Störung des Betriebs oder zum Erlangen von lateralem Zugriff missbraucht werden könnten.
Diese Kontrolle baut weiter auf PR.DS-01.1 auf.

Um den Schutz der kritischen Vermögenswerte der Organisation im Ruhezustand zu ermöglichen, sollten die folgenden Techniken in Betracht gezogen werden:

- Verschlüsselung: Verschlüsselung von Daten im Ruhezustand, auf Festplatten, auf externen Medien, in gespeicherten Dateien, in Konfigurationsdateien und in der Cloud, unter Verwendung starker Verschlüsselungsalgorithmen, um unbefugten Zugriff zu verhindern und die Daten vor Manipulationen zu schützen.
- Zugangskontrollen: Führen Sie strenge Zugangskontrollen ein, um sicherzustellen, dass nur befugtes Personal auf sensible Informationen zugreifen kann.
- Regelmäßige Audits: Führen Sie regelmäßig Sicherheitsaudits durch, um Schwachstellen zu ermitteln und zu beheben.
- Datenmaskierung: Verwenden Sie Datenmaskierungstechniken, um sensible Informationen in Nicht-Produktionsumgebungen zu verbergen (z. B. dürfen DSGVO-sensible Daten aus der Produktionsumgebung nicht ohne Randomisierung in eine Testumgebung kopiert werden, um einen unbefugten Datenzugriff zu verhindern).

PR.DS-01.9 Vermögenswerte des Unternehmens müssen sicher entsorgt werden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Unternehmensressourcen auf sichere und kontrollierte Weise entsorgt werden, um den unbefugten Zugriff auf sensible geschäftliche, persönliche oder betriebliche Daten zu verhindern.

Um dieses Ziel zu unterstützen, sollte die Organisation:

- **Daten vor der Entsorgung bereinigen**
  Sensible Daten sollten von allen Geräten wie Computern, Servern, Festplatten, USB-Laufwerken, mobilen Geräten und Papierdokumenten sicher entfernt („gelöscht") werden, bevor sie außer Betrieb genommen, neu zugewiesen, repariert oder ersetzt werden.
- **Geeignete Vernichtungsmethoden anwenden**
  Für die Vernichtung von Papierunterlagen, digitalen Speichermedien und anderen physischen Datenträgern sollten geeignete Methoden zur Verfügung stehen.
- **Fernlöschfunktion für mobile Geräte aktivieren**
  Die Fernlöschfunktion sollte auf Laptops, Tablets, Telefonen und anderen mobilen Geräten aktiviert werden, um Daten bei Verlust oder Diebstahl zu schützen.
- **Abgelaufene Domänennamen sorgfältig verwalten**
  Abgelaufene Domänen sollten geschützt werden, da sie häufig das Ziel von Cyber-Kriminellen sind. Die folgenden Vorgehensweisen sollten in Betracht gezogen werden:
  - Aktivierung der automatischen Erneuerung oder Verlängerung der Domains für mindestens zehn Jahre.
  - Klare und deutliche Kommunikation von Domainänderungen und interne Verwaltung von Übergängen.
  - Einstellung von automatischen Antworten für E-Mails, die an alte Domänen gesendet werden.
  - Aktualisierung von Einstellungen für Online-Referenzen und Cloud-Services.
  - Änderung oder Löschung von Konten, die unter alten Domänen registriert sind.
  - E-Mail-Adressen für die Anmeldung aktuell halten und MFA aktivieren.
  - Vermeidung der Verwendung nicht zugelassener Cloud-Speicher für sensible Daten.
- **Best Practices für die Vermögensverwaltung befolgen**
  Anleitungen aus vertrauenswürdigen Quellen, wie z. B. die Vorlage für die Verwaltung von Vermögenswerten in der CyFun® Toolbox auf www.cyfun.eu, sollten zur Unterstützung einer sicheren Entsorgung verwendet werden.
- **OT-Anlagen in die Entsorgungsplanung einbeziehen**
  OT-Systeme und -Geräte sollten in die Entsorgungsverfahren einbezogen werden, um sicherzustellen, dass Betriebsdaten und Konfigurationen vor der Stilllegung sicher entfernt werden.

PR.DS-02 Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bei der Übermittlung sind geschützt

PR.DS-02.1 Mobile Speichermedien, die Systemdaten enthalten, werden während des Transports und der Lagerung kontrolliert und geschützt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, den unbefugten Zugriff, die Manipulation oder den Verlust kritischer Systemdaten zu verhindern, wenn tragbare Speichermedien zwischen verschiedenen Standorten verschoben oder außerhalb sicherer Umgebungen gelagert werden.

In OT-Umgebungen, in denen Daten zwischen isolierten Systemen oder entfernten Standorten mit Hilfe physischer Medien übertragen werden können, ist der Schutz dieser Geräte für die Wahrung der Systemintegrität und -vertraulichkeit von entscheidender Bedeutung.

Um dieses Ziel zu erreichen, sollte die Organisation:

- Alle mobilen Speichergeräte vor der Verwendung in Unternehmenssystemen auf schädlichen Code überprüfen.
- Daten verschlüsseln, um die Vertraulichkeit zu gewährleisten, falls ein Gerät verloren geht oder gestohlen wird.
- Während des Transports manipulationssichere Siegel und verschlossene Behälter verwenden.
- Sich auf zuverlässige Kuriere oder sichere Transportdienste verlassen und vermeiden, Geräte unbeaufsichtigt zu lassen.
- Den Zugriff auf gespeicherte Geräte auf autorisiertes Personal beschränken, unterstützt durch Richtlinien zur dokumentierten Zugriffskontrolle.
- Geräte in sicheren, klimatisierten Umgebungen aufbewahren, um physische Schäden zu vermeiden.
- Regelmäßige Audits und Bestandsprüfungen durchführen, um sicherzustellen, dass alle Geräte erfasst und ordnungsgemäß gesichert sind.

PR.DS-02.2 Die Organisation schützt ihre kritischen und sensiblen Informationen während der Übertragung.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass kritische und sensible Informationen vertraulich und unverändert bleiben, während sie über Netzwerke oder zwischen Systemen übertragen werden, insbesondere in Umgebungen, in denen Daten zwischen IT- und OT-Ebenen oder über entfernte Standorte hinweg fließen.

In OT-Kontexten, in denen Daten über weniger sichere oder veraltete Kommunikationskanäle übertragen werden (z. B. zwischen Steuersystemen, Feldgeräten oder Fernüberwachungsstationen), ist ein Schutz während der Übertragung unerlässlich, um ein Abfangen, eine Manipulation oder ein Leck zu verhindern. Diese Kontrolle baut weiter auf PR.DS-01.1 auf.

Um den Schutz der kritischen und sensiblen Informationen der Organisation während der Übertragung zu gewährleisten, sollten die folgenden Techniken in Betracht gezogen werden:

- Verschlüsselung: Verwenden Sie starke Verschlüsselungsprotokolle wie Transport Layer Security (TLS) oder Secure Sockets Layer (SSL), um Daten während der Übertragung zu verschlüsseln. Dadurch wird sichergestellt, dass die Daten, selbst wenn sie abgefangen werden, für Unbefugte unlesbar bleiben.
- Ende-zu-Ende-Verschlüsselung (E2EE): Implementieren Sie E2EE, bei der die Daten auf dem Gerät des Absenders verschlüsselt und erst auf dem Gerät des Empfängers entschlüsselt werden.
- Multi-Faktor-Authentifizierung (MFA): Verlangen Sie MFA für den Zugriff auf sensible Informationen.
- Starke Passwortrichtlinien: Setzen Sie starke Passwortrichtlinien durch, einschließlich der Verwendung komplexer Passwörter und regelmäßiger Aktualisierungen.

- Virtual Private Networks (VPNs): Nutzen Sie VPNs – entweder Site-to-Site oder Remote Access – um sichere Tunnel für die Datenübertragung einzurichten, insbesondere bei Verbindungen über nicht vertrauenswürdige Netzwerke wie öffentliches WLAN.
- Regelmäßige Sicherheitsaudits: Führen Sie regelmäßig Sicherheitsaudits durch, um Schwachstellen in Ihren Datenübertragungsprozessen zu identifizieren und zu beheben.

PR.DS-10 Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bei der Verwendung sind geschützt

PR.DS-10.1 Die kritischen Systeme der Organisation werden gegen Denial-of-Service-Angriffe geschützt oder zumindest die Auswirkungen solcher Angriffe werden begrenzt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass kritische Systeme auch dann verfügbar und betriebsbereit bleiben, wenn sie Ziel von Denial-of-Service-Angriffen (DoS) sind, die darauf abzielen, Dienste zu überlasten oder zu stören.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Die Auswirkungen von DoS-Angriffen begrenzen durch:**
  - Einsatz von Grenzschutzgeräten oder -diensten, die schädlichen Datenverkehr filtern.
  - Sicherstellung einer ausreichenden Netzkapazität und Redundanz, um Traffic-Spitzen aufzufangen.
- **Einschränkung der Möglichkeit, DoS-Angriffe zu starten, durch:**
  - Einschränkung der Verbindungsoptionen, um unbefugte Übertragungen über drahtgebundene, drahtlose oder Satellitenverbindungen zu verhindern.
  - Durchsetzung von Beschränkungen der Ressourcennutzung, um eine Überlastung des Systems zu verhindern.
  - Anwendung einer starken Authentifizierung und Autorisierung, um den Zugang zu kritischen Funktionen zu kontrollieren.
- **Stärkung der Widerstandsfähigkeit des Systems durch:**
  - Durchführung regelmäßiger Sicherheitstests und -audits, um Schwachstellen zu identifizieren und zu beheben.
  - Überwachung des Netzwerkverkehrs auf Anomalien, die auf frühe Anzeichen eines DoS-Versuchs hindeuten können.
- **OT-spezifische Überlegungen**
  In OT-Umgebungen, in denen sich die Verfügbarkeit direkt auf die Sicherheit und die Produktion auswirkt, können selbst kurze Unterbrechungen schwerwiegende Folgen haben. Der DoS-Schutz sollte auf Industrieprotokolle und Altsysteme zugeschnitten sein, um sicherzustellen, dass die Verteidigungsmaßnahmen den Echtzeitbetrieb nicht beeinträchtigen.

PR.DS-11 Backups von Daten werden erstellt, geschützt, gepflegt und getestet

PR.DS-11.1 **Backups der geschäftskritischen Daten der Organisation werden auf einem anderen System durchgeführt und gespeichert als auf dem Gerät, auf dem sich die Originaldaten befinden.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass geschäftskritische Daten regelmäßig gesichert und sicher auf einem separaten System gespeichert werden, um sie vor Datenverlust, Systemausfällen oder Cyberangriffen wie Ransomware zu schützen.

Um dieses Ziel zu unterstützen, sollte die Organisation:

- **Wichtige Daten und Systeme sichern**
  Backups sollten enthalten:
  - Geschäftskritische Daten (z. B. Kundendaten, Finanz- und Betriebsdaten).
  - Systemdaten wie Softwarekonfigurationen, Geräteeinstellungen, Dokumentation und Anwendungsbackups.
- **Eine Backup-Strategie definieren**
  - Kritische Daten sollten kontinuierlich oder nahezu in Echtzeit gesichert werden.
  - Andere wichtige Daten sollten in regelmäßigen, vereinbarten Abständen gesichert werden.
  - Backups sollten auf einem System gespeichert werden, das physisch oder logisch von der ursprünglichen Datenquelle getrennt ist.
    Das bedeutet, dass sie sich nicht auf demselben Gerät, Server oder Speicherbereich wie die Originaldaten befinden dürfen. Idealerweise sollten Backups in einer anderen Sicherheitszone, einem anderen Netzwerksegment oder sogar an einem externen Standort gespeichert werden, um sicherzustellen, dass sie bei Systemausfällen, Ransomware oder anderen Vorfällen, die sich auf die primäre Umgebung auswirken, zugänglich bleiben und nicht beeinträchtigt werden.
- **Netzwerktrennung sicherstellen**
  - Backups sollten nicht im selben Netzwerk wie die Originalsysteme gespeichert werden.
  - Mindestens eine Backup-Kopie sollte vollständig offline oder luftisoliert aufbewahrt werden, um die Wiederherstellung im Falle einer Netzwerkverletzung oder eines Ransomware-Angriffs sicherzustellen.
- **Wiederherstellung planen**
  Recovery Time Objective (RTO – wie schnell die Systeme wiederhergestellt werden müssen) und Recovery Point Objective (RPO – wie viel Datenverlust ist akzeptabel) sollten definiert und regelmäßig überprüft werden, um eine rechtzeitige und effektive Wiederherstellung zu gewährleisten.
- **OT-Umgebungen einbeziehen**
  Backup-Strategien sollten OT-Systeme abdecken, einschließlich Steuerungssystemkonfigurationen, Betriebsdaten und Geräteeinstellungen, die für den industriellen Betrieb entscheidend sind.

PR.DS-11.2 Die Zuverlässigkeit und Integrität von Backups wird regelmäßig überprüft und getestet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Backup-Daten bei Bedarf vertrauenswürdig sind und erfolgreich wiederhergestellt werden können, um die Betriebskontinuität und Resilienz zu unterstützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Wiederherstellungsprozeduren testen**
  Die Verfahren zum Backup von Sicherungskopien sollten regelmäßig getestet werden, um sicherzustellen, dass die Daten genau und vollständig wiederhergestellt werden können.
- **Integrität des Backups verifizieren**
  - Backups sollten vor der Verwendung auf Anzeichen von Kompromittierung, Beschädigung oder Manipulation überprüft werden.
  - Integritätsprüfungen sollten sich auf Indikatoren für Sicherheitsverletzungen oder Datenverluste konzentrieren.
- **Tests planen**
  - Alle Arten von Datenquellen sollten in die Backup- und Wiederherstellungstests einbezogen werden.
  - Die Tests sollten mindestens einmal jährlich oder häufiger auf Stichprobenbasis durchgeführt werden.
- **Mit verwandten Steuerelementen abgleichen**
  Diese Kontrolle sollte in Abstimmung mit RC.RP-05.1 (Wiederherstellungsplanung) durchgeführt werden, um die Konsistenz der Wiederherstellungsstrategien zu gewährleisten.

PR.DS-11.3 Die Organisation bewahrt sichere Backups von geschäftskritischen Daten an einem separaten Speicherort auf, um die Datenverfügbarkeit im Falle eines Systemausfalls oder Datenverlustes zu gewährleisten. Für den Backup-Speicher gelten gleichwertige Sicherheitskontrollen wie für die primäre Umgebung.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation ihre geschäftskritischen Daten in zwei Schlüsselszenarien zuverlässig wiederherstellen kann:

- **Bei Naturkatastrophen oder physische Beschädigung** des primären Standorts (was Offsite- oder Cloud-basierte Backups erfordert).
- **Bei fortgeschrittenen Cyberangriffen**, einschließlich Ransomware oder Insider-Bedrohungen, bei denen Angreifer versuchen können, Backups zu beschädigen oder zu löschen (was isolierte oder manipulationssichere Backups erfordert).

Diese Kontrolle trägt dazu bei, dass eine Organisation ihre kritischen Daten wiederherstellen kann, wenn etwas schief geht. Sie konzentriert sich darauf, Backups getrennt und genauso sicher wie die Originaldaten zu halten, was es besonders nützlich für Organisationen macht, die ihre Cybersicherheitskapazitäten noch ausbauen (Organisationen mit weniger ausgereiften Sicherheitsstrukturen).

- **Zu berücksichtigende Backup-Strategie**
  - Um diese Ziele zu erreichen, sollte die Organisation ein diversifiziertes und resilientes Backup-Konzept einführen, wie z. B. die **3-2-1 Backup-Regel**:
    - Drei Kopien der geschäftskritischen Daten aufbewahren.
    - Speicherung dieser Kopien auf mindestens zwei verschiedenen Arten von Speichermedien (z. B. lokale Festplatte und Cloud).
    - Sicherstellung, dass mindestens eine Kopie an einem anderen Ort oder außerhalb des Firmengeländes aufbewahrt wird.
- **Um sich sowohl gegen physische als auch gegen Cyber-Bedrohungen zu schützen, sollte die Organisation die folgenden Backup-Arten in Betracht ziehen:**

- **Offsite- oder Cloud-Backups:**
  Diese Backups werden an einem geografisch getrennten Ort gespeichert und tragen dazu bei, die Wiederherstellbarkeit im Falle von Naturkatastrophen oder physischen Schäden am Hauptstandort zu gewährleisten.
- **Unveränderliche Backups:**
  Dies sind Backups, die für einen bestimmten Zeitraum nicht verändert oder gelöscht werden können. Sie sind besonders wirksam gegen Ransomware und Insider-Bedrohungen und können automatisiert werden, um den manuellen Aufwand zu verringern.
- **Offline- oder Air-Gapped-Backups:**
  Dabei handelt es sich um Backups, die auf Geräten gespeichert werden, die von allen Netzen, einschließlich dem Internet, vollständig getrennt sind. Diese Isolierung stellt sicher, dass selbst bei einer Beeinträchtigung des Organisationsnetzwerks die Backups unangetastet bleiben.

- Zusätzliche Überlegungen
  - **Geografische Trennung**: Die Backup-Standorte sollten in verschiedenen Regionen liegen, um das Risiko gleichzeitiger Auswirkungen regionaler Katastrophen zu verringern.
  - **Gleiche Sicherheit**: Alle Backup-Standorte sollten das gleiche Maß an Sicherheitskontrollen durchführen wie die primäre Umgebung (z. B. Verschlüsselung, Zugangskontrolle, Überwachung).
  - **Regelmäßige Tests**: Backup- und Wiederherstellungsverfahren sollten regelmäßig getestet werden, um die Datenintegrität und Betriebsbereitschaft zu gewährleisten.

PR.DS-11.4 Die Organisation verifiziert regelmäßig die Integrität und Wiederherstellbarkeit von Backups durch koordinierte Tests mit allen relevanten Kontinuitäts- und Störungsreaktionsfunktionen. Backup-Tests werden in eine umfassendere Ausfallsicherheitsplanung integriert, einschließlich Business Continuity, Disaster Recovery und Reaktion auf Cybervorfälle.

Implementierungshinweise

Diese Kontrolle ist eine Weiterentwicklung von PR.DS-11.3 und stellt sicher, dass Backup-Systeme nicht nur vorhanden sind, sondern auch regelmäßig getestet werden und mit den umfassenderen Wiederherstellungs- und Kontinuitätsplänen der Organisation abgestimmt sind. Sie unterstreicht die Bedeutung einer teamübergreifenden Koordinierung und einer proaktiven Planung, damit die Organisation darauf vorbereitet ist, sich schnell und effektiv von schwerwiegenden Zwischenfällen zu erholen.

Um sicherzustellen, dass die Backup- und Wiederherstellungsfunktionen effektiv sind und in die Gesamtstrategie der Organisation integriert werden, sollten die folgenden Praktiken angewendet werden:

- **Koordination der Backup-Tests über Pläne hinweg**
  Die Backup-Verifizierung sollte in Abstimmung mit den Teams geplant und durchgeführt werden, die für die wichtigsten Kontinuitäts- und Reaktionspläne der Organisation verantwortlich sind. Dazu gehören:
  - Business Continuity Plans (BCP)
  - Disaster Recovery Plans (DRP)
  - Pläne für unvorhergesehene Ereignisse
  - Continuity of Operations Plans (COOP)
  - Pläne für die Krisenkommunikation
  - Pläne für den Schutz kritischer Infrastrukturen
  - Pläne zur Reaktion auf Cybervorfälle
- **Beziehen Sie die Wiederherstellung von Backups in Szenario-Tests mit ein**
  Bei Übungen oder Simulationen von Vorfällen (z. B. Cyberangriffe, Systemausfälle oder Naturkatastrophen) sollte die Wiederherstellung von Backup-Daten ausdrücklich getestet werden. Dadurch wird sichergestellt, dass Backups nicht nur verfügbar, sondern auch nutzbar sind und mit den Zielen für die Wiederherstellungszeit und den Wiederherstellungspunkt (RTO/RPO) übereinstimmen.
- **Ergebnisse dokumentieren und überprüfen**
  Die Ergebnisse der Backup-Verifizierung und der Wiederherstellungstests sollten dokumentiert und mit den relevanten Stakeholdern besprochen werden, um Lücken zu identifizieren und die Verfahren zu verbessern.

PR.DS-11.5 **Backups kritischer Systeme (wie Betriebssysteme, Konfigurationen und Anwendungen) werden von Backups kritischer Informationen (wie Geschäftsdaten, Dokumente und Datenbanken) getrennt gehalten, um eine schnellere und zuverlässigere Wiederherstellung zu ermöglichen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, eine schnellere und zuverlässigere Wiederherstellung zu ermöglichen, indem Backups kritischer Systeme (z. B. Betriebssysteme, Konfigurationen, Anwendungen) von Backups kritischer Informationen (z. B. Geschäftsdaten, Dokumente, Datenbanken) getrennt werden.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Backup-Bereiche trennen**
  - System-Backups sollten Betriebssysteme, Konfigurationen, installierte Software und Einstellungen auf Systemebene umfassen.
  - Informations-Backups sollten geschäftskritische Daten wie Datenbanken, Dokumente und Anwendungsdaten umfassen.
- **Individuelle Backup-Methoden verwenden**
  - System-Backups sollten vollständige Images oder Snapshots verwenden, um den kompletten Systemzustand zu erfassen.
  - Informations-Backups sollten inkrementelle oder differentielle Methoden verwenden, um Datenänderungen effizient zu erfassen.
- **Sensible Daten verschlüsseln**
  Sowohl System- als auch Informations-Backups sollten während der Speicherung und Übertragung verschlüsselt werden, insbesondere wenn sie sensible oder regulierte Daten enthalten.
- **Sich an den Wiederherstellungszielen ausrichten**
  Die Trennung der Backups sollte verschiedene Wiederherstellungszeitziele (RTOs) und Wiederherstellungspunktziele (RPOs) berücksichtigen. So kann beispielsweise die Systemwiederherstellung schneller erfolgen als die Wiederherstellung von Geschäftsdaten.
- **Dokumentieren und automatisieren**
  - Backup-Bereiche und -verfahren sollten klar dokumentiert werden.
  - Backup-Prozesse sollten nach Möglichkeit automatisiert werden, um menschliche Fehler zu vermeiden und Einheitlichkeit zu gewährleisten.

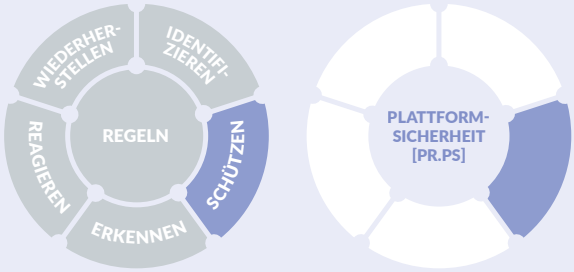
OT-spezifische Überlegungen

In OT-Umgebungen trägt die Trennung von System- und Daten-Backups dazu bei, dass Kontrollsysteme schnell wiederhergestellt werden können, ohne auf die Wiederherstellung großer Datensätze warten zu müssen. Dies unterstützt die Betriebskontinuität und reduziert Ausfallzeiten in kritischen industriellen Prozessen.

Zusammenhang mit PR.DS-11.3 und PR.DS-11.4

PR.DS-11.5 stellt eine Weiterentwicklung – und keine Wiederholung – von PR.DS-11.3 und PR.DS-11.4 dar. Während sich die früheren Kontrollen darauf konzentrieren, wo und wie Backups gespeichert und verifiziert werden, konzentriert sich PR.DS-11.5 darauf, was gesichert wird und wie es logisch getrennt wird, um die Wiederherstellung zu optimieren:

- PR.DS-11.3 stellt sicher, dass Backups sicher und separat aufbewahrt werden.
- PR.DS-11.4 stellt sicher, dass Backups getestet und in die Wiederherstellungsplanung integriert werden.
- PR.DS-11.5 stellt eine funktionale Trennung zwischen System- und Daten-Backups sicher, um eine schnellere und gezieltere Wiederherstellung zu ermöglichen.



Die Hardware, Software (z. B. Firmware, Betriebssysteme, Anwendungen) und Dienste physischer und virtueller Plattformen werden im Einklang mit der Risikostrategie der Organisation verwaltet, um ihre Vertraulichkeit, Integrität und Verfügbarkeit zu schützen

PR.PS-01 Konfigurationsmanagementverfahren werden etabliert und angewendet

PR.PS-01.1 Die Organisation entwickelt, dokumentiert und pflegt eine Basiskonfiguration für ihre geschäftskritischen Systeme.

Implementierungshinweise

Die Kontrolle stellt sicher, dass alle geschäftskritischen Systeme in einem bekannten, sicheren und genehmigten Zustand arbeiten. Eine Basiskonfiguration definiert die Standardeinstellungen für diese Systeme und hilft dabei, unbefugte Änderungen zu erkennen, Sicherheitsrichtlinien durchzusetzen und konsistente Abläufe zu unterstützen.

Um diese Kontrolle zu implementieren, sollten folgende Punkte berücksichtigt werden:

- **Definition des Begriffs „geschäftskritisch"**
  Geschäftskritische Systeme können IT-, OT- (Operational Technology) und möglicherweise IoT- (Internet of Things) Komponenten umfassen, wenn sie wesentliche Geschäftsfunktionen unterstützen:
  - IT-Systeme werden in der Regel intern verwaltet.
  - OT-Systeme können industrielle Kontrollsysteme umfassen.
  - IoT-Systeme (z. B. Sensoren, intelligente Geräte) können geschäftskritisch sein, wenn ihr Ausfall den Betrieb unterbricht oder Sicherheitsrisiken mit sich bringt.
- **Erstellung und Pflege von Basiskonfigurationen**
  Für jedes geschäftskritische System sollte die Basiskonfiguration Folgendes umfassen:
  - Systemkomponenten (z. B. zugelassene Software, Hardware)
  - Betriebssystem- und Anwendungsversionen, einschließlich Patch-Levels
  - Konfigurationseinstellungen und Parameter
  - Netzwerktopologie, aus der hervorgeht, wie die Komponenten miteinander verbunden sind, einschließlich:
    - Externe Verbindungen
    - Server mit sensiblen Daten oder Funktionen
    - DNS- und Sicherheitsservices
    - Logische Anordnung der Komponenten innerhalb der Systemarchitektur
- **Anwendung von Sicherheitsprinzipien**
  - In den Baselines sollte der Grundsatz des geringsten Funktionsumfangs gelten. Nur notwendige Funktionen und Services sollten aktiviert werden.
  - Die Standardeinstellungen sollten überprüft und angepasst werden, um Sicherheitsrisiken bei der Installation oder bei Upgrades zu verringern.
- **Überwachung und Aktualisierung**
  - Kontinuierliche Überwachung der Systeme auf Abweichungen von der genehmigten Baseline.
  - Aktualisierung der Baselines, wenn Systeme gepatcht, aufgerüstet oder neu konfiguriert werden.
- **Cloud- und Anbieter-verwaltete Systeme**
  Bei Systemen, die von Drittparteien verwaltet werden (z. B. Cloud-Services), muss sichergestellt werden, dass die grundlegenden Erwartungen vertraglich festgelegt werden und dass die Anbieter Einblick in die Konfiguration und das Änderungsmanagement gewähren.

PR.PS-01.2 **Die Organisation konfiguriert ihre geschäftskritischen Systeme so, dass sie nur mit den für ihren vorgesehenen Zweck erforderlichen Funktionen betrieben werden. Dazu gehört auch die Überprüfung und Aktualisierung der Basiskonfigurationen, um alle nicht unbedingt erforderlichen Funktionen zu deaktivieren.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, Sicherheitsrisiken und Systemkomplexität zu verringern, indem sichergestellt wird, dass geschäftskritische Systeme so konfiguriert sind, dass sie nur die für ihren Zweck erforderlichen Funktionen ausführen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- Das Prinzip der minimalen Funktionalität anwenden, indem nicht erforderliche Funktionen, Dienste und Komponenten deaktiviert werden.
- Die Basiskonfigurationen regelmäßig überprüfen und aktualisieren, um die betrieblichen Anforderungen und sich entwickelnden Bedrohungen zu berücksichtigen.
- Die folgenden Elemente bewerten und auf das Nötigste beschränken:
  - Installierte Software
  - Aktivierte Dienste
  - Offene Ports
  - Erlaubte Protokolle
  - Systemmerkmale
- Konfigurationen mit Sicherheitsrichtlinien abstimmen, um die Anfälligkeit für Schwachstellen zu minimieren und die Systemleistung zu verbessern.

PR.PS-01.3 **Die Organisation identifiziert und deaktiviert bestimmte Funktionen, Ports, Protokolle und Dienste innerhalb ihrer kritischen Systeme, die für den Geschäftsbetrieb nicht erforderlich sind.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Angriffsfläche kritischer Systeme zu verringern, indem Funktionen, Ports, Protokolle und Dienste, die für den Geschäftsbetrieb nicht unbedingt erforderlich sind, deaktiviert werden.

Um dieses Ziel zu erreichen, sollte die Organisation:

- Systemmerkmale identifizieren, die aufgrund der Rolle des Systems und der damit verbundenen Risiken nicht erforderlich sind.
- Nicht benötigte Elemente deaktivieren, um potenzielle Eintrittspunkte zu begrenzen und die laterale Bewegung innerhalb des Netzes zu verringern.
- Die Konfigurationen regelmäßig bewerten und aktualisieren, um die betrieblichen Anforderungen und sich entwickelnden Bedrohungen zu berücksichtigen.
- Zu den Elementen, bei denen eine Deaktivierung in Betracht kommt, gehören:
  - Bluetooth
  - File Transfer Protocol (FTP)
  - Peer-to-Peer-Vernetzung
  - Andere ungenutzte oder veraltete Dienste

PR.PS-01.4 **Die Organisation trifft technische Sicherheitsvorkehrungen, um eine Richtlinie der „vollständigen Verweigerung“ und „Ausnahmegenehmigung“ durchzusetzen, sodass nur autorisierte Softwareprogramme ausgeführt werden.**

Implementierungshinweise

Das Ziel dieser Kontrolle besteht darin, sicherzustellen, dass nur ausdrücklich autorisierte Software ausgeführt werden darf, um das Risiko zu verringern, dass nicht autorisierte oder schädliche Programme kritische Systeme beeinträchtigen.

Um dieses Ziel zu erreichen, sollte die Organisation Folgendes berücksichtigen:

- Eine Whitelist für Anwendungen implementieren, damit nur zugelassene Software ausgeführt werden kann.
- Gruppenrichtlinien verwenden, um Anwendungssteuerungsregeln systemübergreifend durchzusetzen.
- Software Restriction Policies (SRP) oder ähnliche Mechanismen zur Blockierung nicht autorisierter Software auf der Grundlage von Dateipfad, Hash oder digitaler Signatur anwenden.
- Eine role-based Access Control (RBAC) implementieren, um sicherzustellen, dass nur autorisierte Benutzer bestimmte Anwendungen ausführen können.
- Den Java Security Manager konfigurieren, um einzuschränken, welche Klassen und Methoden in Java-basierten Umgebungen ausgeführt werden können.
- Konfigurationsmanagement-Tools zur konsistenten Durchsetzung von autorisierter Software in allen Systemen verwenden.

PR.PS-01.5 **Nicht autorisierte Konfigurationsänderungen an den Systemen der Organisation werden überwacht und mit geeigneten Maßnahmen zur Risikominderung behandelt.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, nicht autorisierte Konfigurationsänderungen, die die Systemintegrität oder -verfügbarkeit gefährden könnten, zu erkennen und darauf zu reagieren.

Um dieses Ziel zu erreichen, sollte die Organisation Folgendes in Betracht ziehen:

- Überwachung von Konfigurationsänderungen im Einklang mit festgelegten Richtlinien und Verfahren.
- Erkennung und Protokollierung unbefugter Änderungen an Systemeinstellungen.
- Benachrichtigung des zuständigen Personals bei unbefugten Änderungen.
- Stellen Sie genehmigte Konfigurationen umgehend wieder her, um die Betriebsstabilität aufrechtzuerhalten.
- Halten Sie in kritischen Fällen die betroffenen Systemprozesse an, um weitere Auswirkungen zu verhindern.
- Konsultieren Sie die Anleitung in den ENISA NIS2 Technical Implementation Guidance (neueste Version), die eine kontinuierliche Überwachung und umgehende Abmilderung unbefugter Änderungen empfiehlt, um die Widerstandsfähigkeit des Systems und die Einhaltung der Vorschriften zu gewährleisten.

PR.PS-02 Die Software wird entsprechend dem Risiko gewartet, ersetzt und entfernt

PR.PS-02.1 Die Organisation setzt Beschränkungen für die Nutzung und Installation von Software durch und stellt sicher, dass Software auf der Grundlage des mit ihr verbundenen Risikos gewartet, ersetzt oder entfernt wird.

Implementierungshinweise

Ziel dieser Kontrolle ist es, Sicherheits- und Betriebsrisiken zu verringern, indem kontrolliert wird, welche Software verwendet wird, und sichergestellt wird, dass sie ordnungsgemäß gewartet und entfernt wird, wenn sie nicht mehr benötigt oder unterstützt wird.

Um dieses Ziel zu erreichen, sollte die Organisation Folgendes in Betracht ziehen:

- Nur zugelassene Software zulassen und den Zugriff auf der Grundlage von Benutzerrollen und Zuständigkeiten beschränken.
- Nicht mehr unterstützte oder auslaufende Software ersetzen, um ungepatchte Sicherheitslücken zu vermeiden.
- Deinstallation von ungenutzter oder unnötiger Software, einschließlich veralteter Betriebssystem-Dienstprogramme, um die Angriffsfläche zu verringern.
- Anwendung von Patches auf der Basis des Risikos:
  - Kritische Schwachstellen sollten innerhalb weniger Stunden gepatcht werden.
  - Routinemäßige Aktualisierungen sollten einem festgelegten Zeitplan folgen (z. B. wöchentlich oder monatlich).
- In Container-Umgebungen sollten nur vertrauenswürdige und aktuelle Images verwendet werden; veraltete Container sollten ersetzt werden.
- Entfernung oder Deaktivierung von Software und Services, die ein inakzeptables Risiko darstellen, wie beispielsweise FTP- oder Peer-to-Peer-Tools, sofern diese nicht ausdrücklich erforderlich und gesichert sind.
- Sicherstellung, dass die SPS-Programmierung in ICS/OT-Umgebungen vorab genehmigt und geplant wird; Vermeidung von Ad-hoc-Änderungen zum Schutz der Betriebssicherheit.
- Führen eines Softwareinventars mit Versions- und Supportstatus.
- Festlegung von Verfahren für die Genehmigung, das Patchen, den Austausch und die Entfernung von Software.

PR.PS-03 Hardware wird entsprechend dem Risiko gewartet, ersetzt und entfernt

PR.PS-03.1 Hardware, die in geschäftskritischen Umgebungen eingesetzt wird, wird auf der Grundlage des mit ihr verbundenen Sicherheits- und Betriebsrisikos gewartet, ersetzt oder entfernt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die in geschäftskritischen Umgebungen verwendete Hardware sicher, zuverlässig und zweckmäßig bleibt, indem sie auf der Grundlage von Betriebs- und Sicherheitsrisiken verwaltet wird.

Um dieses Ziel zu erreichen, sollte die Organisation Folgendes in Betracht ziehen:

- Regelmäßige Überprüfung, ob die Hardware die erforderlichen Sicherheitsfunktionen (z. B. Verschlüsselung, sicherer Start, Firmware-Updates) unterstützt; Austausch von Hardware, die diese Anforderungen nicht erfüllt.
- Kontrolliertes Ausmustern von veralteter oder nicht mehr unterstützter Hardware.
- Definition und Pflege eines Hardware-Lebenszyklusplans, einschließlich:
  - Verfolgung der Bestände
  - Zeitpläne für das Ende der Nutzungsdauer
  - Zeitpläne für die Ersetzung
  - Sichere Entsorgungsverfahren
- Durchführung von vorbeugenden Wartungsarbeiten und rechtzeitigen Austauschmaßnahmen, um unerwartete Ausfälle zu vermeiden, die den Betrieb oder die Sicherheit beeinträchtigen könnten.
- Sicherstellung, dass die Hardware sichere, aktuelle Software unterstützt; etwaige Einschränkungen, die dies verhindern, beseitigen.

PR.PS-04 Log-Protokolle werden erstellt und für die kontinuierliche Überwachung zur Verfügung gestellt

PR.PS-04.1 Protokolle werden geführt, dokumentiert und überwacht.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Protokolle konsistent geführt, dokumentiert und überwacht werden, um die Sichtbarkeit, Rechenschaftspflicht und frühzeitige Erkennung von Anomalien oder Bedrohungen zu unterstützen.

Um dieses Ziel zu unterstützen, sollte die Organisation:

- **Eine systemübergreifende Protokollierung aktivieren**
  Alle Betriebssysteme, Anwendungen, Services (auch Cloud-basierte) und Sicherheitstools (z. B. Firewalls, Antivirenprogramme) sollten so konfiguriert sein, dass sie Protokolldateien erzeugen.
- **Eine Vielzahl von Protokolltypen einbeziehen**
  Die Protokolle sollten, falls zutreffend, Folgendes umfassen: Audit-Protokolle, Ereignisprotokolle, Anwendungsprotokolle, Sicherheitsprotokolle, Systemprotokolle und Wartungsprotokolle.
- **Protokolldaten schützen**
  Die Protokolle sollten durch Verschlüsselung und Zugriffskontrollen vor unbefugtem Zugriff geschützt werden.
- **Backups erstellen und Protokolle aufbewahren**
  Protokoll-Backups sollten regelmäßig durchgeführt und für einen vordefinierten Zeitraum aufbewahrt werden, basierend auf den geschäftlichen Anforderungen oder gesetzlichen Vorschriften.
- **Die Protokolle auf Anomalien überprüfen**
  Protokolle sollten überprüft werden, um ungewöhnliche Muster oder Verhaltensweisen zu erkennen, wie beispielsweise wiederholte Malware-Erkennungen oder übermäßiger Zugriff auf nicht geschäftliche Websites.
- **Aufbewahrungsfristen definieren**
  Aufbewahrungsfristen für Protokolle sollten klar definiert sein. Die sektorspezifischen Anforderungen sollten berücksichtigt werden.
- **Die Überwachung und Rechenschaftspflicht unterstützen**
  Es sollte eine Überwachung vorhanden sein, die einen Einblick in die Systemaktivitäten ermöglicht und eine wirksame Prüfung und Reaktion auf Vorfälle unterstützt.
- **OT-Systeme einbeziehen**
  Die Protokollierungspraktiken sollten sich auch auf OT-Umgebungen erstrecken, einschließlich industrieller Kontrollsysteme, in denen Protokolle dazu beitragen können, Betriebsanomalien oder unbefugte Zugriffsversuche zu erkennen.

PR.PS-04.2 **Die Organisation stellt sicher, dass Protokollaufzeichnungen eine maßgebliche Zeitquelle oder einen Zeitstempel der internen Uhr enthalten, der mit einer maßgeblichen Zeitquelle verglichen und synchronisiert wird.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Protokolleinträge in allen Systemen eine einheitliche und zuverlässige Zeitreferenz verwenden, so dass die Ereignisse genau verfolgt und miteinander in Beziehung gesetzt werden können.

Um dieses Ziel zu erreichen, sollte die Organisation Folgendes in Betracht ziehen:

- Verwendung einer zuverlässigen Zeitreferenz wie einer GPS-Uhr, eines internen Zeitservers oder einer anderen vertrauenswürdige Quelle, um die Systemuhren zu synchronisieren.
- Die Konfiguration der Systeme zur regelmäßigen Aktualisierung ihrer Uhren, um eine Zeitverschiebung zu vermeiden.
- Die Einrichtung mehrerer Zeitquellen, um Redundanz und Genauigkeit zu gewährleisten.
- Die Überwachung des Synchronisationsstatus und Auslösung von Warnungen, wenn die Systeme nicht mehr synchron sind.
- Die Dokumentation von Verfahren für die Zeitsynchronisation, einschließlich Servereinstellungen, Aktualisierungsintervalle und Überwachungsprozesse.

PR.PS-04.3 **Auditdaten aus den kritischen Systemen der Organisation werden auf ein alternatives System übertragen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Integrität der Prüfungsaufzeichnungen zu schützen, indem sie von kritischen Systemen an einen separaten, sicheren Ort übertragen werden, wo sie nicht verändert oder manipuliert werden können.

Um dieses Ziel zu erreichen, sollte die Organisation Folgendes in Betracht ziehen:

- Die Übertragung von Audit-Daten in ein separates System, in dem die Datensätze nicht von Benutzern oder Services des ursprünglichen Systems geändert werden können.
- Die Sicherstellung, dass das Zielsystem die einmal gespeicherten Prüfungsaufzeichnungen unverändert beibehält.
- Die Überwachung der Auswirkungen von Protokollübertragungen, um Leistungsprobleme auf den Quellsystemen zu vermeiden.
- Die Einführung von Maßnahmen zum Schutz der Daten, ohne den Systembetrieb zu verlangsamen oder zu stören.

PR.PS-04.4 **Die Organisation stellt sicher, dass Fehler in der Auditverarbeitung in den Systemen der Organisation Warnmeldungen erzeugen und definierte Reaktionen auslösen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass jeder Fehler in der Audit-Protokollierung, wie z. B. Fehler bei der Protokollerfassung, -verarbeitung oder -speicherung, Warnmeldungen und vordefinierte Reaktionen auslöst, um die Systemintegrität und Nachvollziehbarkeit zu gewährleisten.

Um dieses Ziel zu erreichen:

- Zu den Audit-Fehlern gehören Software- oder Hardware-Probleme, defekte Protokollierungsmechanismen oder ein voller Speicher.
- Beim Auftreten solcher Fehler sollten automatisch Warnmeldungen generiert und vordefinierte Maßnahmen ausgelöst werden, um sie zu beheben.
- Jedes Audit-Protokoll-Repository, ob auf einem Server, einer Firewall oder einer Anwendung, sollte einzeln und gemeinsam überwacht werden.
- System Logging Protocol (Syslog)-Server oder ähnliche zentralisierte Protokollierungslösungen sollten verwendet werden, um eine zuverlässige Protokollerfassung und Alarmierung zu unterstützen.
- Systeme, die Protokolle erstellen, sollten so konfiguriert sein, dass sie detaillierte Aktivitäts-, Zugangs- und Verhaltensdaten erfassen, um die Grundsätze des „Zero-Trust“ zu unterstützen.
- Audit-Protokolle sollten kontinuierlich überwacht werden, um ihre Verfügbarkeit und Integrität sowie eine ausreichende Speicherkapazität zu gewährleisten.

PR.PS-04.5 **Die Organisation stellt sicher, dass autorisierte Mitarbeiter die Auditprotokollierungs- und Überwachungsmöglichkeiten erweitern oder verbessern kann, wenn dies zur Unterstützung von Untersuchungen oder der Reaktion auf Vorfälle erforderlich ist.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Audit-Protokollierung schnell angepasst werden kann, um bei Sicherheitsvorfällen oder Untersuchungen mehr Transparenz zu schaffen, ohne den normalen Betrieb zu stören.

Um dieses Ziel zu erreichen:

- Sollten Audit-Protokollierungssysteme Anpassungen nach Bedarf ermöglichen, z. B. die Erhöhung der Protokolldetails, die Verlängerung der Aufbewahrungszeit oder die Erweiterung des Erfassungsbereichs.
- Sollte autorisiertes Personal und Bedingungen für die Aktivierung der erweiterten Protokollierung klar definiert werden.
- Sollten die Aktivierungsverfahren Genehmigungen, Dokumentation und Änderungsverfolgung umfassen.
- Sollten die Protokolleinträge in allen IKT- und OT-Systemen regelmäßig auf ihre Richtigkeit und Vollständigkeit überprüft werden.
- Sollten Richtlinien sicherstellen, dass eine erweiterte Protokollierung nur in begründeten Fällen erfolgt und ordnungsgemäß aufgezeichnet wird.
- Sollten technische Kapazitäten, Eskalationswege und die Verfügbarkeit von Personal im Voraus geplant werden, um eine rechtzeitige Aktivierung zu ermöglichen.

PR.PS-05 Installation und Ausführung nicht autorisierter Software wird verhindert

PR.PS-05.1 Web- und E-Mail-Filter werden installiert und verwendet.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko von Malware-Infektionen, Phishing-Angriffen und Datenschutzverletzungen zu verringern, indem effektive Web- und E-Mail-Filterlösungen implementiert und gepflegt werden.

Um dieses Ziel zu unterstützen, sollte die Organisation:

- **Web-Filter implementieren**
  Web-Filter sollten verwendet werden, um den Zugang zu Websites auf der Grundlage von Folgendem zu kontrollieren:
  - Vordefinierte Erlaubnis-/Blockierlisten (z. B. nach URL oder Domäne)
  - Inhaltsanalyse in Echtzeit zur Erkennung bösartiger oder unangemessener Inhalte
  - Techniken wie URL-Filterung, Inhaltsfilterung, DNS-Filterung und client- oder serverseitige Filterung
- **E-Mail-Filter konfigurieren**
  E-Mail-Filter sollten so konfiguriert werden, dass sie:
  - Spam, Phishing-Versuche und schädliche Anhänge oder Links blockieren
  - Eingehende E-Mails (z. B. Newsletter, Benachrichtigungen über soziale Medien) kategorisieren, um die Überladung zu verringern und die Aufmerksamkeit zu erhöhen
  - Zur Verbesserung der E-Mail-Sicherheit nach bekannten Bedrohungen und verdächtigen Mustern scannen
- **Filter auf dem neuesten Stand halten**
  Filterregeln und Bedrohungsdatenbanken sollten regelmäßig aktualisiert werden, um auf neue Bedrohungen zu reagieren.
- **Mit Sicherheitsrichtlinien integrieren**
  Web- und E-Mail-Filter sollten auf die allgemeinen Sicherheitsrichtlinien und Sensibilisierungsmaßnahmen des Unternehmens abgestimmt werden.
- **OT-Überlegungen einbeziehen**
  In OT-Umgebungen sollte der Internet- und E-Mail-Zugang auf das betrieblich Notwendige beschränkt werden. Alle Systeme mit externen Verbindungen sollten gefiltert werden, um zu verhindern, dass sie Bedrohungen ausgesetzt werden.

PR.PS-05.2 Die Installation und Ausführung nicht autorisierter Software wird verhindert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko einer Kompromittierung zu verringern, indem sichergestellt wird, dass nur vertrauenswürdige und genehmigte Software auf den Systemen installiert und ausgeführt wird.

Um dieses Ziel zu erreichen:

- Sollte die Installation und Ausführung von Software auf zuvor genehmigte Anwendungen und Umgebungen beschränkt werden.
- Sollten die Plattformen so konfiguriert werden, dass sie nicht autorisierte Software blockieren und die Ausführung einschränken, wenn das Risiko dies rechtfertigt.
- Sollte die Quelle und Integrität aller neuen Software vor der Installation überprüft werden.
- Sollte der Zugang zu schädlichen Websites über vertrauenswürdige und zugelassene Internet-Filterdienste blockiert werden, die dafür ausgelegt sind, bekannte Online-Bedrohungen zu erkennen und zu stoppen.
- Sollten die Systeme, wenn möglich, so konfiguriert werden, dass nur von der Organisation zugelassene Software installiert werden kann.

PR.PS-06 Sichere Softwareentwicklungspraktiken sind integriert, und ihre Leistung wird während des gesamten Softwareentwicklungszyklus überwacht

PR.PS-06.1 Die Sicherheit wird während des gesamten Lebenszyklus von Systemen und Anwendungen berücksichtigt, unabhängig davon, ob diese intern entwickelt oder extern erworben wurden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Sicherheit von Anfang an in die Systeme und Anwendungen integriert und während ihrer gesamten Lebensdauer – vom Entwurf bis zur Stilllegung – aufrechterhalten wird, unabhängig davon, ob sie intern entwickelt oder gekauft wurden.

Um dieses Ziel zu erreichen:

- **Initiierungsphase:**
  Die Sicherheitsanforderungen sollten frühzeitig definiert, die Risiken identifiziert und die relevanten Stakeholder, einschließlich der Sicherheitsexperten, von Anfang an einbezogen werden.
- **Akquisitions- oder Entwicklungsphase:**
  - Für akquirierte Lösungen: Die Anbieter sollten sichere Entwicklungsverfahren anwenden, Tests nachweisen und die vertraglichen Sicherheitsanforderungen erfüllen.
  - Für die interne Entwicklung: Es sollten sichere Kodierungsverfahren angewandt, Änderungen verwaltet und Sicherheitstests durchgeführt werden.
- **Implementierungsphase:**
  Die Systeme sollten vor dem Einsatz sicher konfiguriert werden, wobei Zugangskontrollen und Verschlüsselung zum Schutz sensibler Daten eingesetzt werden sollten.
- **Betriebs- und Wartungsphase:**
  Die Systeme sollten auf Vorfälle überwacht, regelmäßig aktualisiert und die Sicherheitskontrollen überprüft und bei Bedarf verbessert werden.
- **Entsorgungsphase:**
  Die Systeme sollten sicher außer Betrieb genommen, sensible Daten entfernt und die gewonnenen Erkenntnisse dokumentiert werden, um künftige Prozesse zu verbessern.

PR.PS-06.2 Änderungen und Ausnahmen werden getestet und validiert, bevor sie in operative Systeme implementiert werden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko von Unterbrechungen oder Schwachstellen zu verringern, indem sichergestellt wird, dass alle Änderungen und Ausnahmen ordnungsgemäß getestet und validiert werden, bevor sie auf die operativen Systeme angewendet werden.

Um dieses Ziel zu erreichen:

- Sollten alle vorgeschlagenen Änderungen und Ausnahmen einem formellen Prozess folgen, der Dokumentation, Überprüfung, Test und Genehmigung umfasst.
- Sollten die potenziellen Risiken der Anwendung bzw. Nichtanwendung einer Änderung bewertet und aufgezeichnet werden.
- Sollten Ausnahmen, definiert als genehmigte Abweichungen von Standardrichtlinien oder -verfahren, mit einem klaren Verständnis der Risiken und einem definierten Plan zu deren Verringerung oder Bewältigung bewertet werden.
- Sollten akzeptierte Risiken regelmäßig überprüft werden, um zu bestätigen, dass die ursprüngliche Entscheidung, sie zu akzeptieren, weiterhin gültig ist, insbesondere wenn sich die Bedingungen ändern oder wenn die Akzeptanz auf zukünftigen Aktionen oder Meilensteinen beruhte.
- Diese Praktiken sollten an das betriebliche Umfeld angepasst werden, um ungeplante Ausfallzeiten oder Sicherheitsprobleme zu vermeiden, insbesondere bei OT-Systemen.

PR.PS-06.3 **Sichere Softwareentwicklungspraktiken werden in alle Phasen des Softwareentwicklungslebenszyklus integriert, und ihre Wirksamkeit wird regelmäßig überwacht und verbessert.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Sicherheitsrisiken in der Software zu verringern, indem Schutzmaßnahmen in die gesamte Entwicklung eingebettet und auf der Grundlage der Leistung und der sich entwickelnden Bedrohungen kontinuierlich verbessert werden.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Sicherheit in den Entwicklungslebenszyklus integrieren**
  - Sichere Codierungsstandards und vertrauenswürdige Entwicklungsrahmen sollten angewendet werden.
  - Bedrohungsmodelle sollten frühzeitig erstellt werden, um Risiken zu identifizieren und zu reduzieren.
  - Alle Softwarekomponenten sollten vor Manipulationen und unbefugtem Zugriff geschützt werden.
  - Die Zugangskontrollen für Datenbanken und sensible Daten sollten durchgesetzt werden.
  - Software-Abhängigkeiten und Bibliotheken sollten auf dem neuesten Stand gehalten werden.
  - Veraltete oder nicht verwendete Software sollte sicher entfernt werden.
- **Überwachung der Wirksamkeit von Sicherheitspraktiken**
  - Metriken sollten definiert und verfolgt werden, wie z. B.:
    - Während der Entwicklung gefundene Schwachstellen im Vergleich zu denen in der Produktion.
    - Zeitaufwand für die Behebung festgestellter Probleme.
    - Prozentsatz des Codes, der auf Sicherheit geprüft oder getestet wurde.
    - Teilnahme von Entwicklern an Schulungen zur sicheren Kodierung.
  - Diese Metriken sollten dazu genutzt werden, Lücken zu ermitteln und die Verfahren zu verbessern.
- **Aufbau von Sicherheitsbewusstsein**
  Entwickler und technische Teams sollten regelmäßig Schulungen über sichere Kodierung und Designprinzipien erhalten.
- **Erhaltung und Verbesserung**
  Sichere Entwicklungspraktiken sollten auf der Grundlage von Folgendem überprüft und aktualisiert werden:
  - Neue Bedrohungen oder Schwachstellen.
  - Erkenntnisse aus Vorfällen oder Audits.
  - Branchenstandards und bewährten Verfahren.

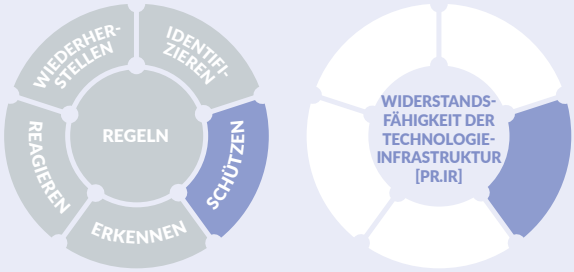
PR.PS-06-4 **Für geplante Änderungen an den kritischen Systemen der Organisation wird eine Analyse der Sicherheitsauswirkungen in einer separaten Testumgebung durchgeführt, bevor die Implementierung in einer Betriebsumgebung erfolgt.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, unbeabsichtigte Sicherheitsrisiken zu vermeiden, indem geplante Änderungen an kritischen Systemen vor der Einführung in einer kontrollierten Umgebung getestet werden.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Das Test-Szenario planen**
  - Sicherheitsrisiken für Systeme, Vermögenswerte, Prozesse und Personen sollten identifiziert werden.
  - Geplante Konfigurationsänderungen oder Systemmodifikationen sollten auf ihre möglichen Auswirkungen auf die Sicherheit hin analysiert werden.
- **Die Testumgebung vorbereiten**
  - Testdaten sollten realistische Betriebsszenarien widerspiegeln.
  - Hardware-, Software- und Netzwerkanforderungen sollten klar definiert sein.
  - Die Testumgebung sollte in Bezug auf Einrichtung und Konfiguration weitgehend die Produktionsumgebung widerspiegeln.
  - Für die Testaktivitäten sollte ausreichend Speicherplatz zur Verfügung stehen.
  - Softwareversionen in der Testumgebung sollten mit denen der Produktionsumgebung übereinstimmen.
- **Sicherheit und Wartungsfreundlichkeit sicherstellen**
  - Die Software in der Testumgebung sollte regelmäßig aktualisiert werden, um bekannte Schwachstellen zu beheben.
  - Virtualisierung oder Containerisierung sollten genutzt werden, um konsistente und replizierbare Umgebungen zu schaffen.
  - Isolated Virtual Machines (VMs) sollten verwendet werden, um Interferenzen mit Betriebssystemen zu vermeiden.
  - In der Testumgebung sollten Sicherheitskontrollen wie Firewalls und Zugangsbeschränkungen implementiert werden.



Sicherheitsarchitekturen werden im Einklang mit der Risikostrategie der Organisation verwaltet, um die Vertraulichkeit, Integrität und Verfügbarkeit von Vermögenswerten sowie die Widerstandsfähigkeit der Organisation zu schützen

PR.IR-01 Netzwerke und Umgebungen sind vor unberechtigtem logischen Zugriff und unbefugter Nutzung geschützt.

PR.IR-01.1 In allen von der Organisation genutzten Netzwerken werden Firewalls installiert, konfiguriert und aktiv gewartet, um vor unbefugtem Zugriff und Cyber-Bedrohungen zu schützen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle von der Organisation genutzten Netzwerke durch die Installation, Konfiguration und aktive Wartung von Firewalls vor unbefugtem Zugriff und Cyber-Bedrohungen geschützt sind.

Diese Kontrolle konzentriert sich auf die Installation, Konfiguration und Wartung von netzbasierten Firewalls, um den unbefugten Zugriff durch Überwachung und Kontrolle des Datenverkehrs, der in das Netz eintritt oder es verlässt, zu verhindern (Schwerpunkt: Kontrolle und Prävention). Im Gegensatz dazu befasst sich die Kontrolle DE.CM-01.1 mit hostbasierten Firewalls, die dazu beitragen, Bedrohungen zu erkennen, die den Netzrand umgehen, indem sie den Datenverkehr zu und von einzelnen Geräten überwachen (Schwerpunkt: Sichtbarkeit und Erkennung).

Um diese Kontrolle zu implementieren, sollte die Organisation:

- Die Netzwerkgrenzen schützen
  - Zwischen dem internen Netzwerk und dem Internet sollte eine Firewall installiert werden. Diese kann in einen drahtlosen Zugangspunkt, einen Router oder ein vom ISP bereitgestelltes Gerät integriert werden.
  - Firewalls sollten auf der Grundlage einer grundlegenden Sicherheitsrichtlinie konfiguriert werden, die nach dem Prinzip „alles standardmäßig verweigern, nur Ausnahmen zulassen“ funktioniert.
- Endpunktgeräte sichern
  - Auf allen Endpunktgeräten, einschließlich Laptops, Smartphones und anderen vernetzten Systemen, sollte eine Software-Firewall installiert und regelmäßig aktualisiert werden.
  - Lokale Firewalls sollten auch bei der Nutzung von VPNs oder Cloud-Services aktiv bleiben.
- Arbeitsumgebungen für Heim- und Remote-Arbeit sichern
  - Für Heimnetzwerke, die für Telearbeit genutzt werden, sollten Router mit integrierten Firewalls verwendet werden, die aktiviert, sicher konfiguriert und auf dem neuesten Stand gehalten werden sollten.
  - Software-Firewalls sollten auf allen Remote-Arbeitsgeräten aktiv und aktualisiert sein.
  - Die Standard-Administrator-Anmeldedaten für Heimrouter sollten regelmäßig geändert und aktualisiert werden.

- **Umgebungen für Betriebstechnik (OT) schützen**
  - Der Fernzugriff auf OT-Systeme sollte als Zugriff durch Drittparteien und nicht als normale Telearbeit behandelt werden.
  - Es sollte eine klare Trennung zwischen IT- und OT-Netzen durchgesetzt werden.
  - Wenn ein IT-zu-OT-Zugang erforderlich ist, sollte er über einen sicheren Jump-Host erfolgen, der sich in einer speziellen DMZ befindet.
- **Die Erkennung mit IDPS verbessern**
  Ein Intrusion Detection and Prevention System (IDPS) sollte in Betracht gezogen werden, um den Netzwerkverkehr auf verdächtige Aktivitäten zu überwachen und zu analysieren und den Gesamtschutz zu verbessern.

PR.IR-01.2 Um kritische Systeme zu schützen, implementieren Organisationen Netzwerksegmentierung und -trennung entsprechend den Vertrauensgrenzen und der Kritikalität der Ressourcen, wodurch die Ausbreitung von Bedrohungen begrenzt und eine strenge Zugriffskontrolle durchgesetzt wird

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Ausbreitung von Cyber-Bedrohungen zu begrenzen und eine strenge Zugangskontrolle durchzusetzen, indem eine Netzwerksegmentierung und -trennung auf der Grundlage von Vertrauensgrenzen und der Kritikalität von Systemen eingeführt wird.

Um diese Kontrolle zu implementieren, sollten folgende Punkte berücksichtigt werden:

- **Definition von Sicherheitszonen**
  Netzwerke sollten in verschiedene Zonen unterteilt werden (z. B. Büro, Produktion, Gäste, Mobil). Der Verkehr zwischen den Zonen sollte überwacht und kontrolliert werden, zum Beispiel durch Firewalls.
- **Ausrichtung der Segmentierung an Vertrauen und Kritikalität**
  Die Segmentierung sollte widerspiegeln, welche Benutzer und Systeme vertrauenswürdig sind und wie kritisch die einzelnen Güter sind. Nach dem Prinzip des geringsten Privilegs sollte nur die unbedingt notwendige Kommunikation zwischen den Zonen erlaubt sein.
- **Vermeidung von flachen Netzwerken**
  Flache Netzwerke sollten vermieden werden, da die Kompromittierung eines Systems die gesamte Umgebung gefährden könnte. Die Segmentierung soll dazu beitragen, Bedrohungen innerhalb einer einzigen Zone einzudämmen.
- **Trennung von IT- und OT-Umgebungen**
  In Umgebungen mit industriellen Systemen (OT) sollten Büro- und Produktionsnetzwerke getrennt werden. Gast- und mobile Netzwerke sollten keinen direkten Zugang zu internen Büro- oder Produktionssystemen haben. Die Segmentierung sollte der Norm IEC 62443 entsprechen, insbesondere den Anforderungen SR 5.1 bis SR 5.3.
- **Vorsichtige Nutzung von VLANs**
  VLANs sollten nur als Teil einer umfassenderen Defense-in-Depth-Strategie eingesetzt werden. Sie sollten nicht allein zur Erfüllung der Anforderungen der Sicherheitsstufe 2 gemäß IEC 62443-3-3 herangezogen werden. VLANs sollten mit Firewalls, Zugangskontrollen und Überwachung kombiniert werden.
- **Durchsetzung der Segmentierung mit Firewalls**
  Firewalls sollten so konfiguriert werden, dass sie standardmäßig jeglichen Datenverkehr blockieren und nur bestimmte, genehmigte Verbindungen zulassen. Die Segmentierung und Abtrennung sollte durch gut gepflegte Firewall-Regeln in Übereinstimmung mit der Kontrolle PR.IR-01.1 durchgesetzt werden.
- **Segmentierung vs. Trennung verdeutlichen**
  - Die Segmentierung sollte dazu dienen, Netzwerke logisch zu unterteilen und den Verkehr zwischen den Zonen zu steuern.
  - Die Trennung sollte dort angewendet werden, wo Systeme isoliert werden müssen, ohne dass eine direkte Kommunikation stattfindet, es sei denn, dies ist ausdrücklich erlaubt.

PR.IR-01.3 **Um die Betriebsstabilität und -sicherheit zu gewährleisten, identifiziert, dokumentiert und kontrolliert die Organisation ausnahmslos alle Verbindungen zwischen den Komponenten ihrer kritischen Systeme.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die betriebliche Stabilität und Sicherheit aufrechtzuerhalten, indem sichergestellt wird, dass alle Verbindungen zwischen Komponenten kritischer Systeme bekannt, dokumentiert und aktiv verwaltet werden.

In OT-Umgebungen können undokumentierte oder unkontrollierte Verbindungen – ob physisch, drahtlos oder logisch – Schwachstellen verursachen, Prozesse stören oder Sicherheitsmechanismen umgehen.

Um die Netzwerkverbindungen zwischen den Systemkomponenten effektiv zu verwalten und zu sichern, sollten die folgenden Praktiken berücksichtigt werden:

- **Konfigurationsmanagement**
  Organisationen sollten Konfigurationsmanagementprozesse einführen, um sicherzustellen, dass alle Änderungen an Netzverbindungen dokumentiert, überprüft und genehmigt werden. Konfigurationsdateien und Protokolle sollten auf dem neuesten Stand gehalten und sicher aufbewahrt werden.
- **Zugangskontrollen**
  Es sollten strenge Zugangskontrollen durchgesetzt werden, um sicherzustellen, dass nur befugte Mitarbeiter die Netzkonfigurationen ändern können. Eine rollenbasierte Zugriffskontrolle (RBAC) sollte verwendet werden, um den Zugriff auf der Grundlage von Arbeitsaufgaben und betrieblichen Erfordernissen zu beschränken.
- **Regelmäßige Audits**
  Regelmäßige Audits sollten durchgeführt werden, um zu überprüfen, ob alle dokumentierten Verbindungen korrekt sind und ob keine unbefugten Änderungen vorgenommen wurden. Die Auditergebnisse sollten dazu genutzt werden, die Dokumentation zu aktualisieren und die Kontrollen zu verstärken.
- **Verbindung zum Asset Management (ID.AM)**
  Verbindungen zwischen Systemkomponenten sollten unter ID.AM (Asset Management) dokumentiert und unter dieser Anforderung (PR.IR-01.3) kontrolliert werden, um Konsistenz, Nachvollziehbarkeit und Durchsetzbarkeit in der gesamten Cybersicherheitsarchitektur der Organisation zu gewährleisten.

PR.IR-01.4 **Die Organisation implementiert angemessene Maßnahmen zum Schutz der Grenzen, um die Kommunikation an den externen und wichtigen internen Grenzen ihrer kritischen Systeme sowohl in IT- als auch in OT-Umgebungen zu überwachen und zu kontrollieren und so einen sicheren und zuverlässigen Betrieb zu gewährleisten.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, einen sicheren und zuverlässigen Betrieb zu gewährleisten, indem die Kommunikation an wichtigen Netzwerkgrenzen aktiv überwacht und kontrolliert wird - insbesondere dort, wo kritische Systeme mit externen Netzwerken oder weniger vertrauenswürdigen internen Zonen verbunden sind.

In OT-Umgebungen, in denen Altsysteme oft nicht über integrierte Sicherheitsfunktionen verfügen, ist ein Grenzschutz unerlässlich, um unbefugten Zugriff zu verhindern, potenzielle Bedrohungen einzudämmen und die Prozessintegrität zwischen IT- und OT-Bereichen aufrechtzuerhalten.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Geräte zum Schutz von Grenzen**
  Firewalls, Sicherheits-Gateways und Router sollten an externen und internen Grenzen eingesetzt werden, um Richtlinien zur Filterung und Weiterleitung von Datenverkehr durchzusetzen. Diese Geräte sollten nach dem Modell „standardmäßig verweigern, ausnahmsweise zulassen“ arbeiten.
- **Zonierung und Isolierung in OT-Umgebungen**
  In OT-Umgebungen sollte der Grenzschutz eine strikte Trennung zwischen Steuerungssystemen und externen Netzwerken beinhalten. Zonen sollten auf der Grundlage von Kritikalität und Vertrauen definiert werden, und die Kommunikation zwischen Zonen sollte streng kontrolliert und überwacht werden.
- **Unidirektionale Gateways (Datendioden)**
  Wenn Daten von sicheren OT-Systemen zu externen Zielen (z. B. Cloud-Services oder Regulierungsbehörden) fließen müssen, sollten unidirektionale Gateways verwendet werden, um eingehende Bedrohungen zu verhindern und gleichzeitig die Übertragung ausgehender Daten zu ermöglichen.
- **Verschlüsselte Kommunikation**
  Die grenzüberschreitende Kommunikation sollte mit sicheren Protokollen (z. B. VPNs, TLS) verschlüsselt werden, um die Daten während der Übertragung zu schützen und Vertraulichkeit und Integrität zu gewährleisten.
- **Intrusion Detection and Prevention**
  Intrusion Detection and Prevention Systems (IDPS) sollten an wichtigen Grenzen eingesetzt werden, um den Datenverkehr auf Anomalien zu überwachen, unbefugte Zugriffsversuche zu erkennen und bösartige Aktivitäten zu blockieren.
- **Durchsetzung der Zugangskontrolle**
  Der Zugang zu Grenzgeräten und Kommunikationskanälen sollte auf befugte Mitarbeiter beschränkt werden. Network Access Control-Lösungen (NAC-Lösungen) sollten in Betracht gezogen werden, um die Authentifizierung von Geräten und Benutzern an den Zugangspunkten durchzusetzen.
- **Kontinuierliche Überwachung und kontinuierliches Patching**
  Grenzgeräte und Kommunikationskanäle sollten kontinuierlich auf verdächtige Aktivitäten überwacht werden. Alle Systeme, die der externen oder zonenübergreifenden Kommunikation ausgesetzt sind, sollten regelmäßig aktualisiert und gepatcht werden, um bekannte Sicherheitslücken zu schließen.

PR.IR-01.5 **Die Organisation implementiert, soweit möglich, authentifizierte Proxy-Server oder Firewalls mit URL-Filterung und Fähigkeiten zur Erkennung von Bedrohungen für definierten Kommunikationsverkehr zwischen ihren kritischen Systemen und externen Netzwerken.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, das Risiko des Eindringens von Cyber-Bedrohungen in kritische Systeme zu verringern, indem die ausgehende und eingehende Kommunikation über authentifizierte Proxys oder Firewalls gefiltert und geprüft wird.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Zugangskontrollen**
  Proxy-Server und Firewalls sollten strenge Zugangskontrollen durchführen und nur autorisierte Benutzer und Systeme zulassen. Zur Unterstützung des Null-Vertrauens-Prinzips sollten starke Authentifizierungsmethoden wie die Multi-Faktor-Authentifizierung (MFA) eingesetzt werden.
- **Verschlüsselung**
  Die Kommunikation zwischen Clients und Proxy-Servern sollte mit den aktuellsten und sichersten Versionen von SSL/TLS verschlüsselt werden, um vor Abhör- und Man-in-the-Middle-Angriffen zu schützen.
- **Threat Intelligence und URL-Filterung**
  Um die Kommunikation in IT- und OT-Umgebungen effektiv zu überwachen und zu kontrollieren, sollten Proxy-Server und Firewalls:
  - Threat Intelligence-Feeds integrieren, um bekannte schädliche Domänen, IP-Adressen und URLs zu erkennen und zu blockieren.
  - URL-Filterung anwenden, um den Zugriff auf schädliche oder nicht autorisierte Webinhalte zu verhindern.
- In OT-Umgebungen, in denen es den Systemen oft an eingebauten Sicherheitsfunktionen mangelt, sollte eine intelligente Filterung an den Netzgrenzen eingesetzt werden, um:
  - schädlichen Datenverkehr zu erkennen und zu blockieren, bevor er kritische Systeme erreicht.
  - Datenexfiltration und unbefugter externer Kommunikation zu verhindern.
  - Kommunikationsrichtlinien ohne Unterbrechung der betrieblichen Abläufe durchzusetzen.

  Diese Maßnahmen sollten Teil einer mehrschichtigen Verteidigungsstrategie sein, die einen sicheren und zuverlässigen Betrieb sowohl in IT- als auch in OT-Bereichen unterstützt.
- **Protokollierung und Überwachung**
  Detaillierte Protokollierung und kontinuierliche Überwachung sollten aktiviert werden, um den Zugriff zu verfolgen, Anomalien zu erkennen und die Reaktion auf Zwischenfälle zu unterstützen. Die Protokolle sollten regelmäßig auf Anzeichen einer Gefährdung überprüft werden.
- **Firewall-Konfiguration**
  Firewalls sollten so konfiguriert werden, dass sie nur ausdrücklich genehmigten Datenverkehr zu und von Proxy-Servern zulassen. Es sollte eine Politik der „standardmäßigen Ablehnung“ durchgesetzt werden.
- **Regelmäßige Updates und Patches**
  Proxy-Server, Firewalls und die ihnen zugrunde liegenden Systeme sollten regelmäßig aktualisiert und gepatcht werden, um bekannte Schwachstellen zu beheben und die Sicherheit zu gewährleisten.
- **Leistung und Zuverlässigkeit**
  Der Lastausgleich sollte verwendet werden, um den Datenverkehr auf mehrere Proxy-Server oder Firewalls zu verteilen und so eine hohe Verfügbarkeit und optimale Leistung zu gewährleisten. Die Ressourcennutzung sollte überwacht werden, um Überlastung und Verschlechterung zu vermeiden.

PR.IR-01.6 **Die Organisation stellt sicher, dass ihre kritischen Systeme so ausgelegt sind, dass sie bei einem Betriebsausfall einer Grenzschutzgeräte sicher ausfallen und geschützt bleiben.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass kritische Systeme geschützt bleiben und nicht angreifbar werden, wenn eine Firewall, ein Proxy oder ein anderes Grenzschutzgerät ausfällt.

In OT-Umgebungen, in denen Verfügbarkeit und Sicherheit an erster Stelle stehen, sollten Systeme so konzipiert sein, dass sie sicher ausfallen, z. B. indem sie standardmäßig in einen „alle ablehnen"-Zustand versetzt werden, betroffene Segmente isoliert werden oder Warnmeldungen ausgelöst werden, so dass der Ausfall einer Komponente nicht das gesamte System gefährdet oder unbefugten Zugriff ermöglicht.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Ausfallsichere Konfiguration**
  Geräte sollten so konfiguriert werden, dass sie im Falle eines Ausfalls in einen sicheren Zustand übergehen (z. B. Ablehnung des gesamten Datenverkehrs), um unbefugten Zugriff oder Datenlecks zu verhindern.
- **Redundanz und Hochverfügbarkeit**
  Redundante Systeme oder Failover-Mechanismen sollten vorhanden sein, um einen kontinuierlichen Schutz zu gewährleisten. Vermeiden Sie Single Points of Failure, insbesondere in OT-Umgebungen, in denen die Betriebszeit entscheidend ist.
- **Regelmäßige Tests und Wartung**
  Failover-Mechanismen und sichere Ausfallkonfigurationen sollten regelmäßig getestet werden. Die Wartung soll sicherstellen, dass die Geräte in einem sicheren und funktionsfähigen Zustand bleiben.
- **Integrität der Zugriffskontrolle**
  Zugriffskontrolllisten (ACLs) und Sicherheitsrichtlinien sollten bei Ausfällen geschützt und unverändert bleiben, um die Sicherheit des Systems zu gewährleisten.
- **Überwachung und Warnungen**
  Es sollten Echtzeitüberwachungen und -warnungen implementiert werden, um Fehler sofort zu erkennen und Abhilfemaßnahmen einzuleiten.
- **Segmentierung und Isolierung**
  Die Netzgestaltung sollte eine Segmentierung und Isolierung vorsehen, um die Auswirkungen eines Ausfalls zu begrenzen und Kaskadeneffekte zwischen den Systemen zu verhindern.

Diese Praktiken stehen im Einklang mit anerkannten Standards wie NIST SP 800-53 Rev. 5, NIST SP 800-53A und IEC 62443-3-3 SR 5.2 RE 3 – Fail Close, die den Schwerpunkt auf Ausfallsicherheit und Widerstandsfähigkeit in kritischen Infrastruktursystemen legen.

PR.IR-01.7 **Die Organisation stellt sicher, dass Entwicklungs- und Testumgebungen strikt von der Produktionsumgebung getrennt sind, insbesondere bei ICS-/OT-Systemen, bei denen jede Überschneidung die Sicherheit gefährden, die Gesundheit gefährden oder wesentliche Abläufe stören könnte.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, unbeabsichtigte Unterbrechungen, Sicherheitsrisiken oder Sicherheitsverletzungen zu verhindern, indem sichergestellt wird, dass Entwicklungs- und Testaktivitäten nicht in die laufenden Betriebssysteme eingreifen.

In OT-Umgebungen, wie z. B. bei industriellen Steuerungssystemen (ICS), können selbst geringfügige Überschneidungen zwischen Test und Produktion zu unsicheren Bedingungen, Prozessunterbrechungen oder zur Offenlegung sensibler Konfigurationen führen. Eine strikte Trennung trägt zur Wahrung der Systemintegrität bei, unterstützt die Änderungskontrolle und verringert das Risiko versehentlicher oder schädlicher Handlungen, die sich auf kritische Abläufe auswirken.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Strikte Trennung der Umgebungen**
  Entwicklungs- und Testaktivitäten sollten in Umgebungen durchgeführt werden, die physisch oder logisch von der Produktionsumgebung getrennt sind. Dies ist besonders wichtig in ICS/OT-Umgebungen, in denen die Betriebssicherheit und Zuverlässigkeit nicht beeinträchtigt werden darf.
- **Pre-Deployment Testing**
  Jede für die IKT- oder OT-Umgebung vorgesehene Änderung sollte zunächst in einer Nicht-Produktionsumgebung getestet werden. Auf diese Weise lassen sich vor der Einführung mögliche Auswirkungen und notwendige Anpassungen bewerten.
- **Realistische Testumgebungen**
  Testumgebungen sollten die Produktionsumgebung in Bezug auf Konfiguration, Architektur und Datenfluss genau nachbilden, um genaue Testergebnisse zu gewährleisten.
- **Sichere Entwicklungspraktiken**
  Cybersicherheitsfunktionen sollten so früh wie möglich in den Entwicklungszyklus integriert und getestet werden, wobei die Grundsätze des sicheren Entwicklungszyklus (SDLC) zu beachten sind.

PR.IR-01.8 **Die Organisation definiert, überwacht und kontrolliert den Informations- und Datenfluss innerhalb und zwischen ihren kritischen Systemen, um sicherzustellen, dass nur autorisierte und sichere Datenaustausche stattfinden, unabhängig von Netzwerkgrenzen oder Systemarchitektur.**

Implementierungshinweise

Diese Anforderung baut auf PR.IR-01.3 (Kontrolle von Systemverbindungen) und PR.IR-01.4 (Schutz von Systemgrenzen) auf, geht aber noch weiter, indem sie sich darauf konzentriert, welche Daten sich wo und unter welchen Bedingungen bewegen dürfen – und nicht nur darauf, wie Systeme verbunden oder segmentiert sind.

Sie ergänzt auch ID.AM-03.2, die verlangt, dass Netzwerkkommunikation und interne Datenflüsse abgebildet, dokumentiert, autorisiert und aktualisiert werden. PR.IR-01.8 stellt sicher, dass diese dokumentierten Abläufe auch aktiv durchgesetzt und überwacht werden.

Die Kontrolle des Informations- und Datenflusses ist in ICS-/OT-Umgebungen besonders wichtig, da jeder unbefugte oder unbeabsichtigte Datenaustausch die Gesundheit, die Sicherheit und den Umweltschutz gefährden kann und daher streng geregelt werden muss.

Um diese Anforderung wirksam umzusetzen, sollte die Organisation:

- **Richtlinien zur Flusskontrolle festlegen und durchsetzen**
  Es sollten Tools und Richtlinien eingesetzt werden, um zu kontrollieren, wie Daten zwischen Systemen und innerhalb verschiedener Teile des Netzwerks fließen, damit nur autorisierte Datenflüsse stattfinden.
- **Daten während der Übertragung und im Ruhezustand verschlüsseln**
  Nutzen Sie sichere Verschlüsselungsprotokolle wie TLS/SSL für Daten während der Übertragung und AES-256 für Daten im Ruhezustand, um Vertraulichkeit und Integrität zu gewährleisten.
- **Multi-Faktor-Authentifizierung (MFA) verwenden**
  MFA sollte implementiert werden, um die Identität von Benutzern zu verifizieren, die auf Systeme zugreifen, die sensible Daten verarbeiten oder übertragen.
- **APIs sichern**
  APIs, die für die systemübergreifende Kommunikation verwendet werden, sollten sicheren Entwicklungsverfahren entsprechen und regelmäßig auf Schwachstellen überprüft werden.
- **Kontinuierliche Überwachung implementieren**
  Echtzeit-Überwachungstools sollten unbefugte Datenflüsse oder Anomalien erkennen und Warnmeldungen ausgeben, um eine sofortige Reaktion zu ermöglichen.
- **Regelmäßige Audits durchführen**
  Regelmäßige Audits sollten die Einhaltung der Datenflussrichtlinien überprüfen und potenzielle Schwachstellen oder unbefugte Änderungen identifizieren.
- **Netzwerksegmentierung anwenden**
  Segmentieren Sie das Netzwerk, um unnötige Datenflüsse zu beschränken und die Auswirkungen potenzieller Sicherheitsverletzungen zu begrenzen.
- **Fernzugriff sichern**
  VPNs sollten verwendet werden, um Remote-Systeme und Benutzer sicher mit dem Netzwerk der Organisation zu verbinden.
- **Prävention von Datenverlusten (DLP) einsetzen**
  DLP-Lösungen sollten die Übertragung sensibler Informationen überwachen und kontrollieren, insbesondere wenn diese die Organisation verlassen.
- **Mitarbeiter schulen und sensibilisieren**
  Mitarbeiter sollten in Bezug auf Richtlinien zum Umgang mit Daten und die Bedeutung der Kontrolle von Informationsflüssen geschult werden.
- **Phishing-Angriffe simulieren**
  Es sollten regelmäßig Phishing-Simulationen durchgeführt werden, um das Risiko von Social-Engineering-Angriffen zu verringern.

PR.IR-01.9 **Die Organisation verwaltet Schnittstellen zu externen Telekommunikationsdiensten im Rahmen ihrer umfassenden Netzwerksicherheitsrichtlinie, indem sie festlegt, wie der Datenverkehr kontrolliert wird, die Vertraulichkeit und Integrität der übertragenen Informationen gewährleistet und alle Ausnahmen von den festgelegten Regeln überprüft und dokumentiert.**

Implementierungshinweise

Diese Kontrolle baut auf PR.IR-01.8 auf, indem sie sich speziell darauf konzentriert, wie die externe Kommunikation im Rahmen der Netzsicherheitspolitik der Organisation geregelt wird. Während Firewall-Konfigurationen und grundlegende Sicherheitseinstellungen für die technische Durchsetzung sorgen, liegt der Schwerpunkt dieser Anforderung auf der Ebene der Richtlinien und der Überwachung.

Um dies wirksam umzusetzen, sollte die Organisation:

- **Das Verkehrsflußmanagement in die Netzsicherheitsrichtlinie integrieren**
  Die Netzsicherheitsrichtlinie sollte klare Regeln dafür enthalten, wie der Daten- und Sprachverkehr zwischen internen Systemen und externen Telekommunikationsdiensten fließen darf.
- **Sicherheitsziele und den Geltungsbereich definieren**
  Die Richtlinie sollte die Ziele für den Schutz der externen Kommunikation umreißen und angeben, welche Systeme und Dienste abgedeckt werden.
- **Den Datenverkehr kontrollieren und überwachen**
  Der Netzwerkverkehr sollte kontinuierlich überwacht werden, um sicherzustellen, dass er den festgelegten Regeln entspricht. Verdächtige oder unzulässige Flüsse sollten Warnmeldungen auslösen und untersucht werden.
- **Daten während der Übertragung schützen**
  Die Vertraulichkeit und Integrität der übertragenen Daten sollte durch Verschlüsselungsprotokolle wie TLS/SSL gewährleistet werden.
- **Ausnahmen dokumentieren und überprüfen**
  Ausnahmen von den Verkehrsflussregeln (z. B. vorübergehender Zugang für Dritte) sollten formell dokumentiert, begründet und regelmäßig überprüft werden.
- **Auf Vorfälle reagieren**
  Die Organisation sollte darauf vorbereitet sein, ungewöhnliche oder schädliche Verkehrsmuster schnell zu isolieren und darauf zu reagieren.
- **Die Richtlinienabstimmung beibehalten**
  Die Komponente für den Datenverkehr sollte auf andere Elemente der Netzwerksicherheitsrichtlinie abgestimmt sein, darunter Zugriffskontrolle, VPN-Nutzung, Patch-Management und Reaktion auf Vorfälle.

PR.IR-02 Die technischen Vermögenswerte der Organisation sind vor Umweltbedrohungen geschützt

PR.IR-02.1 Die Organisation definiert, implementiert und pflegt Richtlinien und Verfahren in Bezug auf Notfall- und Sicherheitssysteme, Brandschutzsysteme und Umweltkontrollen für ihre kritischen Systeme.

Implementierungshinweise

Ziel dieser Kontrolle ist es, kritische Systeme vor Umweltgefahren und Notfällen zu schützen, die den Betrieb stören, die Ausrüstung beschädigen oder die Sicherheit gefährden könnten – insbesondere in OT-Umgebungen, in denen sich die physikalischen Bedingungen direkt auf die Systemverfügbarkeit und die menschliche Sicherheit auswirken.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Risikobewertungen** für alle Standorte durchführen, an denen sich kritische Systeme befinden, um Umwelt- und Notfallrisiken zu ermitteln.
- **Richtlinien und Verfahren** für Brandschutz, Notfallmaßnahmen und Umweltkontrollen festlegen.
- **Überwachungssysteme** wie Temperatur-, Feuchtigkeits-, Rauch- und Wasserlecksensoren installieren, die bei abnormalen Bedingungen Alarm schlagen.
- **Brandschutzmaßnahmen implementieren**, einschließlich geeigneter Unterdrückungssysteme (z. B. auf Gasbasis für Rechenzentren), Alarme, Detektoren und Feuerlöscher.
- **Regelmäßige Inspektionen und Wartungen** von Brandschutz- und Umweltsystemen, einschließlich HLK und Notbeleuchtung durchführen.
- **Umweltschutzauflagen in Verträge mit Drittparteien aufnehmen** und Nachweise über deren Einhaltung und Aufrechterhaltung fordern.
- **Mitarbeiter** mindestens einmal jährlich in Bezug auf Notfallverfahren und die Durchführung von Evakuierungs- und Brandschutzübungen schulen.

PR.IR-02.2 Die Organisation richtet Feuermeldevorrichtungen ein, die im Falle eines Brandes automatisch aktiviert werden und wichtige Mitarbeiter benachrichtigen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Brandereignisse frühzeitig erkannt und wichtige Mitarbeiter automatisch alarmiert werden, um eine schnelle und koordinierte Reaktion zu ermöglichen – insbesondere in Umgebungen, in denen kritische Systeme die Sicherheit oder wichtige Abläufe unterstützen.

Um dieses Ziel zu erreichen, sollte die Organisation:

- Automatische Brandmeldeanlagen mit Rauch- und Wärmemeldern einsetzen, die ohne manuelles Eingreifen aktiviert werden.
- Brandmeldeanlagen gegebenenfalls mit automatischen Löschanlagen (z. B. Sprinkleranlagen oder gasbasierte Anlagen) integrieren.
- Systeme so konfigurieren, dass bei Aktivierung automatisch die zuständigen Mitarbeiter oder die Notfallhelfer benachrichtigt werden.
- Eine Benachrichtigungsliste mit klar zugewiesenen Rollen definieren und pflegen und sicherstellen, dass die einzelnen Personen über die erforderlichen Zugriffsrechte und Berechtigungen verfügen – insbesondere in sensiblen oder klassifizierten Umgebungen.

PR.IR-03 Es sind Mechanismen implementiert, um die Anforderungen an die Widerstandsfähigkeit in normalen und ungünstigen Situationen zu erfüllen

PR.IR-03.1 **Die Organisation implementiert Mechanismen, die sicherstellen, dass kritische Systeme und Dienste sowohl im Normalbetrieb als auch unter ungünstigen Bedingungen betriebsbereit bleiben oder schnell wiederhergestellt werden können.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass kritische Systeme und Dienste sowohl im Normalbetrieb als auch unter widrigen Umständen wie Cyberangriffen, Hardwareausfällen oder Naturkatastrophen betriebsbereit bleiben oder schnell wiederhergestellt werden können.

Diese Kontrolle unterstützt das übergeordnete Ziel der operativen Resilienz. Während Redundanz (wie in GV.OC-04.3 beschrieben) durch die Duplizierung von Komponenten dazu beiträgt, Ausfälle zu verhindern, gewährleistet die Resilienz, dass der Betrieb auch bei Ausfällen weiterlaufen oder schnell wiederhergestellt werden kann. Beides ist für die Aufrechterhaltung der Verfügbarkeit in komplexen IT- und OT-Umgebungen unerlässlich.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Resilienzziele definieren**
  - Identifizieren Sie kritische Systeme und definieren Sie akzeptable Wiederherstellungszeiten (RTO) und Wiederherstellungspunkte (RPO).
  - Bringen Sie Resilienzziele mit Business-Continuity- und Disaster-Recovery-Plänen in Einklang.
- **Auf Resilienz ausgelegt sein**
  - Implementieren Sie fehlertolerante Architekturen (z. B. Clustering, Lastausgleich, geografische Redundanz).
  - Nutzen Sie verschiedene Technologien und Anbieter, um die Abhängigkeit von einzelnen Fehlerquellen zu verringern.
- **Stellen Sie Betriebsbereitschaft sicher**
  - Testen Sie Failover-Systeme regelmäßig durch Simulationen und Umschaltungen.
  - Halten Sie Betriebsverfahren und Wiederherstellungsanweisungen auf dem neuesten Stand und korrekt.
- **Cyber-Resilienz verbessern**
  - Integrieren Sie Resilienzstrategien in Ihre Notfallpläne (z. B. Eindämmung von Ransomware, Datenwiederherstellung).
  - Nutzen Sie unveränderliche Backups und Netzwerksegmentierung, um die Auswirkungen von Cybervorfällen zu begrenzen.
- **Die Resilienz von Drittparteien bewerten**
  - Bewerten Sie die Resilienz kritischer Dienstleistungsanbieter und dokumentieren Sie die Ergebnisse.
  - Nehmen Sie Anforderungen an Resilienz und Wiederherstellung in Service Level Agreements (SLAs) auf.
- **Kontinuierliche Verbesserung fördern**
  - Überprüfen und aktualisieren Sie Resilienzmechanismen nach Vorfällen oder größeren Veränderungen.
  - Beziehen Sie die gewonnenen Erkenntnisse in die zukünftige Planung und Prüfung ein.

PR.IR-04 Eine angemessene Ressourcenkapazität zur Gewährleistung der Verfügbarkeit wird aufrechterhalten

PR.IR-04.1 Eine angemessene Planung der Ressourcenkapazitäten stellt sicher, dass die Verfügbarkeit der kritischen Systeminformationen der Organisation in den Bereichen Informationsverarbeitung, Netzwerke, Telekommunikation und Datenspeicherung aufrechterhalten bleibt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass für kritische Systeme jederzeit genügend Rechen-, Speicher- und Netzwerkressourcen zur Verfügung stehen, indem der aktuelle und künftige Kapazitätsbedarf vorausgeplant wird.

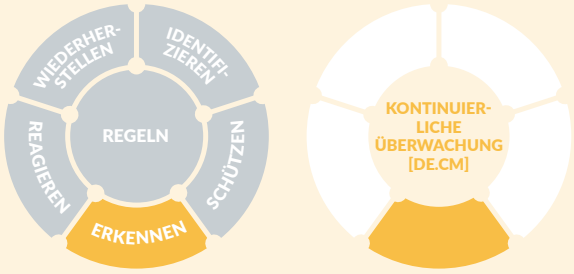
Um dieses Ziel zu erreichen, sollte die Organisation:

- **Prognosen erstellen und planen**
  Der Ressourcenbedarf sollte regelmäßig auf der Grundlage des Geschäftswachstums, saisonaler Muster und Nutzungstrends prognostiziert werden. Der künftige Bedarf an Rechen-, Speicher- und Netzwerkkapazität sollte vorhergesehen werden, um Leistungsprobleme oder Ausfälle zu vermeiden.
- **Beschaffungsvorlaufzeiten berücksichtigen**
  Bei der Kapazitätsplanung sollten mögliche Verzögerungen bei der Lieferung von Hardware oder Services aufgrund von Störungen in der Lieferkette oder geopolitischen Ereignissen berücksichtigt werden. Die Pufferkapazität sollte beibehalten werden, um unerwartete Nachfrage oder Verzögerungen bei der Erweiterung aufzufangen.
- **Schwellenwerte überwachen und festlegen**
  Systeme sollten kontinuierlich überwacht werden, um die Nutzung zu verfolgen. Schwellenwerte und Warnmeldungen sollten so konfiguriert werden, dass sie rechtzeitig Skalierungsmaßnahmen auslösen, bevor die Leistung beeinträchtigt wird.
- **Hochverfügbare Komponenten einsetzen**
  Redundante Komponenten (z. B. RAID-Arrays, doppelte Netzwerkschnittstellen, Notstromversorgung) sollten eingesetzt werden, um Ausfallzeiten aufgrund von Hardwarefehlern zu reduzieren. Diese sollten die Kapazitätsplanung ergänzen, nicht ersetzen.
- **Regelmäßig überprüfen und anpassen**
  Kapazitätspläne sollten regelmäßig überprüft und auf der Grundlage von Änderungen der Geschäftsstrategie, der Technologie oder externer Risikofaktoren aktualisiert werden.


WARNING!
SYSTEM WARNING

ERKENNEN

Erkennen



Vermögenswerte werden überwacht, um Anomalien, Indikatoren für Kompromittierung und andere potenziell unerwünschte Ereignisse zu finden

DE.CM-01 Netzwerke und Netzwerkdienste werden überwacht, um potenziell unerwünschte Ereignisse zu erkennen

DE.CM-01.1 Firewalls werden an den Netzgrenzen installiert und betrieben, einschließlich Endpunkt-Firewalls.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Sichtbarkeit und Erkennung von Bedrohungen auf Geräteebene zu verbessern, insbesondere von Bedrohungen, die herkömmliche Schutzmechanismen am Netzwerkrand umgehen können.

Diese Kontrolle konzentriert sich auf den Einsatz von hostbasierten Firewalls zur Erkennung von Bedrohungen, die den Netzwerkperimeter umgehen könnten, indem der Datenverkehr zu und von einzelnen Geräten überwacht und kontrolliert wird (Schwerpunkt: Sichtbarkeit und Erkennung). Im Gegensatz dazu befasst sich die Kontrolle PR.IR-01.1 mit netzwerkbasierten Firewalls, die den unbefugten Zugriff verhindern sollen, indem sie den in das Netzwerk eintretenden oder es verlassenden Datenverkehr kontrollieren (Schwerpunkt: Kontrolle und Prävention).

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Umfassende Definition von Endpunkten**: Schließen Sie Desktops, Laptops, Server, Smartphones und, soweit möglich, OT-Komponenten (Operational Technology) wie SPSen und HMIs sowie IoT-Geräte ein.
- **Installation von Host-basierten Firewalls**: Stellen Sie sicher, dass Firewalls auf allen Endgeräten installiert, aktiv und richtig konfiguriert sind. Diese Firewalls helfen, verdächtige Aktivitäten direkt auf dem Gerät zu erkennen und zu blockieren, auch wenn es mit sicheren Netzwerken oder VPNs verbunden ist.
- **Segmentierung von Netzwerkressourcen**: Gruppieren Sie Systeme auf der Grundlage ihrer Kritikalität oder Funktion (stellen Sie z. B. öffentlich zugängliche Dienste wie E-Mail-, Web- und VPN-Server in eine DMZ).
- **Verwendung von vordefinierten Firewall-Regeln**: Legen Sie Regeln fest, um den ein- und ausgehenden Datenverkehr zu filtern, und helfen Sie so, Anomalien oder bösartiges Verhalten zu erkennen.
- **Begrenzung der Internet-Gateways**: Reduzieren Sie die Anzahl der Verbindungspunkte zum Internet, um die Belastung zu minimieren und die Überwachung zu vereinfachen.

DE.CM-01.2 Antiviren-, Anti-Spyware- und andere Anti-Malware-Programme werden installiert und aktualisiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Geräte der Organisation (IT- und OT-Ressourcen) vor schädlicher Software geschützt sind, indem Anti-Malware-Tools eingesetzt und regelmäßig aktualisiert werden.

Um dieses Ziel zu erreichen, beachten Sie Folgendes:

- **Umfang des Schutzes**
  - IT-Geräte: Installieren Sie Anti-Malware-Software auf allen Benutzer- und Systemgeräten, einschließlich Desktops, Laptops, Servern, Smartphones und Tablets.
  - OT-Geräte: Erweitern Sie den Schutz auf OT-Geräte wie SPS, HMIs, SCADA-Server und technische Workstations, sofern dies technisch machbar ist.
- **Aktualisierungs- und Scanning-Verfahren**
  - IT: Konfigurieren Sie Anti-Malware-Tools so, dass sie in Echtzeit oder zumindest täglich aktualisiert werden, gefolgt von automatischen oder geplanten Scans.
  - OT: Planen Sie Updates und Scans sorgfältig, um Betriebsunterbrechungen zu vermeiden. Nutzen Sie Wartungsfenster und testen Sie Updates vor der Bereitstellung.
- **Maßgeschneiderte Lösungen für OT**
  - Verwenden Sie schlanke oder OT-spezifische Anti-Malware-Tools, die mit Echtzeitsystemen kompatibel sind.
  - Für ältere oder ressourcenbeschränkte OT-Geräte sollten Sie Folgendes in Betracht ziehen:
    - Whitelisting von Anwendungen
    - Netzwerkbasierte Malware-Erkennung
    - Nutzen Sie spezialisierte Tools zur stillen Überwachung von Industriesystemen, um ungewöhnliche oder verdächtige Aktivitäten zu erkennen, ohne in den Betrieb der Systeme einzugreifen (passive Überwachung).
- **Telearbeit und BYOD**
  Wenden Sie die gleichen Schutzstandards an für:
  - Für Telearbeit genutzte Heimcomputer
  - Persönliche Geräte (BYOD), die für berufliche Aufgaben genutzt werden
  - Verwenden Sie Endpunktschutzplattformen, um Richtlinien auf allen Geräten durchzusetzen.
- **Zentralisiertes Management und zentralisierte Überwachung**
  - Verwenden Sie zentralisierte Tools zur Verwaltung von Anti-Malware-Konfigurationen, Updates und Warnungen in IT- und OT-Umgebungen.
  - Integrieren Sie Malware-Warnungen in die umfassenderen Sicherheitsüberwachungs- und Incident-Response-Prozesse der Organisation.
- **Kontinuierliche Verbesserung**
  - Überprüfen und testen Sie regelmäßig die Wirksamkeit der Anti-Malware.
  - Aktualisieren Sie Richtlinien und Tools auf der Grundlage neuer Bedrohungen und der aus Vorfällen gewonnenen Erkenntnisse.

DE.CM-01.3 Die Organisation überwacht und identifiziert die unbefugte Nutzung ihrer geschäftskritischen Systeme durch die Erkennung unbefugter lokaler Verbindungen, Netzwerkverbindungen und Fernverbindungen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation einen unbefugten Zugriff auf ihre geschäftskritischen Systeme oder deren Missbrauch erkennen und darauf reagieren kann. Dazu gehört die Identifizierung verdächtiger lokaler, Netzwerk- oder Remote-Verbindungen, die auf eine Sicherheitsverletzung oder den Missbrauch sensibler Systeme hindeuten könnten.

Um dieses Ziel zu erreichen, beachten Sie Folgendes:

- Die Überwachung der Netzkommunikation sollte an der Außengrenze der geschäftskritischen Systeme der Organisation und an den wichtigsten internen Grenzen innerhalb dieser Systeme erfolgen.
- Einrichtungen sollten auf nicht autorisierte oder betrügerische drahtlose Netzwerke überwacht werden, die es Angreifern ermöglichen könnten, normale Kontrollen zu umgehen.
- Kritische Netzwerkdienste wie das Domain Name System (DNS – übersetzt die Namen von Websites in IP-Adressen), das Border Gateway Protocol (BGP – hilft bei der Weiterleitung des Internetverkehrs) und andere Netzwerkdienste sollten auf Anzeichen von Manipulationen oder Missbrauch überwacht werden.
- Beim Hosting von Anwendungen, die über das Internet zugänglich sind, sollte eine Web Application Firewall (WAF) zum Schutz vor Angriffen in Betracht gezogen werden. Wenn die Anwendung nicht webbasiert ist, sollte sie mit anderen geeigneten Methoden geschützt werden, z. B. mit einem Identitätsanbieter (IdP) zur Zugriffskontrolle.

DE.CM-01.4 Die Organisation überwacht ihr Netzwerk kontinuierlich, um Anzeichen für Cyber-Bedrohungen oder ungewöhnliche Aktivitäten zu erkennen, wobei klar definierte Regeln für potenzielle Sicherheitsvorfälle gelten.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation ihr Netzwerk und ihre Systeme kontinuierlich überwacht, um Anzeichen für Cyber-Bedrohungen oder ungewöhnliche Aktivitäten zu erkennen. Dies geschieht anhand klar definierter Regeln, mit deren Hilfe festgestellt werden kann, was als potenzieller Sicherheitsvorfall zu werten ist.

Um dies zu erreichen, beachten Sie Folgendes:

- Diese Kontrolle baut auf DE.AE-08.1 auf. Dieser Punkt fordert, dass Vorfälle auf der Grundlage vordefinierter Kriterien gemeldet werden müssen.
- Die Organisation sollte entscheiden, welche Arten von Cybersicherheitsereignissen und Warnzeichen überwacht werden müssen, und festlegen, welche Informationen in Audit-Protokollen aufgezeichnet werden müssen.
- Automatisierte Tools sollten eingesetzt werden, um verdächtige Aktivitäten wie unerwarteten Netzwerkverkehr, fehlgeschlagene Anmeldeversuche oder falsche Systemeinstellungen zu erkennen.
- Die Überwachung sollte flexibel sein und in risikoreichen Zeiten verstärkt werden, z. B. wenn Bedrohungswarnungen eingehen, bei geopolitischen Spannungen oder nach internen Problemen.
- Die Überwachung sollte nicht nur digitale Systeme, sondern auch physische Räume, das Verhalten der Mitarbeiter und gegebenenfalls die Interaktion mit Dienstleistern umfassen.
- Die Netzaktivität sollte kontinuierlich analysiert werden, um Veränderungen zu erkennen, die auf eine Schwächung der Sicherheit hindeuten könnten, und zwar nach dem Prinzip „Zero-Trust“.
- Alarme sollten automatisch ausgelöst werden, wenn bestimmte Schwellenwerte erreicht sind, und bekannte Fehlalarme sollten herausgefiltert werden, um die Mitarbeiter nicht zu überfordern.

DE.CM-02 Die physische Umgebung wird überwacht, um potenziell unerwünschte Ereignisse zu finden

DE.CM-02.1 Die physische Umgebung wird überwacht, um potenziell unerwünschte Ereignisse zu finden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die physischen Räume, in denen sich kritische Systeme und Daten befinden, auf Anzeichen verdächtiger oder schädlicher Aktivitäten überwacht werden. Dies hilft dabei, potenzielle Bedrohungen wie unbefugten Zugriff, Manipulationen oder andere ungewöhnliche Ereignisse in der physischen Umgebung zu erkennen.

Um dieses Ziel zu erreichen, beachten Sie Folgendes:

- Protokolle von physischen Zugangssystemen (z. B. Badge-Lesegeräte) sollten auf ungewöhnliche Muster überprüft werden, z. B. wenn jemand versucht, zu ungewöhnlichen Zeiten einzutreten, oder wenn wiederholte Versuche fehlschlagen, einen gesperrten Bereich zu betreten.
- Die Aufzeichnungen über den Zugang von Besuchern (z. B. Unterschriftenlisten oder digitale Check-Ins) sollten regelmäßig überprüft werden, um sicherzustellen, dass nur befugte Personen die Sicherheitsbereiche betreten haben.
- Physische Sicherheitseinrichtungen (wie Schlösser, Türverriegelungen, Scharnierstifte und Alarmanlagen) sollten auf Anzeichen von Manipulationen oder Beschädigungen überprüft werden, die auf einen Einbruchsversuch hindeuten könnten.

DE.CM-02.2 Der physische Zugang zu den kritischen Systemen und Geräten der Organisation wird zusätzlich zur Überwachung des physischen Zugangs zur Einrichtung durch physische Einbruchsalarme, Überwachungsgeräte und unabhängige Überwachungsteams ergänzt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, den Schutz kritischer Systeme und Geräte zu verstärken, indem die grundlegende physische Zugangskontrolle durch aktive Einbruchserkennung, Überwachungstechnologien und unabhängige Überwachungsmöglichkeiten ergänzt wird. Dies trägt dazu bei, dass Bedrohungen der physischen Sicherheit rechtzeitig erkannt werden und darauf reagiert werden kann.

Um dieses Ziel zu erreichen, beachten Sie Folgendes:

- Es sollten Systeme zur Erkennung von Eindringlingen eingesetzt werden, um unbefugte physische Eindringversuche zu erkennen. Diese Systeme können Bewegungssensoren, Tür-/Fensterkontaktsensoren und Glasbruchmelder umfassen, die Alarm auslösen, wenn ungewöhnliche Aktivitäten festgestellt werden.
- Überwachungstechnologien wie CCTV-Kameras, Videoaufzeichnungssysteme und Zugangskontrollsysteme sollten eingesetzt werden, um Aktivitäten in sensiblen Bereichen kontinuierlich zu überwachen und aufzuzeichnen. Diese Systeme helfen bei der Verifizierung von Vorfällen und unterstützen die Ermittlungen.
- Die Nachverfolgung von Besuchern sollte verbessert werden, indem alle Besucher, einschließlich Auftragnehmer und Zeitarbeitskräfte, mit Hilfe digitaler Systeme oder manueller Protokolle erfasst werden.
- Unabhängige Überwachungsteams, in der Regel externe Sicherheitsexperten, sollten beauftragt werden, die Überwachungssysteme zu kontrollieren und auf Vorfälle zu reagieren. Diese Teams verfügen über spezielles Fachwissen und arbeiten getrennt von den internen Mitarbeitern, weshalb es wichtig ist, die Anforderungen an die Cybersicherheit von Dritten auf ihre Tätigkeiten anzuwenden.
- Die Überwachung und Erkennung von Eindringlingen sollte in umfassendere Sicherheitsmaßnahmen integriert werden, damit Warnmeldungen mit anderen physischen und digitalen Anzeichen für eine Kompromittierung in Zusammenhang gebracht werden können.

DE.CM-03 Die Aktivitäten der Mitarbeiter und die Nutzung der Technologie werden überwacht, um potenziell schädliche Ereignisse zu erkennen.

DE.CM-03-1 Es werden Endpunkt- und Netzschutzinstrumente zur Überwachung des Endnutzerverhaltens auf gefährliche Aktivitäten implementiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation riskantes oder verdächtiges Verhalten von Benutzern auf Geräten und in Netzwerken erkennen und darauf reagieren kann. Dies hilft bei der Erkennung von Bedrohungen wie Malware-Infektionen, Systemmissbrauch oder Versuchen, Sicherheitskontrollen zu umgehen – unabhängig davon, ob diese von externen Angreifern oder Insidern verursacht werden.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Organisationen sollten den Einsatz einer Kombination moderner Sicherheitstools in Betracht ziehen, die zusammenarbeiten, um ein vollständiges Bild der Benutzer- und Systemaktivitäten zu erhalten:
  - Intrusion Detection and Prevention Systems (IDPS): Diese Tools überwachen den Netzwerkverkehr und können verdächtige Aktivitäten wie Hacking-Versuche oder die Ausnutzung von Schwachstellen blockieren oder melden.
  - Web Application Firewalls (WAFs) und API-Gateways: Sie tragen zum Schutz von Online-Anwendungen und -Services bei, indem sie schädlichen Datenverkehr filtern und unbefugten Zugriff verhindern.
- Darüber hinaus kann ein mehrstufiger Ansatz mit fortschrittlichen Erkennungs- und Reaktionstools für Echtzeit-Transparenz und schnellere Reaktionen sorgen:
  - Endpoint Detection and Response (EDR): Überwacht die Aktivitäten auf einzelnen Geräten (wie Laptops oder Servern), um Bedrohungen wie Malware oder unbefugten Zugriff zu erkennen.
  - Network Detection and Response (NDR): Analysiert den Netzwerkverkehr, um ungewöhnliche Muster zu erkennen, z. B. seitliche Bewegungen oder versteckte Angriffe.
  - Identity Threat Detection and Response (ITDR): Konzentriert sich auf die Erkennung des Missbrauchs von Benutzerkonten, wie z. B. gestohlene Anmeldedaten oder Insider-Bedrohungen.
  - User and Entity Behaviour Analytics (UEBA): Verwendet maschinelles Lernen, um normales Verhalten zu verstehen und Anomalien zu erkennen, die auf eine Bedrohung hindeuten könnten.
- Diese Tools sind Teil einer modernen, mehrschichtigen Sicherheitsstrategie und werden häufig in branchenüblichen Best Practices und Frameworks wie der von Gartner eingeführten Security Operations Centre (SOC) Visibility Triad erwähnt.

DE.CM-03-2 Es werden Endpunkt- und Netzschutzinstrumente zur Überwachung des Endnutzerverhaltens auf gefährliche Aktivitäten verwaltet.

Implementierungshinweise

Diese Kontrolle baut auf DE.CM-03.1 auf und verlagert den Schwerpunkt von der Implementierung auf die laufende Verwaltung der Überwachungsinstrumente. Ziel dieser Kontrolle ist es, sicherzustellen, dass die Tools, die zur Überwachung des Benutzerverhaltens und zur Erkennung schädlicher Aktivitäten auf Geräten und in Netzwerken eingesetzt werden, ordnungsgemäß gewartet und aktiv verwaltet werden. Dies unterstützt die kontinuierliche Wirksamkeit der Tools, wenn sich die Bedrohungen weiterentwickeln, und stellt sicher, dass die von ihnen erzeugten Warnungen genau, relevant und hilfreich sind, um echte Sicherheitsrisiken zu erkennen.

Um dieses Ziel zu erreichen, beachten Sie Folgendes:

- Tools zur Überwachung von Geräten wie Laptops, Mobiltelefonen und Servern sollten regelmäßig überprüft werden, um sicherzustellen, dass sie ordnungsgemäß funktionieren, mit den neuesten Bedrohungsinformationen aktualisiert werden und in der Lage sind, neue Arten von Angriffen zu erkennen.

- Es sollte ein zentrales System verwendet werden, um Protokolle aus verschiedenen Quellen zu sammeln und zu analysieren. Diese Protokolle sollten vollständig und auf dem neuesten Stand sein und verdächtige Aktivitäten erkennen lassen.
- Die Protokolle über den Systemzugang, z. B. Anmeldeversuche oder Zugang außerhalb der normalen Geschäftszeiten, sollten regelmäßig überprüft werden. Es sollten Warnmeldungen eingerichtet werden, um Sicherheitsteams über ungewöhnliche Muster zu informieren.
- Die Tools zur Analyse des Nutzerverhaltens sollten im Laufe der Zeit fein abgestimmt werden. Sicherheitsteams sollten Warnungen überprüfen, Erkennungsregeln anpassen, um Fehlalarme zu reduzieren und die Genauigkeit zu verbessern.
- Täuschungstools, wie z. B. gefälschte Systeme oder Dateien, die Angreifer anlocken sollen, sollten genau überwacht werden. Warnungen dieser Tools sind oft frühe Anzeichen für einen echten Angriff und sollten mit hoher Priorität behandelt werden.
- Sicherheitsteams sollten regelmäßig prüfen, wie gut alle Überwachungstools funktionieren, Erkennungsregeln aktualisieren und sicherstellen, dass die Tools in die Prozesse zur Reaktion auf Vorfälle integriert sind.
- Die Rollen und Zuständigkeiten für die Überwachung und Reaktion auf Warnmeldungen sollten klar definiert werden. Die Mitarbeiter sollten darin geschult werden, die Instrumente wirksam einzusetzen und angemessen auf Vorfälle zu reagieren.

DE.CM-06 Aktivitäten und Dienstleistungen externer Dienstleister werden überwacht, um potenziell unerwünschte Ereignisse zu erkennen

DE.CM-06.1 Aktivitäten und Services externer Dienstleister werden gesichert und überwacht, um potenziell unerwünschte Ereignisse zu erkennen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die von externen Dienstleistern durchgeführten Aktivitäten, ob vor Ort oder per Fernzugriff, sicher verwaltet und kontinuierlich überwacht werden. Dies hilft dabei, ungewöhnliche oder schädliche Handlungen zu erkennen, die sich auf die Systeme, Daten oder Services der Organisation auswirken könnten.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Zu den externen Anbietern können Subunternehmer, Anbieter von Cloud-Services, IT-Support-Teams, Softwareentwickler und andere Drittparteien gehören, die an der Wartung, Entwicklung oder Sicherheit des Systems beteiligt sind.
- Die Überwachung sollte sich auf Folgendes konzentrieren:
  - Zugangs- und Anmeldeaktivitäten, einschließlich der Art und Weise, wie und wann sich externe Benutzer mit den Systemen verbinden.
  - Datenübertragungen und Netzwerkverkehr, um ungewöhnliche oder unbefugte Informationsbewegungen zu erkennen.
  - Systemänderungen, wie z. B. Software-Updates oder Konfigurationsanpassungen, die von externen Parteien vorgenommen werden.
- Alle Fern- und Vor-Ort-Aktivitäten von externen Anbietern sollten protokolliert und überprüft werden, um unbefugte Handlungen oder risikoreiches Verhalten zu erkennen.
- Cloud-Services und Internet-Provider sollten auf unerwartetes Verhalten oder Leistungsprobleme überwacht werden, die auf ein Sicherheitsproblem hindeuten könnten.
- Es sollte ein zentrales Protokollierungssystem verwendet werden, um Daten von allen externen Services zu erfassen und zu analysieren.
- Alle Sicherheitsvorfälle, an denen externe Anbieter beteiligt sind – wie z. B. Malware-Infektionen, Phishing-Versuche oder unbefugter Zugriff – sollten frühzeitig erkannt, schnell gemeldet und wirksam behandelt werden.

DE.CM-06.2 **Die Einhaltung der Sicherheitsrichtlinien und -verfahren für die Mitarbeiter sowie der vertraglichen Sicherheitsanforderungen durch externe Dienstleister wird im Hinblick auf ihre Cybersicherheitsrisiken überwacht.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass externe Dienstleister die Personalsicherheitsrichtlinien und Vertragsbedingungen der Organisation einhalten, insbesondere wenn sie Zugang zu sensiblen Systemen oder Daten haben. Dies trägt dazu bei, das Risiko von Sicherheitsvorfällen zu verringern, die durch Mitarbeiter von Drittanbietern verursacht werden, und gewährleistet, dass für die Anbieter die gleichen Standards gelten wie für die internen Mitarbeiter.

Um dieses Ziel zu erreichen, beachten Sie Folgendes:

- Externe Anbieter sollten klar definierte Sicherheitsverantwortlichkeiten haben, die in Verträgen oder Service Level Agreements dokumentiert sind.
- Die Verträge sollten Anforderungen wie diese enthalten:
  - Hintergrundüberprüfungen für Mitarbeiter des Anbieters
  - Unterzeichnung von Vertraulichkeitsvereinbarungen
  - Einhaltung der Richtlinien zur akzeptablen Nutzung
- Die Einhaltung dieser Anforderungen sollte regelmäßig kontrolliert werden, einschließlich der Überprüfung der absolvierten Sicherheitsschulungen und der unterzeichneten Vereinbarungen.
- Die Anbieter sollten verpflichtet werden, die Organisation unverzüglich zu benachrichtigen, wenn Mitarbeiter mit Systemzugang versetzt werden oder ihre Funktion aufgeben, damit die Zugangsrechte unverzüglich entzogen werden können.
- In regelmäßigen Abständen sollten Audits durchgeführt werden, um zu bestätigen, dass die Anbieter die Sicherheitsrichtlinien einhalten. Dazu kann gehören:
  - Überprüfung von Zugriffsprotokollen und Berechtigungen
  - Überprüfung der Onboarding- und Offboarding-Verfahren
  - Sicherstellung, dass nur befugte Personen Zugang zu kritischen Systemen haben
- Alle Probleme oder Verstöße sollten dokumentiert, gemeldet und durch Korrekturmaßnahmen und Nachprüfungen behoben werden.

DE.CM-09 Computerhardware und -software, Laufzeitumgebungen und deren Daten werden überwacht, um potenziell schädliche Ereignisse zu erkennen

DE.CM-09.1 **Die Organisation überwacht Computerhardware, Software, Laufzeitumgebungen und deren Daten, um potenziell nachteilige Ereignisse zu erkennen.**

Implementierungshinweise

Diese Kontrolle soll sicherstellen, dass Organisationen ihre Computersysteme und Daten kontinuierlich überwachen, um potenziell schädliche Ereignisse frühzeitig zu erkennen. Dies trägt dazu bei, den Überblick zu behalten, zeitnahe Reaktionen zu unterstützen und das Risiko von Sicherheitsvorfällen zu verringern.

Um das Ziel dieser Kontrolle zu erreichen, sollte die Organisation Folgendes berücksichtigen:
- Aktivieren Sie die Systemprotokollierung auf Computern und Servern, um wichtige Ereignisse aufzuzeichnen.
- Verwenden Sie den integrierten Viren- oder Endpunktschutz, um Bedrohungen zu erkennen und Warnmeldungen zu generieren.
- Überprüfen Sie regelmäßig Protokolle und Warnmeldungen, um ungewöhnliche Aktivitäten oder Fehler zu erkennen.
- Speichern Sie Protokolle in einem gemeinsamen Ordner oder einem einfachen Protokoll-Viewer, um den Zugriff und die Überprüfung zu erleichtern.
- Legen Sie eine Routine (z. B. wöchentlich oder monatlich) für die Überprüfung der Protokolle und die Aktualisierung der Überwachungstools fest.
- Beauftragen Sie eine Person mit der Überwachung, auch wenn es sich um eine Teilzeitstelle handelt.

DE.CM-09.2 Die Organisation führt Hardware-Integritätsprüfungen durch, um unbefugte Manipulationen an kritischer Systemhardware zu erkennen. Die Kontrollen entsprechen dem Risikoprofil und der operativen Kapazität der Organisation.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass kritische Hardwarekomponenten vor unbefugten Eingriffen geschützt sind. Durch die Implementierung von Integritätsprüfungen, die dem Risikoniveau und der Betriebskapazität der Organisation entsprechen, ist es möglich, physische oder Firmware-bedingte Änderungen zu erkennen, die die Sicherheit beeinträchtigen könnten.

Um dieses Ziel zu erreichen, sollten Sie die folgenden Elemente berücksichtigen:
- **Definieren Sie, was geschützt werden muss**
  Identifizieren Sie, welche Systeme am kritischsten sind, z. B. Server mit sensiblen Daten, industrielle Kontrollsysteme (ICS/SCADA) oder kryptografische Geräte, und setzen Sie Prioritäten auf der Grundlage der Auswirkungen auf das Geschäft, der rechtlichen Anforderungen und der Gefährdung durch Bedrohungen.
- **Wählen Sie das richtige Schutzniveau**
  Wählen Sie die Kontrollen danach aus, wie kritisch das System ist und was die Organisation unterstützen kann:
  - **Grundlegende Kontrollen**: Verschlossene Serverräume, manipulationssichere Siegel, sicheres Booten und regelmäßige Hardware-Audits.
  - **Intermediäre Kontrollen**: Warnmeldungen beim Öffnen der Hardware, Verwendung von Trusted Platform Modules (TPMs) und Tools zur Firmware-Validierung.
  - **Erweiterte Kontrollen**: Fernvalidierung des Hardwarestatus, manipulationssichere kryptografische Hardware (HSMs) und Überwachung auf Anomalien auf Hardwareebene mithilfe von Sicherheitstools.
- **Verbindung zu Sicherheitsoperationen**
  Leiten Sie Warnmeldungen von Hardware-Integritätstools an zentrale Überwachungssysteme (wie SIEM oder SOC) weiter, um Echtzeit-Transparenz zu gewährleisten. Legen Sie fest, wie bei Verdacht auf Manipulation zu reagieren ist.
- **Weisen Sie klare Verantwortlichkeiten zu**
  Legen Sie Rollen für die Entwicklung, Implementierung und Reaktion auf Hardware-Integritätsprobleme fest. Verwenden Sie Rollenprofile (z. B. von ENISA ECSF), um die Zuständigkeiten festzulegen:
  - Sicherheitsarchitekten entwerfen die Kontrollen.
  - Systemadministratoren implementieren und überwachen sie.
  - Mitarbeiter des Vorfallsmanagements untersuchen Warnmeldungen.
- **Dokumentation und Überprüfung**
  Integrieren Sie Hardware-Integritätsprüfungen in Sicherheitsrichtlinien, Risikobewertungen und Audit-Protokolle. Überprüfen Sie ihre Wirksamkeit mindestens einmal pro Jahr oder nach größeren Veränderungen oder Zwischenfällen.
- **Schulung der Mitarbeiter und Sensibilisierung**
  Schulen Sie die zuständigen Mitarbeiter darin, Anzeichen von Manipulationen zu erkennen, Integritätstools korrekt anzuwenden und Meldeverfahren einzuhalten.

DE.CM-09.3 Der Krisenreaktionsplan der Organisation muss Maßnahmen zur Aufdeckung unbefugter Eingriffe in die Hardware kritischer Systeme enthalten.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass der Notfallplan der Organisation Maßnahmen zur Erkennung und Reaktion auf unbefugte Eingriffe in kritische Hardware enthält. Dies hilft der Organisation, schnell und effektiv zu reagieren, wenn jemand versucht, wichtige Systeme physisch oder digital zu kompromittieren. Diese Kontrolle kann auf praktische und skalierbare Weise durchgeführt werden.

Durch die Berücksichtigung der nachstehenden Maßnahmen können auch kleine Organisationen die Erkennung von Hardwaremanipulationen effektiv in ihre Reaktionsmöglichkeiten auf Vorfälle einbeziehen, ohne dass dafür umfangreiche Ressourcen erforderlich sind:

- **Plan für die Reaktion auf Vorfälle**
  Der Plan für die Reaktion auf Vorfälle sollte klare Anweisungen enthalten, welche Schritte zu unternehmen sind, wenn der Verdacht auf Hardwaremanipulationen besteht.
- **Regelmäßige Inspektionen**
  Lassen Sie IT- und OT-Mitarbeiter oder benanntes Personal regelmäßig die kritische Hardware auf Anzeichen von Manipulationen überprüfen, wie z. B. gebrochene Siegel, lose Kabel oder unerwartete Veränderungen.
- **Überwachung von Tools**
  Einfache Tools können verwendet werden, um Warnmeldungen zu senden, wenn etwas Ungewöhnliches mit einem Gerät geschieht, z. B. wenn das Gehäuse geöffnet wird, ein neues USB-Gerät angeschlossen wird oder das System unerwartet neu gestartet wird. Viele dieser Tools sind so konzipiert, dass sie vor allem für kleine Organisationen erschwinglich und einfach zu nutzen sind.
- **Schulung und Sensibilisierung**
  Schulen Sie die Mitarbeiter darin, Anzeichen von Hardwaremanipulationen zu erkennen und verdächtige Aktivitäten zu melden. Sensibilisierung ist der Schlüssel zur Früherkennung.
- **Unterstützung von Anbietern**
  Nutzen Sie die Tools oder Dienste von Hardware-Anbietern, um Manipulationen zu erkennen. Diese sind häufig in Supportverträgen enthalten.

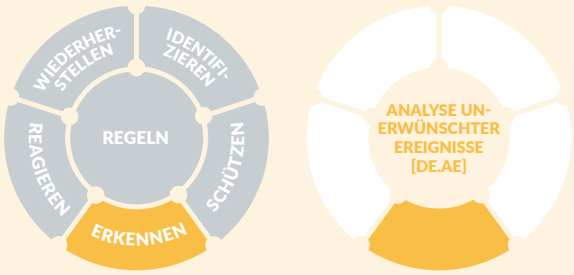
DE.CM-09.4 Die Organisation richtet ein System ein, um genau zwischen legitimen Warnmeldungen und Fehlalarmen zu unterscheiden und so eine effektive Erkennung und Entfernung von schädlichem Code sicherzustellen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation echte Bedrohungen genau erkennen kann und gleichzeitig unnötige Warnmeldungen aufgrund von Fehlalarmen vermieden werden. Dies trägt dazu bei, die Effektivität der Erkennung und Entfernung von schädlichem Code zu verbessern und gleichzeitig die Zeit- und Ressourcenverschwendung bei der Reaktion auf harmlose Aktivitäten zu reduzieren.

Um schädlichen Code effektiv zu erkennen und zu entfernen und gleichzeitig Fehlalarme zu vermeiden, sollten die folgenden Praktiken beachtet werden:

- **Automatische Updates**
  Tools zum Schutz vor schädlichem Code sollten so konfiguriert werden, dass sie nach Möglichkeit automatisch oder manuell nach einem festgelegten Zeitplan aktualisiert werden, entsprechend den Richtlinien der Organisation und den betrieblichen Einschränkungen.
- **Sichere Entwicklungspraktiken**
  Software, die in IT- und OT-Systemen eingesetzt wird, sollte sicheren Entwicklungspraktiken unterliegen, einschließlich Codeüberprüfungen und Schwachstellenanalysen, um das Risiko der Einschleusung von schädlichem Code zu minimieren.
- **Mehrschichtiger Schutz**
  Sowohl signaturbasierter Schutz (der bekannte Bedrohungen erkennt) als auch verhaltensbasierter Schutz (der nach ungewöhnlichen oder verdächtigen Aktivitäten sucht) sollten an Orten eingesetzt werden, an denen Netzwerke mit dem Internet verbunden sind, an denen Mitarbeiter auf Kontrollsysteme zugreifen und an denen Dateien oder Daten zwischen Systemen ausgetauscht werden.
- **Scannen nach Bedrohungen**
  Schutztools sollten so eingestellt sein, dass sie regelmäßige Scans und, soweit möglich, Echtzeitprüfungen von Dateien und Datenübertragungen durchführen, insbesondere von solchen, die aus externen Quellen oder von Wechselmedien stammen.
- **Blockierung und Quarantäne**
  Entdeckter schädlicher Code sollte blockiert und isoliert werden, um zu verhindern, dass er andere Systeme beeinträchtigt. In OT-Umgebungen sollte dies auf eine Weise geschehen, die den kritischen Betrieb nicht stört.
- **Warnungen und Benachrichtigungen**
  Warnungen sollten an die zuständigen Mitarbeiter gesendet werden, wenn schädliche Code entdeckt wird, mit klaren Verfahren für die Reaktion sowohl im IT- als auch im OT-Kontext.



Anomalien, Indikatoren für eine Kompromittierung und andere potenziell unerwünschte Ereignisse werden analysiert, um die Ereignisse zu charakterisieren und Cybersicherheitsvorfälle zu erkennen.

DE.AE-02 Potenziell unerwünschte Ereignisse werden analysiert, um die damit verbundenen Aktivitäten besser zu verstehen

DE.AE-02.1 Cybersecurity- und Informationssicherheitsereignisse werden überprüft und analysiert, um potenzielle Angriffsziele und -methoden in Übereinstimmung mit den geltenden Gesetzen, Vorschriften, Standards und Richtlinien zu ermitteln.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Ereignisse im Bereich der Cyber- und Informationssicherheit überprüft und analysiert werden, um Angriffsziele und -methoden zu erkennen. Dies ermöglicht es Organisationen, effektiv auf Bedrohungen zu reagieren und gleichzeitig die Einhaltung gesetzlicher, regulatorischer und richtlinienbezogener Anforderungen zu gewährleisten.

Um dieses Ziel zu erreichen, beachten Sie Folgendes:

- Organisationen sollten bei der Überprüfung von Sicherheitsvorfällen die einschlägigen Bundes- und Landesgesetze, Branchenvorschriften, Normen und internen Richtlinien beachten.
- Log-Analyse-Tools sollten verwendet werden, um Berichte zu erstellen und verdächtige Aktivitäten zu erkennen.
- System- und Anwendungsprotokolle sollten regelmäßig überprüft werden, um Anzeichen für Sicherheitsbedrohungen zu erkennen, z. B. wiederholte fehlgeschlagene Anmeldeversuche oder ungewöhnliche Datenübertragungen.
- Die Protokolle sollten auf Muster analysiert werden, die auf versuchte oder laufende Angriffe hinweisen.
- Bedrohungsdaten sollten genutzt werden, um über neue Bedrohungen und Angriffstechniken informiert zu sein, und die Sicherheitsmaßnahmen sollten entsprechend angepasst werden.
- Es sollten regelmäßige Prüfungen und Bewertungen durchgeführt werden, um die Sicherheitslage der Organisation zu beurteilen.
- Die Ergebnisse dieser Audits sollten zur Verbesserung der Überwachung und Analyse genutzt werden

DE.AE-02.2 Die Organisation implementiert, soweit möglich, automatisierte Mechanismen zur Überprüfung und Analyse erkannter Ereignisse.

Implementierungshinweise

Das Ziel dieser Kontrolle besteht darin, sicherzustellen, dass die Organisation, soweit praktikabel, Automatisierung einsetzt, um die effiziente und konsistente Überprüfung und Analyse erkannter Cybersicherheitsvorfälle zu unterstützen. Dies trägt dazu bei, das Risiko menschlicher Fehler zu verringern, die Erkennung von und Reaktion auf Bedrohungen zu beschleunigen und begrenzte Sicherheitsressourcen (insbesondere in kleineren Organisationen) auf höherwertige Aufgaben wie die Untersuchung komplexer Vorfälle oder die Verbesserung des Schutzes zu konzentrieren.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Nutzung integrierter Funktionen**
  Aktivieren und konfigurieren Sie Protokollierungs- und Warnfunktionen in bestehenden Plattformen (z. B. Microsoft 365, Google Workspace, Firewalls), um verdächtige Aktivitäten automatisch zu erkennen.
- **Einsatz von schlanken Erkennungstools**
  Nutzen Sie kostengünstige Endpoint Detection and Response (EDR)-Lösungen, die automatisierte Warnmeldungen und grundlegende Analysen bieten, beispielsweise zur Erkennung von Malware oder ungewöhnlichem Anmeldeverhalten.
- **Erwägung von Managed Detection Services**
  Für Organisationen mit begrenzten internen Ressourcen kann ein Managed Detection and Response (MDR)-Service ausgelagerte Überwachung, Bedrohungserkennung und Incident Response bieten.
- **Automatisierung in Bereichen mit hoher Auswirkung**
  Konzentrieren Sie die Automatisierung auf häufige Bedrohungsindikatoren, wie zum Beispiel:
  - Mehrere fehlgeschlagene Anmeldeversuche
  - Ungewöhnlicher Zugang zu sensiblen Dateien
  - Unerwarteter ausgehender Verkehr
- **Integration von Bedrohungsdaten**
  Verwenden Sie kostenlose oder kostengünstige Bedrohungsdaten-Feeds, um Erkennungstools mit bekannten Indikatoren für eine Gefährdung und das Verhalten von Angreifern zu verbessern.
- **Beibehaltung manueller Überprüfungsverfahren**
  Planen Sie regelmäßige manuelle Überprüfungen von Protokollen und Warnmeldungen, um Bedrohungen zu identifizieren, die automatisierte Tools möglicherweise übersehen, insbesondere solche, die neue oder subtile Angriffstechniken beinhalten.

DE.AE-03 Informationen aus verschiedenen Quellen werden miteinander in Beziehung gesetzt

DE.AE-03.1 Die Protokollierungsfunktion der Schutz- und Erkennungsinstrumente ist aktiviert. Die Protokolle werden gesichert, für einen vordefinierten Zeitraum aufbewahrt und regelmäßig überprüft, um ungewöhnliche oder potenziell schädliche Aktivitäten zu identifizieren.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Sicherheitstools die Protokollierung aktiviert haben, die Protokolle für eine bestimmte Zeit aufbewahrt werden und regelmäßig auf ungewöhnliche oder schädliche Aktivitäten überprüft werden. Dies hilft dabei, Bedrohungen frühzeitig zu erkennen und Maßnahmen zu ergreifen. Beispiele für solche Tools sind Firewalls, Antiviren-Software, Endpunkt-Erkennung und Intrusion Detection Systeme.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Protokolle sollten sicher aufbewahrt und gemäß einem festgelegten Aufbewahrungszeitplan auf der Grundlage geltender gesetzlicher, behördlicher oder betrieblicher Anforderungen aufbewahrt werden.
- Tools und Lösungen zur Erkennung von Ereignissen sollten so konfiguriert werden, dass sie bei verdächtigen oder schädlichen Aktivitäten automatische Warnmeldungen erzeugen.
- Es sollte ein dokumentiertes Verfahren zur regelmäßigen Überprüfung von Protokollen und Dashboards vorhanden sein, um eine rechtzeitige Erkennung und Reaktion zu unterstützen.
- Bei der Überprüfung der Protokolle sollten Muster wie wiederholte Malware-Infektionen, abnormaler Netzwerkverkehr oder übermäßiger Zugriff auf nicht geschäftsbezogene Websites festgestellt werden.
- Werden solche Muster festgestellt, sollten Folgemaßnahmen festgelegt werden, wie z. B. die Verstärkung bestimmter Sicherheitskontrollen, die Aktualisierung von Erkennungsregeln oder die Durchführung gezielter Sensibilisierungsmaßnahmen.

DE.AE-03.2 Die Organisation stellt sicher, dass Ereignisdaten aus kritischen Systemen unter Verwendung von Informationen aus mehreren relevanten Quellen erfasst und korreliert werden.

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Organisation in die Lage zu versetzen, komplexe oder verteilte Bedrohungen zu erkennen, indem Ereignisdaten aus verschiedenen Systemen und Quellen kombiniert und analysiert werden. Durch die Korrelation dieser Daten lassen sich Muster erkennen, die bei der isolierten Überwachung von Systemen möglicherweise nicht sichtbar sind.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Relevante Quellen für Ereignisdaten können Systemprotokolle, Audit-Protokolle, Netzwerküberwachungs-Tools, physische Zugriffsaufzeichnungen und Berichte von Benutzern oder Administratoren sein.
- Die Protokolldaten sollten kontinuierlich, idealerweise in Echtzeit oder nahezu in Echtzeit, zur Speicherung und Analyse an ein zentrales System übermittelt werden. Dies verbessert die Fähigkeit, Muster zu erkennen und schnell auf mögliche Probleme zu reagieren.
- Die Zentralisierung von Protokollen auf einer kleinen Anzahl dedizierter Server oder Plattformen, wie z. B. einem SIEM, schlanken Protokollverwaltungstools, Cloud-basierten Protokollierungsdiensten oder verwalteten Erkennungsdiensten (oft Teil von Managed Detection and Response, MDR), kann eine effiziente Analyse und Korrelation von Ereignissen über Systeme hinweg unterstützen.
- Cyber-Bedrohungsdaten können zur Verbesserung der Ereigniskorrelation verwendet werden, indem sie Kontext über bekannte Bedrohungen, Angriffsmethoden und Indikatoren für eine Gefährdung liefern.
- Bedrohungsdaten sollten sicher in Erkennungsinstrumente und -prozesse integriert werden, um eine genauere und rechtzeitige Identifizierung von Bedrohungen zu ermöglichen.

DE.AE-03.3 **Die Organisation kombiniert die Ereignisanalyse mit Informationen aus Schwachstellenscans, Systemleistungsdaten, der Überwachung kritischer Systeme und der Anlagenüberwachung, soweit dies möglich ist.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Fähigkeit der Organisation zu stärken, komplexe oder versteckte Bedrohungen zu erkennen, indem die Ereignisanalyse mit anderen relevanten Datenquellen kombiniert wird.

Diese umfassendere Sichtweise unterstützt eine genauere und rechtzeitige Identifizierung verdächtiger Aktivitäten, und um das Ziel dieser Kontrolle zu erreichen, sollte Folgendes berücksichtigt werden:

- Tools, die Daten aus verschiedenen Systemen erfassen und verknüpfen (wie SIEM, XDR oder SOAR), sollten zur Unterstützung dieser Integration eingesetzt werden.
- Sicherheitsprobleme, die von Lieferanten oder vertrauenswürdigen Quellen gemeldet werden, sollten schnell erfasst und auf mögliche Risiken überprüft werden.
- Daten aus verschiedenen Überwachungssystemen sollten zusammengeführt werden, um Muster oder Probleme leichter erkennen zu können.
- Die Einrichtung sollte eine schnelle Erkennung und Reaktion ermöglichen, wenn etwas Ungewöhnliches gefunden wird.

DE.AE-04 Die geschätzten Auswirkungen und das Ausmaß von unerwünschten Ereignissen sind bekannt

DE.AE-04.1 **Die Organisation bewertet die negativen Auswirkungen festgestellter Ereignisse auf ihre Betriebsabläufe, Vermögenswerte und Personen und setzt diese Auswirkungen in Beziehung zu den Ergebnissen ihrer Risikobewertungen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation versteht, wie entdeckte Ereignisse Schaden anrichten könnten, und dieses Verständnis als Grundlage für risikobasierte Entscheidungen und Reaktionen nutzt.

Um das Ziel dieser Kontrolle zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Zur Unterstützung dieser Bewertung sollten Tools eingesetzt werden, die helfen, den Umfang und die Auswirkungen von Ereignissen abzuschätzen.
- Bei der Bewertung sollte berücksichtigt werden, wie sich Probleme in einem Teil eines Systems auf andere verbundene Teile auswirken könnten.
- Zu den negativen Auswirkungen können finanzielle Verluste, Unterbrechungen von Diensten, Schäden an Geräten oder Personenschäden gehören.
- Zu den erkannten Ereignissen können Cybervorfälle, Systemausfälle oder Naturkatastrophen gehören.
- Der Schweregrad und die Wahrscheinlichkeit dieser Auswirkungen sollten bewertet und mit bestehenden Risikobewertungen verglichen werden.
- Dieser Vergleich sollte dabei helfen, Prioritäten für Maßnahmen zu setzen, Ressourcen zuzuweisen und die Reaktionsplanung zu verbessern.

DE.AE-06 Informationen über unerwünschte Ereignisse werden den befugten Mitarbeitern und den Tools zur Verfügung gestellt

DE.AE-06.1 **Informationen über unerwünschte Ereignisse werden umgehend an die autorisierten Mitarbeiter und Systeme weitergeleitet, um eine zeitnahe Erkennung, Untersuchung und Reaktion zu ermöglichen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Informationen über unerwünschte Ereignisse umgehend an die richtigen Personen und Systeme weitergeleitet werden, damit unverzüglich geeignete Maßnahmen ergriffen werden können. Dies unterstützt eine schnellere Erkennung, Untersuchung und Reaktion auf potenzielle Bedrohungen oder Unterbrechungen.

Um das Ziel dieser Kontrolle zu erreichen, berücksichtigen Sie bitte Folgendes:

- **Arten von unerwünschten Ereignissen**: Dazu gehören Indikatoren wie ungewöhnliche Kontoaktivitäten, unbefugter Zugriff, Änderungen der Systemkonfiguration, physische Sicherheitsverletzungen oder Malware-Warnungen.
- **Erkennung und Alarmierung**: Nutzen Sie Cybersicherheits-Tools, um derartige Ereignisse zu erkennen und autorisierte Mitarbeiter (z. B. SOC-Analysten, Incident Responder) automatisch zu alarmieren.
- **Integration mit Ticketingsystemen**: Die Warnmeldungen sollten in das Ticketingsystem der Organisation integriert werden. Tickets sollten:
  - Automatisch für vordefinierte Alarmtypen generiert werden.
  - Manuell erstellt werden, wenn technische Mitarbeiter verdächtige Aktivitäten feststellen.
- **Zugang zu Protokollen und Analysen**: Autorisierte Mitarbeiter müssen jederzeit Zugang zu Protokolldaten und Analyseergebnissen haben, um Untersuchungen zu unterstützen.
- **Bewertung von Reifegrad und Wirksamkeit**: Bewertung der Umsetzung der Kontrolle durch Überprüfung:
  - Dokumentation der Verfahren zur Erzeugung, Überprüfung und Eskalation von Warnmeldungen. Diese Dokumentation sollte regelmäßig überprüft und aktualisiert werden.
  - Einsatz von Automatisierung für Standardwarnungen, mit manuellen Prozessen als Backup.
  - Zugangskontrollen für Warnmeldungen und Protokolle mit regelmäßiger Überprüfung der Berechtigungen (der Zugang zu Warnmeldungen und Protokollen sollte auf befugte Mitarbeiter beschränkt sein).
  - Die Überwachung und Berichterstattung sollte beispielsweise die Anzahl der Warnmeldungen, die Reaktionszeiten und die Einhaltung der Verfahren erfassen.
  - Die mit der Bearbeitung von Warnmeldungen betrauten Mitarbeiter sollten regelmäßig geschult werden, um sicherzustellen, dass sie wissen, wie die Warnmeldungen zu interpretieren sind und wie man darauf reagiert.

DE.AE-08 Zwischenfälle werden gemeldet, wenn unerwünschte Ereignisse die definierten Kriterien für Vorfälle erfüllen.

DE.AE-08.1 Vorfälle werden gemeldet, wenn unerwünschte Ereignisse die definierten und dokumentierten Kriterien für Vorfälle erfüllen.

Implementierungshinweise

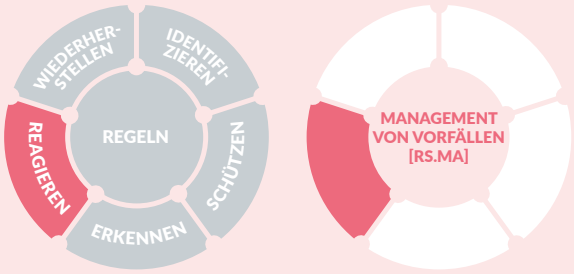
Ziel dieser Kontrolle ist es, sicherzustellen, dass unerwünschte Ereignisse identifiziert und gemeldet werden, wenn sie klar definierte und dokumentierte Kriterien erfüllen. Sie betont die Bedeutung einheitlicher Schwellenwerte und Richtlinien, um zu bestimmen, wann ein Ereignis als Vorfall einzustufen ist, und unterstützt so ein zeitnahes Bewusstsein und eine angemessene Eskalation oder Reaktion.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- Die Kriterien für Vorfälle (Regeln für die Einstufung als Vorfall) sollten klar definiert, dokumentiert und regelmäßig überprüft werden.
- Diese Kriterien sollten dabei helfen, zu bestimmen, wann ein unerwünschtes Ereignis zu einem meldepflichtigen Vorfall wird.
- Die Kriterien sollten auf bekannten Mustern normaler und abnormaler Aktivitäten beruhen, einschließlich der Lehren aus früheren Vorfällen.
- Bekannte falsch-positive Ergebnisse sollten bei der Festlegung der Kriterien berücksichtigt werden, um unnötige Meldungen zu vermeiden.
- Wenn ein Ereignis die definierten Kriterien erfüllt, sollte es als Vorfall behandelt und gemäß den Verfahren der Organisation gemeldet werden.
- Wo es sinnvoll und möglich ist, sollten die Systeme so konfiguriert werden, dass sie diesen Prozess unterstützen, indem sie Warnmeldungen erzeugen, wenn die Kriterien für einen Vorfall erfüllt sind. Dies kann dazu beitragen, Vorfälle schneller zu erkennen, insbesondere in größeren oder komplexeren Umgebungen.

REAGIEREN

Reagieren



Reaktionen auf erkannte Cybersicherheitsvorfälle werden verwaltet

RS.MA-01 Der Plan für die Reaktion auf einen Vorfall wird in Abstimmung mit den relevanten Dritten ausgeführt, sobald ein Vorfall gemeldet wird.

RS.MA-01.1 Während oder nach einem Cybersicherheitsvorfall, der die kritischen Systeme der Organisation betrifft, wird ein Plan zur Reaktion auf Vorfälle umgesetzt, der definierte Rollen, Verantwortlichkeiten und Befugnisse umfasst.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass während oder nach einem Cybersecurity-Ereignis, das sich auf die kritischen Systeme der Organisation auswirkt, ein genau definierter Plan zur Reaktion auf Vorfälle ausgeführt wird, der eine rechtzeitige Erkennung, Eindämmung, Kommunikation und Wiederherstellung ermöglicht.

Um dieses Ziel zu unterstützen, sollte die Organisation:

- **Einen dokumentierten Reaktionsplan entwickeln**
  Der Plan sollte vordefinierte Anweisungen und Verfahren zur Erkennung von Cybersicherheitsvorfällen, zur effektiven Reaktion und zur Unterstützung der Wiederherstellung kritischer Systeme enthalten.
- **Erkennungsfähigkeiten einbeziehen**
  Erkennungstechnologien sollten vorhanden sein, um bestätigte Vorfälle automatisch zu melden und Reaktionsmaßnahmen auszulösen.
- **Rollen, Verantwortlichkeiten und Befugnisse definieren**
  Der Plan sollte eindeutig Folgendes identifizieren:
  - Wer ist an der Reaktion beteiligt
  - Kontaktdaten der wichtigsten Mitarbeiter
  - Wer ist befugt, die Wiederherstellung einzuleiten
  - Wer ist für die externe Kommunikation zuständig (z. B. Regulierungsbehörden, Partner, Medien)
- **Den Plan regelmäßig überprüfen und aktualisieren**
  Der Plan sollte überprüft und aktualisiert werden, um Änderungen in der Bedrohungslage, der Organisationsstruktur oder den aus früheren Vorfällen gewonnenen Erkenntnissen Rechnung zu tragen.

- **Den Plan durch Übungen testen**
  Es sollten Simulationen und Tabletop-Übungen durchgeführt werden, um die Wirksamkeit des Plans zu überprüfen und Verbesserungsmöglichkeiten zu identifizieren.
- **OT-Umgebungen einbeziehen**
  Der Plan sollte die Reaktion auf einen Vorfall in OT-Systemen behandeln, einschließlich der Koordinierung mit Sicherheitsprotokollen, der Isolierung betroffener Industrieanlagen und der Wiederherstellung von Betriebsabläufen.

RS.MA-01.2 Die Organisation koordiniert Maßnahmen zur Reaktion auf Informations-/Cybersicherheitsvorfälle mit allen vorab festgelegten Stakeholdern.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle relevanten internen und externen Beteiligten bei einem Cybersecurity- oder Informationsvorfall effektiv zusammenarbeiten.

Um dieses Ziel zu erreichen:
- Sollten Maßnahmen zur Reaktion auf einen Vorfall mit vordefinierten Stakeholdern koordiniert werden, darunter Unternehmensleiter, IT- und OT-Systemverantwortliche, Cybersicherheitsteams, Anbieter, Personalabteilung, Rechtsabteilung, physische Sicherheit, Betrieb und Beschaffung.
- Sollte die Koordinierung gemäß dem dokumentierten Plan für die Reaktion auf Vorfälle der Organisation erfolgen.
- Sollte für jeden Vorfall eine leitende Person benannt werden, die die Reaktion verwaltet und für eine klare Kommunikation sorgt.
- Sollten, falls erforderlich, zusätzliche Pläne, wie z. B. Business Continuity oder Disaster Recovery, zur Unterstützung der Reaktion aktiviert werden.
- Sollten die Informationen zur richtigen Zeit an die richtigen Personen weitergegeben werden, und zwar nach festgelegten Kommunikationsverfahren.
- Sollten die verschiedenen Arten von Vorfällen erkannt und entsprechend behandelt werden:
  - Informationsvorfälle (z. B. versehentliche Datenexposition)
  - Vorfälle im Bereich der Cybersicherheit (z. B. Malware, Hacking)
  - OT-Vorfälle (z. B. Störungen industrieller Kontrollsysteme)
- Bei OT-Vorfällen sollten spezielle OT-Mitarbeiter hinzugezogen werden, und es können andere Reaktionsverfahren erforderlich sein, um Sicherheit und Betrieb zu schützen.

RS.MA-02 Berichte über Vorfälle werden gesichtet und validiert

RS.MA-02.1 Berichte über Informations-/Cybersicherheitsvorfälle werden in Übereinstimmung mit den Verfahren der Organisation zur Reaktion auf Vorfälle behandelt und validiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle gemeldeten Vorfälle systematisch überprüft und bewertet werden, bevor weitere Maßnahmen ergriffen werden. Diese Kontrolle ist ein grundlegender Schritt im Prozess der Reaktion auf Vorfälle, und Folgendes sollte berücksichtigt werden:
- **Unwichtige oder falsche Meldungen herausfiltern**
  Nicht jede eingegangene Meldung ist ein echter Vorfall. Durch diese Kontrolle wird sichergestellt, dass nur auf legitime, für die Cybersicherheit relevante Vorfälle reagiert wird.

- **Rechtzeitige und angemessene Reaktion**
  Durch die frühzeitige Einstufung und Validierung von Meldungen können Organisationen echten Bedrohungen Priorität einräumen und vermeiden, dass Ressourcen für nicht relevante Probleme verschwendet werden.
- **Unterstützung einer konsistenten Entscheidungsfindung**
  Die Anwendung strukturierter Triage- und Validierungskriterien trägt dazu bei, dass die Reaktion auf Vorfälle konsistent und wiederholbar ist und mit den Unternehmensrichtlinien übereinstimmt.
- **Ermöglichung einer effektiven Eskalation und Kategorisierung**
  Die Validierung ist eine Voraussetzung für die Kategorisierung und Eskalation von Vorfällen (wie in RS.MA-03.1 gefordert). Andernfalls könnte der Reaktionsprozess fehlgeleitet oder verzögert werden.
- **Verbesserung des Situationsbewusstseins**
  Eine frühzeitige Validierung trägt dazu bei, ein klareres Bild von der Bedrohungslandschaft zu erhalten und die Koordination zwischen den Teams zu verbessern.

RS.MA-02.2 Automatisierte Tools werden zur Unterstützung der Untersuchung und Folgenabschätzung validierter Vorfälle im Bereich der Cybersicherheit verwendet.

Implementierungshinweise

Mit dieser Kontrolle soll sichergestellt werden, dass die Organisationen mit den technischen Fähigkeiten ausgestattet sind, um Cybersicherheitsvorfälle effizient und genau zu behandeln, sobald sie validiert wurden.

Um diese Kontrolle zu implementieren, sollten folgende Punkte berücksichtigt werden:

- Automatisierte Tools sollten dabei helfen, Vorfallsdaten zu sammeln, zu analysieren und zu korrelieren, um eine zeitnahe und genaue Untersuchung zu unterstützen.
- Diese Tools sollten dabei helfen, den Umfang, die Schwere und die potenziellen Auswirkungen von Vorfällen zu ermitteln, die durch Sichtung validiert wurden. Ein validierter Vorfall ist ein Vorfall, bei dem bestätigt wurde, dass er mit der Cybersicherheit zusammenhängt (kein falscher Alarm oder ein nicht damit zusammenhängendes technisches Problem), vordefinierte Schwerekriterien erfüllt (z. B. Indikatoren für eine Gefährdung, Bedrohungsdaten oder bekannte Angriffsmuster) und der Reaktionsmaßnahmen erfordert (d. h. der Schwellenwert für eine weitere Untersuchung, Einstufung und Eskalation ist erreicht).
- Die folgenden Arten von Tools können zur Unterstützung dieser Aktivitäten in Betracht gezogen werden:
  - Security Information and Event Management-Systeme (SIEM-Systeme) für die zentralisierte Protokollerfassung und -analyse.
  - Extended Detection and Response (XDR)-Plattformen für die integrierte Erkennung von Bedrohungen an Endpunkten, in Netzwerken und auf Servern.
  - SOAR-Plattformen (Security Orchestration, Automation and Response) zur Automatisierung von Arbeitsabläufen und Koordinierung von Reaktionsmaßnahmen.
  - Threat Intelligence-Plattformen zur Anreicherung von Vorfallsdaten mit externem Bedrohungskontext.
  - Network Intrusion Detection Systems (NIDS) zur Überwachung und Meldung verdächtiger Netzwerkaktivitäten.
  - Computer Incident Response Centres (CIRCs) zur zentralen Koordinierung und Expertenanalyse.
- Automatisierte Mechanismen sollten in den Prozess der Reaktion auf Vorfälle integriert werden, um sicherzustellen, dass validierte Vorfälle effizient untersucht und in Übereinstimmung mit dem Plan der Organisation zur Reaktion auf Vorfälle angemessen priorisiert werden.

RS.MA-03 Vorfälle werden kategorisiert und nach Prioritäten geordnet

RS.MA-03.1 **Informations-/Cybersicherheitsvorfälle werden gemäß dem Reaktionsplan für Vorfälle kategorisiert, priorisiert und eskaliert.**

Implementierungshinweise

Diese Kontrolle ist eine Weiterentwicklung von RS.MA-02.1 und soll sicherstellen, dass ein Vorfall nach seiner Validierung systematisch nach seiner Art, Dringlichkeit und möglichen Auswirkung klassifiziert und verwaltet wird, so dass die Organisation effizient, konsequent und angemessen reagieren kann.

Daher sollten folgende Punkte berücksichtigt werden:

- Vorfälle sollten auf der Grundlage ihrer Art (z. B. Datenschutzverletzung, Ransomware, DDoS, Kontokompromittierung) und des validierten Ausmaßes ihrer Auswirkungen überprüft und klassifiziert werden.
- Die Schätzung und Validierung des Ausmaßes eines Vorfalls – weiterentwickelt in RS.AN-08.1 (Essential) – sollte die Einstufung und Priorisierung von Vorfällen beeinflussen.
- Indikatoren wie Umfang, Schweregrad und Zeitsensibilität sollten die Entscheidungen über die Priorisierung leiten.
- Software Bills of Materials (SBOM) können die Folgenabschätzung unterstützen, indem sie die betroffenen Komponenten und Abhängigkeiten identifizieren.
- Die Kriterien für die Einstufung, Priorisierung und Eskalation sollten im Reaktionsplan für Vorfälle dokumentiert und konsequent angewendet werden.
- Strategien zur Reaktion auf Vorfälle sollten die Notwendigkeit einer schnellen Wiederherstellung mit den potenziellen Vorteilen einer Beobachtung des Angreiferverhaltens oder einer tieferen Untersuchung abwägen.
- Die Eskalationsverfahren sollten mit den benannten internen und externen Beteiligten koordiniert werden, um eine rechtzeitige und angemessene Reaktion zu gewährleisten.

RS.MA-05 Die Kriterien für die Einleitung der Wiederherstellung eines Vorfalls werden angewendet

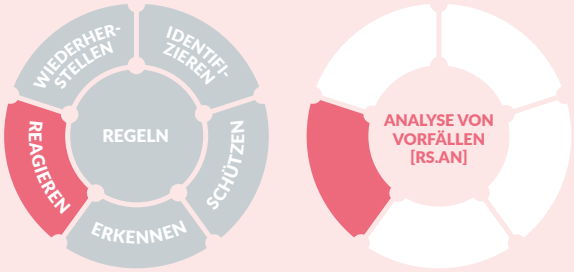
RS.MA-05.1 **Es sind eindeutige Kriterien zu definieren und anzuwenden, um zu bestimmen, wann Wiederherstellungsprozesse bei Vorfällen eingeleitet werden müssen.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Organisationen über einen klaren, konsistenten und risikobasierten Entscheidungsprozess verfügen, um zu bestimmen, wann Wiederherstellungsmaßnahmen nach einem Cybersicherheitsvorfall eingeleitet werden sollen.

Daher sollten folgende Punkte berücksichtigt werden:

- Die Kriterien für die Einleitung der Wiederherstellung nach einem Vorfall sollten auf den bekannten oder angenommenen Merkmalen des Vorfalls beruhen, wie z. B. der Schwere, dem Umfang und den möglichen Auswirkungen auf den Betrieb, die Daten oder die Systeme.
- Bei der Entscheidung, mit der Wiederherstellung zu beginnen, sollte auch die mögliche Störung des laufenden Betriebs durch die Wiederherstellungsmaßnahmen berücksichtigt werden.
- Wiederherstellungszeitpunkte (Recovery Point Objectives, RPO) und Wiederherstellungszeiten (Recovery Time Objectives, RTO) sollten in die Kriterien aufgenommen werden, um sicherzustellen, dass die Wiederherstellungsmaßnahmen mit den Anforderungen an die Geschäftskontinuität und den akzeptablen Schwellenwerten für Ausfallzeiten oder Datenverluste übereinstimmen.



Untersuchungen werden durchgeführt, um eine wirksame Reaktion zu gewährleisten und Forensik- und Wiederherstellungsaktivitäten zu unterstützen

RS.AN-03 Es wird eine Analyse durchgeführt, um festzustellen, was während eines Vorfalls geschehen ist und was die Ursache für den Vorfall war

RS.AN-03.1 Jeder Vorfall wird analysiert, um festzustellen, was geschehen ist, und um seine Ursache zu ermitteln.

Implementierungshinweise

Ziel dieser Kontrolle ist es, das gesamte Ausmaß eines Cybersicherheitsvorfalls zu verstehen und seine Ursache zu ermitteln, um eine wirksame Reaktion und die Prävention ähnlicher zukünftiger Ereignisse zu ermöglichen.

Um dieses Ziel zu erreichen, sollte die Organisation Folgendes berücksichtigen:

- Die Abfolge der Ereignisse während des Vorfalls sollte rekonstruiert werden, wobei zu ermitteln ist, welche Systeme, Vermögenswerte und Ressourcen beteiligt waren.
- Schwachstellen, Bedrohungen und Bedrohungsakteure, die mit dem Vorfall in Verbindung stehen, sollten ermittelt werden, unabhängig davon, ob sie direkt oder indirekt beteiligt sind.
- Bei Bedarf sollte eine forensische Analyse durchgeführt werden, um die gesammelten Daten zu untersuchen und die Ursache zu ermitteln.
- Die Analyse sollte sich darauf konzentrieren, die zugrundeliegenden, systemischen Ursachen zu ermitteln, nicht nur die unmittelbaren Auslöser.
- Cyber-Täuschungstechnologien sollten überprüft werden, um zusätzliche Erkenntnisse über das Verhalten von Angreifern zu gewinnen.

RS.AN-06 Die während einer Untersuchung durchgeführten Maßnahmen werden aufgezeichnet, und die Integrität und Herkunft der Aufzeichnungen wird gewahrt

RS.AN-06.1 Während einer Untersuchung durchgeführte Maßnahmen werden aufgezeichnet, und die Integrität und Herkunft der Aufzeichnungen wird gewahrt

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Maßnahmen, die während einer Untersuchung eines Vorfalls ergriffen werden, ordnungsgemäß aufgezeichnet werden und dass die Integrität und der Ursprung dieser Aufzeichnungen geschützt werden.

Um dieses Ziel zu erreichen, sollte die Organisation:

- Von allen an der Reaktion auf Vorfälle beteiligten Mitarbeitern (z. B. Responder, Systemadministratoren, Ingenieure) verlangen, dass sie ihre Maßnahmen so protokollieren, dass Manipulationen oder Löschungen verhindert werden.
- Dem Verantwortlichen für den Vorfall die Verantwortung für die Dokumentation der gesamten Untersuchung übertragen, einschließlich Zeitplänen, Entscheidungen und Informationsquellen.
- Sicherstellen, dass alle Aufzeichnungen sicher gespeichert werden und bis zu ihrer ursprünglichen Quelle zurückverfolgt werden können.

RS.AN-07 Daten und Metadaten von Vorfällen werden gesammelt und ihre Integrität und Herkunft wird bewahrt

RS.AN-07.1 Daten und Metadaten von Vorfällen sollen gesammelt und geschützt werden, um ihre Genauigkeit, Authentizität und Rückverfolgbarkeit sicherzustellen.

Implementierungshinweise

Das Ziel dieser Kontrolle ist es, sicherzustellen, dass alle relevanten Informationen zu einem Cybersicherheitsvorfall genau erfasst, sicher gespeichert und zuverlässig zurückverfolgt werden können, damit sie für Reaktions-, Untersuchungs- und Rechts- oder Compliance-Zwecke effektiv genutzt werden können.

Daher sollten folgende Punkte berücksichtigt werden:

- Vorfallsdaten und Metadaten (z. B. die Quelle der Daten und der Zeitpunkt ihrer Erfassung) sollten so erfasst und gespeichert werden, dass sie vor Manipulationen oder Verlust geschützt sind.
- Die Integrität und der Ursprung dieser Informationen sollten durch Methoden wie diese gewahrt werden:
  - **Dokumentation der Überwachungskette**, um zu verfolgen, wie die Daten von der Erfassung bis zur Analyse gehandhabt werden.
  - **Digitale Signaturen und Verschlüsselung** zum Schutz vor unbefugtem Zugriff und zur Bestätigung der Authentizität.
  - **Audit-Protokolle**, um aufzuzeichnen, wer wann auf die Daten zugegriffen oder sie geändert hat.
- Das Sammeln und der Schutz dieser Informationen sollten zu Folgendem beitragen:
  - **Einer zeitnahen Reaktion**, indem sie dabei helfen, zu verstehen, wann und wie sich der Vorfall ereignet hat.
  - **Einer Untersuchung und Analyse** durch Bereitstellung zuverlässiger Details über Ursache, Umfang und Auswirkungen des Vorfalls.
  - **Rechtlichen und Compliance-Anforderungen**, indem sichergestellt wird, dass die Daten bei Bedarf als Beweismittel verwendet werden können.

RS.AN-08 Das Ausmaß eines Vorfalls wird geschätzt und validiert

RS.AN-08.1 Das Ausmaß eines Vorfalls wird geschätzt und validiert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Organisationen ein klares Verständnis des vollen Umfangs und der Auswirkungen eines Cybersicherheitsvorfalls haben, so dass Reaktionsmaßnahmen angemessen skaliert, priorisiert und koordiniert werden können.

Daher sollten folgende Punkte berücksichtigt werden:

- Bei der Bewertung des Umfangs und der Auswirkungen eines Vorfalls sollte nicht nur das ursprünglich betroffene System untersucht werden, sondern auch andere Systeme oder Geräte, die möglicherweise gefährdet sind.
- Indikatoren für eine Gefährdung (Indicators of Compromise, IoCs), wie z. B. ungewöhnliche Netzwerkaktivitäten, unbefugte Zugriffsversuche oder unerwartete Softwareänderungen, sollten ermittelt werden, um zu verstehen, wie weit sich der Vorfall ausgebreitet hat.
- Anzeichen für ein Fortbestehen, einschließlich Hintertüren oder Malware, die einen weiteren Zugriff ermöglichen, sollten untersucht werden, um festzustellen, ob der Angreifer weiterhin in der Umgebung aktiv ist.
- Um eine zeitnahe und gründliche Analyse zu ermöglichen, sollten automatisierte Tools verwendet werden, um nach IoCs und Persistenzmechanismen in potenziell betroffenen Vermögenswerten zu suchen.
- Das validierte Ausmaß des Vorfalls sollte darüber Auskunft geben, wie der Vorfall kategorisiert, priorisiert und eskaliert wird, wie in RS.MA-03.1 (wichtig) beschrieben, um sicherzustellen, dass die Reaktionsmaßnahmen auf das tatsächliche Risiko und die geschäftlichen Auswirkungen abgestimmt sind.

Reaktionsmaßnahmen werden mit internen und externen Stakeholdern koordiniert, wie es die Gesetze, Vorschriften oder Richtlinien vorschreiben.

RS.CO-02 Interne und externe Stakeholdern werden über Vorfälle informiert

RS.CO-02.1 Informationen über Vorfälle im Bereich der Cybersicherheit werden den Mitarbeitern in einer klaren und leicht verständlichen Weise mitgeteilt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle Mitarbeiter zeitnah und in verständlicher Weise über Cybersicherheitsvorfälle informiert werden, damit sie angemessen reagieren und zur Risikominderung beitragen können.

Um dies zu erreichen:

- Sollte ein Plan zur Reaktion auf Vorfälle (Incident Response Plan, IRP) vorhanden sein. In diesem Plan wird dargelegt, wie die Organisation auf Cybersicherheitsvorfälle reagieren wird, einschließlich der Frage, wer wofür verantwortlich ist und wie verschiedene Arten von Bedrohungen eskaliert werden können.
- Der IRP sollte ein Kommunikationsprotokoll enthalten, in dem erläutert wird, wie genaue und relevante Informationen während eines Vorfalls schnell und effizient an die Mitarbeiter weitergegeben werden.
- Der Plan sollte die zu verwendenden Kommunikationskanäle festlegen, z. B. E-Mail, interne Messaging-Plattformen, Telefonanrufe oder ein spezielles Portal für Vorfälle.
- Vorlagen für Störfallmeldungen sollten im Voraus erstellt werden. Diese Vorlagen sollten wichtige Details enthalten, z. B. die Art des Vorfalls, wie schwerwiegend er ist, welche Systeme betroffen sind und welche Maßnahmen die Mitarbeiter ergreifen sollten.
- Die Mitteilungen sollten in einer klaren, einfachen Sprache verfasst sein, die Fachbegriffe vermeidet, so dass alle Mitarbeiter verstehen können, was geschieht und was von ihnen erwartet wird.
- Die Geschäftsleitung sollte Zusammenfassungen auf hoher Ebene erhalten, in denen die Auswirkungen des Vorfalls, die damit verbundenen Risiken und die Schritte zur Behebung des Problems erläutert werden.

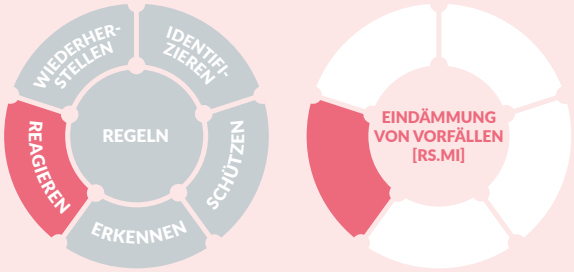
RS.CO-02.2 **Cybersecurity-Vorfälle werden innerhalb der im Plan zur Reaktion auf Vorfälle festgelegten Fristen an die relevanten externen Beteiligten weitergegeben, einschließlich der gesetzlich vorgeschriebenen Meldung wichtiger Vorfälle an die Behörden.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass alle relevanten externen Parteien rechtzeitig, sicher und angemessen über Cybersicherheitsvorfälle informiert werden, um das Vertrauen zu erhalten und gesetzliche und vertragliche Verpflichtungen zu erfüllen.

Um dies zu erreichen:

- Die Weitergabe von Informationen sollte sicher und im Einklang mit dem Plan der Organisation zur Reaktion auf Vorfälle und etwaigen Vereinbarungen über die Weitergabe von Informationen erfolgen.
- Zu den relevanten Stakeholdern können bestimmte interne Rollen, betroffene Kunden, Lieferanten, Drittdienstleister und Geschäftspartner gehören.
- Kunden und Partner sollten benachrichtigt werden, wenn sie von einem Vorfall betroffen sind, und klare Anweisungen erhalten, welche Maßnahmen sie ergreifen müssen.
- Die Kommunikation mit externen Parteien sollte entsprechend den vertraglichen Anforderungen oder Vereinbarungen erfolgen.
- Die Krisenkommunikation sollte mit kritischen Lieferanten koordiniert werden, um eine einheitliche Kommunikation zu gewährleisten.
- Bei der Weitergabe von Informationen über Taktiken oder Techniken von Angreifern sollten alle sensiblen oder identifizierenden Daten entfernt werden.
- Die Personalabteilung sollte informiert werden, wenn es sich bei dem Vorfall um schädliche Aktivitäten eines Insiders handelt.
- Die Geschäftsleitung sollte regelmäßig über den Stand der Dinge bei größeren Vorfällen informiert werden.
- Nationale Behörden wie das CSIRT, die Strafverfolgungsbehörden oder die Aufsichtsbehörden sollten auf der Grundlage der im IRP festgelegten Kriterien und mit Genehmigung der Geschäftsleitung benachrichtigt werden.
- Die gesamte Berichterstattung sollte den relevanten nationalen und EU-Rechtsvorschriften, wie der EU-Durchführungsverordnung, entsprechen.
- Öffentliche Aktualisierungen über Vorfälle werden unter einer separaten Kontrolle (RC.CO-04.1) behandelt.



Aktivitäten werden durchgeführt, um die Ausbreitung eines Vorfalls zu verhindern und seine Auswirkungen einzudämmen

RS.MI-01 Vorfälle werden eingedämmt

RS.MI-01.1 **Cybersicherheitsvorfälle werden eingedämmt und beseitigt. Jede Entscheidung über die Übernahme und Beibehaltung bestimmter Cybersicherheitsrisiken ist förmlich zu dokumentieren.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, die Ausbreitung von Cybersicherheitsvorfällen zu verhindern, ihre Ursache zu beseitigen und sicherzustellen, dass alle akzeptierten Risiken eindeutig erfasst und genehmigt werden.

Um dies zu erreichen:

- Sollte ein formeller Prozess zur Risikoakzeptanz für Cybersicherheitsrisiken eingerichtet werden, die als wenig folgenschwer gelten und keine Gefahr für kritische Geschäftssysteme darstellen. Diese Risiken sollten von der verantwortlichen Person oder dem Team auf der Grundlage der Risikotoleranz der Organisation überprüft und genehmigt werden.
- Cybersicherheitstools wie Antivirensoftware oder integrierte Sicherheitsfunktionen in Betriebssystemen und Netzwerkgeräten sollten die Möglichkeit haben, automatisch Maßnahmen zur Eindämmung oder Beseitigung von Bedrohungen zu ergreifen, wenn dies angemessen ist.
- Reaktionsteams für Vorfälle sollten in der Lage sein, bei Bedarf manuell Maßnahmen zur Beendigung und Beseitigung von Vorfällen auszuwählen und auszuführen.
- Vertrauenswürdige Drittparteien, wie z. B. Internetdienstleister oder Anbieter von verwalteten Sicherheitsdiensten, sollten bei Eindämmungs- und Beseitigungsmaßnahmen helfen dürfen, wenn dies Teil des Reaktionsplans der Organisation ist.

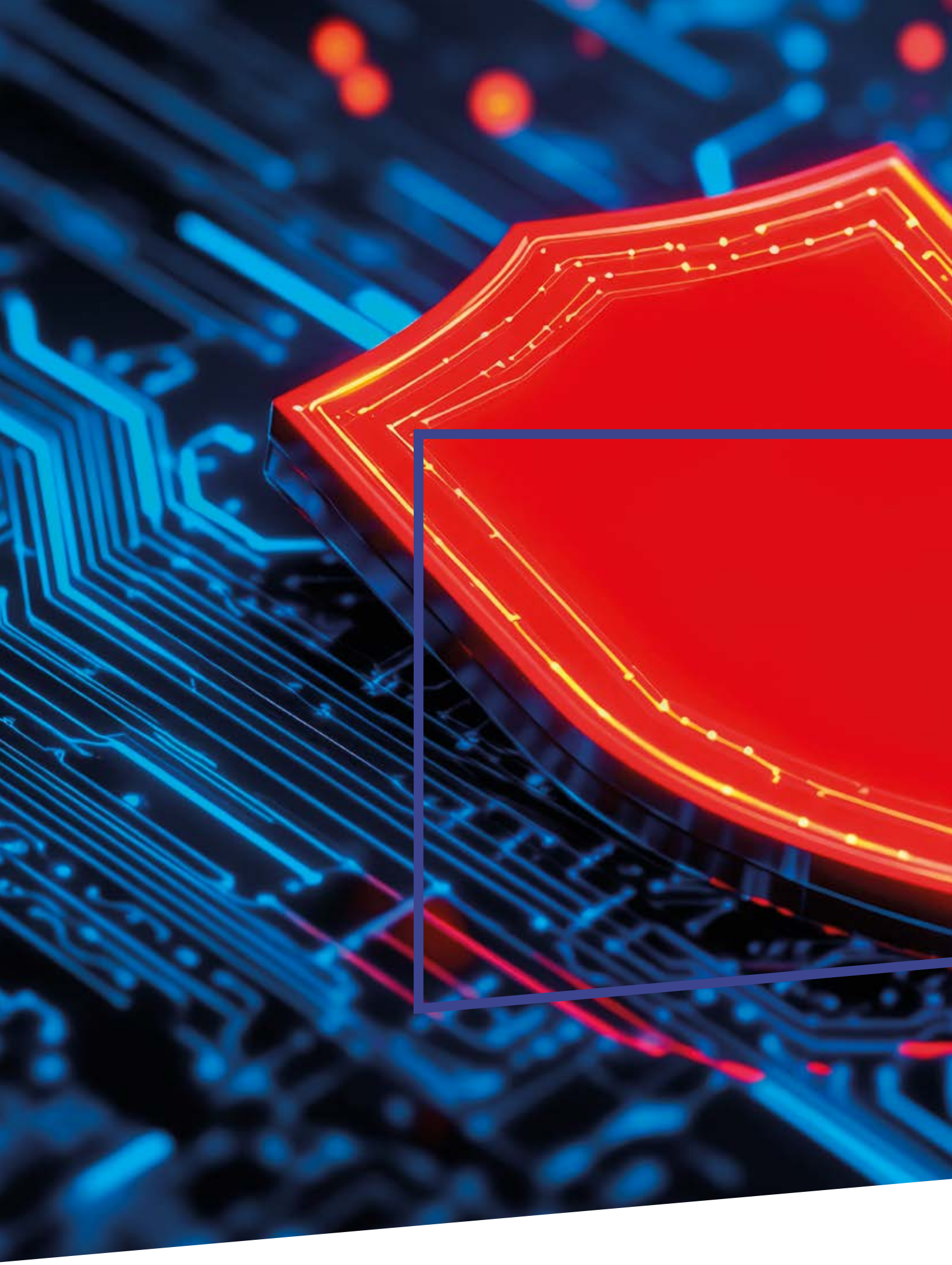
RS.MI-01.2 Die Organisation erkennt unbefugten Zugriff oder Datenlecks und ergreift geeignete Abhilfemaßnahmen, einschließlich der Überwachung kritischer Systeme an externen Grenzen und wichtigen internen Punkten.

Implementierungshinweise

Ziel dieser Kontrolle ist es, unbefugte Zugriffe und Datenlecks rechtzeitig zu erkennen und geeignete Abhilfemaßnahmen zu ergreifen. Dies soll dazu beitragen, die Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit von Daten zu schützen, unabhängig davon, ob sie gespeichert, übertragen oder aktiv genutzt werden, und zwar sowohl in IT- als auch in OT-Umgebungen (Operational Technology).

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Kritische Systeme überwachen**
  An den externen Netzgrenzen und an wichtigen internen Punkten erfolgen, um Anomalien oder unbefugte Zugriffsversuche zu erkennen.
- **Daten in allen Zuständen schützen**
  Die Daten sollten durch Verschlüsselung, digitale Signaturen und kryptografische Hashes geschützt werden, um die Vertraulichkeit und Integrität während der Speicherung, Übertragung und Nutzung zu gewährleisten.
- **Die ausgehende Kommunikation kontrollieren**
  Ausgehende Mitteilungen, die sensible Daten enthalten, sollten je nach Datenklassifizierung automatisch blockiert oder verschlüsselt werden.
- **Die Nutzung persönlicher Services einschränken**
  Der Zugang zu persönlichen Kommunikationsplattformen (z. B. persönliche E-Mails, File-Sharing-Services) von organisatorischen Systemen aus sollte eingeschränkt werden, um das Risiko von Datenlecks zu verringern.
- **Die Wiederverwendung von Daten in Nicht-Produktionsumgebungen verhindern**
  Sensible Produktionsdaten sollten nicht in Entwicklungs- oder Testumgebungen wiederverwendet werden, sofern sie nicht ordnungsgemäß anonymisiert oder maskiert sind.
- **Temporäre Daten löschen**
  Sensible Daten sollten aus dem Speicher oder dem temporären Zwischenspeicher gelöscht werden, sobald sie nicht mehr benötigt werden.
- **Das Identitäts- und Zugriffsmanagement auditieren**
  Systeme wie Microsoft Active Directory sollten regelmäßig auditiert werden, wobei der Schwerpunkt auf privilegierten Konten und der Konsistenz der Zugriffskontrolle liegen sollte.
- **OT-spezifische Machbarkeit sicherstellen**
  In OT-Umgebungen sollten Erkennungs- und Abhilfemaßnahmen angepasst werden, um eine Beeinträchtigung der Sicherheit oder der Betriebskontinuität zu vermeiden. Passive Überwachung und Protokollierung auf Schnittstellenebene können eingesetzt werden, wenn eine direkte Integration nicht möglich ist.
- **Sich an den ENISA-Leitlinien orientieren**
  Diese Praktiken stehen im Einklang mit den ENISA-Berichten zur Bedrohungslandschaft und den Leitlinien zu Informationslecks, die Empfehlungen zur Erkennung und Eindämmung von Datenschutzverletzungen und unbefugtem Zugriff enthalten.



WIEDER-
HERSTELLEN

Wiederherstellen

Es werden Wiederherstellungsmaßnahmen durchgeführt, um die betriebliche Verfügbarkeit von Systemen und Diensten zu gewährleisten, die von Cybersicherheitsvorfällen betroffen sind

RC.RP-01 Der Wiederherstellungsteil des Vorfallsreaktionsplans wird ausgeführt, sobald er vom Vorfallsreaktionsprozess initiiert wurde

RC.RP-01.1 Wiederherstellungsprozesse für Katastrophen und Informations-/Cybersicherheitsvorfälle werden entwickelt und durchgeführt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation schnell und effektiv auf Katastrophen, Informationssicherheitsvorfälle und Cybersecurity-Ereignisse reagieren kann, indem ein strukturierter Wiederherstellungsprozess entwickelt und ausgeführt wird, der Menschen, Systeme und Daten schützt.

Um dieses Ziel zu unterstützen, sollte die Organisation:

- **Einen Wiederherstellungsprozesses entwickeln**
  Ein dokumentierter Prozess sollte die Sofortmaßnahmen im Falle eines Brandes, eines medizinischen Notfalls, eines Diebstahls, einer Naturkatastrophe oder eines Vorfalls im Bereich der Informations- und Cybersicherheit leiten.
- **Rollen und Zuständigkeiten definieren**
  Im Wiederherstellungsprozess sollte festgelegt werden, wer zur Einleitung von Wiederherstellungsverfahren befugt ist und wer mit externen Beteiligten kommuniziert.
- **Informationen und Systeme schützen**
  Der Prozess sollte Schritte zur Sicherung von Informationen und Systemen beinhalten, wie z. B. das Abschalten oder Sperren von Geräten, die Umstellung auf Backup-Standorte oder die Sicherung physischer Dokumente.
- **Verfahren zur Kontaktaufnahme festlegen**
  Eine Liste mit internen und externen Kontakten sollte geführt und in den Wiederherstellungsplan aufgenommen werden, damit sie bei einem Vorfall schnell zugänglich sind.
- **Sensibilisierung und Bereitschaft sicherstellen**
  Personen, die für die Wiederherstellung verantwortlich sind, sollten mit dem Wiederherstellungsplan vertraut sein und wissen, welche Genehmigungen zur Durchführung der einzelnen Schritte erforderlich sind.
- **Mit dem Incident Response Plan integrieren**
  Der Wiederherstellungsprozess sollte Teil des umfassenderen Incident Response Plan (IRP) sein oder mit diesem abgestimmt werden, um Konsistenz und Koordination zu gewährleisten.

- **OT-Umgebungen einbeziehen**
  Die Wiederherstellungsplanung sollte OT-Systeme berücksichtigen, einschließlich Verfahren zur Wiederherstellung des industriellen Betriebs, zur Sicherung von Steuerungssystemen und zur Koordinierung mit Sicherheitsprotokollen.
- **Für künftige Verbesserungen planen**
  Diese Kontrolle dient als Grundlage für eine fortgeschrittene Wiederherstellungsplanung, die in der Kontrolle RC.RP-06.1 weiter entwickelt wird.

RC.RP-02 Wiederherstellungsmaßnahmen werden ausgewählt, eingegrenzt, nach Prioritäten geordnet und durchgeführt.

RC.RP-02.1 Die wesentlichen Funktionen und Dienste der Organisation sollen mit geringem oder ohne Verlust der Betriebskontinuität fortgeführt, und die Kontinuität wird bis zur vollständigen Wiederherstellung des Systems aufrechterhalten.

Implementierungshinweise

Ziel dieser Kontrolle ist es, Störungen kritischer Betriebsabläufe während Vorfällen zu minimieren und sicherzustellen, dass diese funktionsfähig bleiben, bis die Systeme vollständig wiederhergestellt sind.

Um dieses Ziel zu erreichen, sollte die Organisation:

- **Für Kontinuität planen**
  - Es sollte ein Betriebskontinuitätsplan erstellt werden, um wesentliche Funktionen zu identifizieren und Verfahren für einen unterbrechungsfreien Betrieb während Vorfällen festzulegen.
  - Es sollte ein Vorfallreaktionsplan enthalten sein, in dem die Schritte zur Eindämmung, Schadensbeurteilung und stufenweisen Wiederherstellung aufgeführt sind.
- **Den Betrieb bis zur Wiederherstellung aufrechterhalten**
  - Kontinuitätsmaßnahmen sollten die wesentlichen Funktionen unterstützen, bis eine vollständige Wiederherstellung erreicht ist.
  - Vorübergehende Umgehungslösungen, redundante Systeme oder manuelle Verfahren sollten eingesetzt werden, wenn dies zur Aufrechterhaltung des Betriebs erforderlich ist.
- **Wiederherstellung priorisieren**
  - Zur Festlegung der Wiederherstellungsprioritäten sollten eine Analyse der betrieblichen Auswirkungen und eine Systemkategorisierung vorgenommen werden.
  - Systeme sollten auf der Grundlage der Auswirkungen eines Verlusts der Verfügbarkeit, Integrität oder Vertraulichkeit kategorisiert werden, wobei sicherheitskritischen OT-Umgebungen besondere Aufmerksamkeit gewidmet werden sollte.
- **Datenresilienz sicherstellen**
  - Um eine schnelle und zuverlässige Datenwiederherstellung zu ermöglichen, sollten robuste Backup-Lösungen eingesetzt werden.
  - Backups sollten gesichert und regelmäßig getestet werden.
- **Überwachen und Reagieren**
  - Systeme sollten kontinuierlich überwacht werden, um Störungen frühzeitig zu erkennen.
  - Es sollten schnelle Maßnahmen ergriffen werden, um die Auswirkungen auf den Betrieb zu minimieren.
- **Testen und Verbessern**
  - Wiederherstellungsverfahren sollten regelmäßig getestet werden, um ihre Wirksamkeit sicherzustellen.
  - Die Wiederherstellungsmaßnahmen sollten dokumentiert und überprüft werden, um die Bereitschaft im Laufe der Zeit zu verbessern.

RC.RP-05 Die Integrität der wiederhergestellten Anlagen wird verifiziert, Systeme und Dienste werden wiederhergestellt und der normale Betriebszustand wird bestätigt

RC.RP-05.1 Die Integrität wiederhergestellter Systeme und Anlagen wird überprüft, bevor sie wieder in Betrieb genommen werden. Die Systeme und Services werden vollständig wiederhergestellt, und der normale Betrieb bestätigt.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass Systeme und Services nach einem Vorfall nicht nur wiederhergestellt werden, sondern auch überprüft wird, dass sie sicher, unversehrt und voll funktionsfähig sind, bevor der normale Betrieb wieder aufgenommen wird.

Um dieses Ziel zu erreichen, sollten die folgenden Punkte berücksichtigt werden:

- Wiederhergestellte Systeme sollten auf Anzeichen einer Kompromittierung, wie Schadsoftware oder unbefugten Zugriff, überprüft werden, bevor sie wieder online gestellt werden.
- Die Ursache des Vorfalls sollte ermittelt und beseitigt werden, um eine Wiederholung zu verhindern.
- Alle Wiederherstellungsmaßnahmen sollten überprüft werden, um sicherzustellen, dass sie korrekt durchgeführt wurden und keine Sicherheitslücken bestehen.
- Eine abschließende Prüfung sollte bestätigen, dass das System sicher, vollständig und für den normalen Gebrauch bereit ist.

RC.RP-06 Das Ende der Wiederherstellung des Vorfalls wird auf der Grundlage von Kriterien erklärt, und die Dokumentation des Vorfalls wird abgeschlossen

RC.RP-06.1 Das Ende der Wiederherstellung nach einem Vorfall wird anhand vordefinierter Kriterien offiziell erklärt, und alle dokumentationsrelevanten Unterlagen zum Vorfall werden vervollständigt und überprüft.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass der Prozess zur Wiederherstellung nach einem Vorfall formell und verantwortungsbewusst abgeschlossen wird und dass eine umfassende Dokumentation erstellt wird, um die Rechenschaftspflicht, das Lernen und die zukünftige Breitschaft zu unterstützen.

Um dieses Ziel zu erreichen, sollten die folgenden Punkte berücksichtigt werden:

- Es sollte ein Nachbericht erstellt werden, der Folgendes enthält:
  - Eine Zusammenfassung des Vorfalls und seiner Auswirkungen.
  - Die Schritte, die zur Reaktion und Wiederherstellung unternommen wurden.
  - Lehren und Empfehlungen für Verbesserungen.
- Bevor die Widerherstellungsphase für abgeschlossen erklärt werden kann, sollten die folgenden Kriterien erfüllt sein:
  - Alle betroffenen Systeme und Services sind voll funktionsfähig.
  - In der Umgebung gibt es keine bekannten Bedrohungen oder Schwachstellen.
  - Die Daten wurden wiederhergestellt und auf ihre Integrität verifiziert.
  - Erforderliche Sicherheits-Patches oder Updates wurden installiert.
  - Es gibt eine Überwachung, um wiederkehrende oder damit verbundene Probleme zu erkennen.
  - Der After-Action-Bericht wird fertiggestellt und von den relevanten Stakeholdern überprüft.
  - Alle Beteiligten werden darüber informiert, dass der Vorfall aufgeklärt wurde.

Die Wiederherstellungsaktivitäten werden mit internen und externen Parteien koordiniert

RC.CO-03 Die Wiederherstellungsmaßnahmen und die Fortschritte bei der Wiederherstellung der Betriebsfähigkeit werden den benannten internen und externen Stakeholdern mitgeteilt

RC.CO-03.1 Wiederherstellungsmaßnahmen und Fortschritte bei der Wiederherstellung der Betriebsfähigkeit werden gemäß den festgelegten Kommunikationsverfahren an bestimmte interne und externe Stakeholder kommuniziert.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Wiederherstellungsmaßnahmen und die Fortschritte bei der Wiederherstellung der Betriebsfähigkeit allen relevanten internen und externen Stakeholdern klar und konsistent kommuniziert werden. Dies unterstützt die Transparenz, die Koordination und die fundierte Entscheidungsfindung während der Wiederherstellungsphase eines Vorfalls.

Um dieses Ziel zu erreichen, sollten die folgenden Punkte berücksichtigt werden:

- Aktuelle Informationen zur Wiederherstellung, einschließlich der Fortschritte bei der Wiederherstellung von Systemen und Services, sollten sicher und einheitlich an interne und externe Stakeholder weitergegeben werden, in Übereinstimmung mit den Reaktionsplänen der Organisation und den Vereinbarungen über den Informationsaustausch.
- Die Geschäftsleitung sollte regelmäßig über den Stand der Wiederherstellungsmaßnahmen informiert werden, insbesondere bei größeren Vorfällen.
- Die in den Verträgen mit Lieferanten und Partnern festgelegten Kommunikationsprotokolle sollten eingehalten werden, um einen rechtzeitigen und genauen Informationsaustausch zu gewährleisten.
- Die Krisenkommunikation mit kritischen Lieferanten sollte koordiniert werden, um abgestimmte Wiederherstellungsmaßnahmen zu unterstützen.
- Wenn keine tatsächlichen Vorfälle stattgefunden haben, sollten Tabletop-Übungen durchgeführt werden, um die Kommunikationsverfahren für die Wiederherstellung und die Koordination der Stakeholder zu testen und zu validieren.

RC.CO-04 Die Öffentlichkeit wird über die Wiederherstellung von Vorfällen mithilfe genehmigter Methoden und Mitteilungen informiert

RC.CO-04.1 **Öffentliche Informationen zur Wiederherstellung nach einem Vorfall werden über genehmigte Kommunikationskanäle und Nachrichten gemäß den festgelegten Verfahren weitergegeben.**

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die öffentliche Kommunikation während der Wiederherstellungsphase eines Vorfalls korrekt und rechtzeitig erfolgt und über genehmigte Kanäle weitergeleitet wird, um das Vertrauen aufrechtzuerhalten, das Reputationsrisiko zu beherrschen und die gesetzlichen oder behördlichen Verpflichtungen zu erfüllen.

Um dieses Ziel zu erreichen, sollten die folgenden Punkte berücksichtigt werden:

- Bewährte Methoden der öffentlichen Kommunikation, wie Pressemitteilungen, offizielle Websites oder benannte Sprecher, sollten im Voraus festgelegt und konsequent eingesetzt werden.
- Es sollten Kontaktinformationen für relevante Parteien (z. B. interne Mitarbeiter, Drittanbieter, Strafverfolgungsbehörden, Anbieter von Cyber-Versicherungen, Regierungsbehörden) erstellt und gepflegt werden.
- Die Kontaktlisten sollten regelmäßig (z. B. jährlich) überprüft und verifiziert werden, um ihre Richtigkeit sicherzustellen.
- Es sollten primäre und sekundäre Kommunikationsmechanismen (z. B. Telefonanrufe, E-Mails, Briefe) festgelegt werden, wobei zu berücksichtigen ist, dass einige Methoden während eines Vorfalls nicht verfügbar sein können.
- Die Kommunikationsprotokolle und -mechanismen sollten in regelmäßigen Abständen oder bei wesentlichen organisatorischen Änderungen überprüft werden.
- Wenn keine tatsächlichen Vorfälle stattgefunden haben, sollten Tabletop-Übungen oder Simulationen durchgeführt werden, um die Verfahren zur öffentlichen Kommunikation zu testen und die Bereitschaft sicherzustellen.

RC.CO-04.2 **Die Organisation benennt einen Beauftragten für Öffentlichkeitsarbeit (Public Relations Officer, PRO), der die Kommunikation mit der Öffentlichkeit während der Wiederherstellung nach einem Informations-/Cybersicherheitsvorfall leitet und sicherstellt, dass die Öffentlichkeit unter Wahrung der Vertraulichkeit, Integrität und Genauigkeit der Informationen auf dem Laufenden gehalten wird.**

Implementierungshinweise

Das Ziel dieser Kontrolle ist es, sicherzustellen, dass die öffentliche Kommunikation während der Wiederherstellung von Cybersicherheits- oder Informationssicherheitsvorfällen professionell gehandhabt wird, korrekt ist und mit den Vertraulichkeits- und Integritätsstandards der Organisation übereinstimmt. Durch die Ernennung eines spezifischen Public Relations Officers (PRO) stellt die Organisation sicher, dass die Kommunikation mit der Öffentlichkeit von einer geschulten Person wahrgenommen wird, die das Vertrauen aufrechterhalten, den Ruf der Organisation schützen und die gesetzlichen und regulatorischen Anforderungen erfüllen kann.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Ernennung eines Public Relations Officer (PRO)**: Ernennen Sie eine qualifizierte Person, die sich um die öffentliche Kommunikation während der Wiederherstellung eines Zwischenfalls kümmert. Die Tätigkeitsbeschreibung des PRO kann Folgendes umfassen:
  - Entwicklung von Kommunikationsstrategien
  - Verfassen und Verbreiten von Pressemitteilungen

    - Aufbau und Pflege von Beziehungen zu Journalisten und Medien, um eine positive Berichterstattung zu gewährleisten (Medienarbeit).
    - Handhabung der Kommunikation in Krisenzeiten, um den Ruf der Organisation zu wahren (Krisenmanagement).
    - Verfolgung der Medienberichterstattung und Durchführung von Medienanalysen zur Einschätzung der öffentlichen Wahrnehmung (Beobachtung der Medienberichterstattung).
- **Entwicklung von Kommunikationsprotokollen**: Legen Sie klare Protokolle fest, die der PRO bei der Weitergabe von Informationen an die Öffentlichkeit befolgt, um die Vertraulichkeit, Integrität und Genauigkeit aller Informationen zu gewährleisten.
- **Schulung und Vorbereitung**: Schulen Sie den PRO in Kommunikationsstrategien für Zwischenfälle und stellen Sie sicher, dass er darauf vorbereitet ist, bei einem Zwischenfall schnell zu handeln.
- **Regelmäßige Überprüfungen**: Überprüfen und aktualisieren Sie die Kommunikationsprotokolle regelmäßig, um sie an neue Herausforderungen anzupassen und ihre Wirksamkeit zu gewährleisten.

RC.CO-04.3 Die Organisation setzt eine Krisenkommunikationsstrategie um, um negative Auswirkungen während einer Krise einzudämmen und dabei zu helfen ihren Ruf nach der Krise wiederherzustellen.

Implementierungshinweise

Ziel dieser Kontrolle ist es, sicherzustellen, dass die Organisation auf ein effektives Kommunikationsmanagement während und nach einer Krise vorbereitet ist, um Reputationsschäden zu minimieren, das Vertrauen der Stakeholder zu erhalten und den Wiederaufbau zu unterstützen.

Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **Entwickelung der Strategie**: Erstellen Sie einen umfassenden Krisenkommunikationsplan, der die Verfahren für die Kommunikation mit Mitarbeitern, Kunden, Partnern, Aufsichtsbehörden und den Medien während und nach einer Krise festlegt. Stellen Sie sicher, dass die gesamte Kommunikation den gesetzlichen Anforderungen und Branchenvorschriften entspricht.
- **Weisen Sie Rollen und Verantwortlichkeiten zu**: Ernennen Sie ein Krisenkommunikationsteam, einschließlich eines Sprechers, das sich um die öffentliche und interne Kommunikation kümmert. Die Beteiligung von PR-Fachkräften, Rechtsberatern und Führungskräften sollte in Betracht gezogen werden.
- **Einrichtung von Kommunikationskanälen**: Ermitteln Sie zuverlässige Kanäle für die Verbreitung von Informationen, z. B. soziale Medien, Pressemitteilungen und interne Kommunikationsplattformen, und richten Sie diese ein. Die Medienberichterstattung und die sozialen Medien sollten kontinuierlich auf Fehlinformationen oder negative Stimmungen überwacht werden. Auf Ungenauigkeiten sollte sofort reagiert und diese korrigiert werden.
- **Schulungen und Übungen**: Führen Sie regelmäßig Schulungen und Krisensimulationen durch, um sicherzustellen, dass das Team auf eine effektive Reaktion vorbereitet ist.
- **Überwachung und Anpassung**: Überwachen Sie die Situation kontinuierlich und passen Sie die Kommunikationsstrategie bei Bedarf an die sich verändernden Umstände an.
- **Überprüfung nach der Krise**: Überprüfen Sie nach der Krise die Kommunikationsmaßnahmen, um Erkenntnisse zu identifizieren und zukünftige Reaktionen zu verbessern.

ANHÄNGE

ANHANG A: LISTE DER SCHLÜSSELMASSNAHMEN FÜR DAS SICHERHEITSNIVEAU „BASIC“

Identifizieren

ID.AM-08 Systeme, Hardware, Software, Services und Daten werden während ihres gesamten Lebenszyklus verwaltet

ID.AM-08.2 Patches und Sicherheitsupdates für Betriebssysteme und kritische Systemkomponenten werden installiert.

Schützen

PR.AA-01 Identitäten und Berechtigungsnachweise für autorisierte Benutzer, Dienste und Hardware werden von der Organisation verwaltet

PR.AA-01.1 Identitäten und Anmeldedaten für autorisierte Benutzer, Services und Hardware werden verwaltet.

PR.AA-03 Benutzer, Services und Hardware sind authentifiziert

PR.AA-03.2 Für den Fernzugriff auf die Netzwerke der Organisation ist eine Multi-Faktor-Authentifizierung (MFA) erforderlich.

PR.AA-05 Zugriffsberechtigungen, Berechtigungen und Autorisierungen werden in einer Richtlinie definiert, verwaltet, durchgesetzt und überprüft und berücksichtigen die Prinzipien der geringsten Rechte und der Aufgabentrennung

PR.AA-05.1 Zugriffsberechtigungen, -rechte und -autorisierungen werden definiert, verwaltet, durchgesetzt und überprüft.

PR.AA-05.2 Es wird festgelegt, wer Zugang zu den geschäftskritischen Informationen und Technologien der Organisation benötigt und wie der Zugang gewährt werden kann.

PR.AA-05.3 Zugriffsrechte, Privilegien und Berechtigungen sind auf die Systeme und spezifischen Informationen beschränkt, die für die Erfüllung der Aufgaben erforderlich sind (Grundsatz des geringsten Privilegs).

PR.AA-05.4 Niemand hat Verwaltungsrechte für alltägliche Aufgaben.

PR.DS-11 Backups von Daten werden erstellt, geschützt, gepflegt und getestet

PR.DS-11.1 Backups der geschäftskritischen Daten der Organisation sind auf einem anderen System als dem Gerät, auf dem sich die Originaldaten befinden, durchzuführen und zu speichern.

PR.PS-04 Log-Protokolle werden erstellt und für die kontinuierliche Überwachung zur Verfügung gestellt

PR.PS-04.1 Protokolle werden geführt, dokumentiert und überprüft.

PR.IR-01 Netzwerke und Umgebungen sind vor unbefugtem logischem Zugriff und unbefugter Nutzung geschützt

PR.IR-01.1 In allen von der Organisation genutzten Netzwerken werden Firewalls installiert, konfiguriert und aktiv gewartet, um vor unbefugtem Zugriff und Cyber-Bedrohungen zu schützen.

PR.IR-01.2 Um kritische Systeme zu schützen, implementieren Organisationen Netzwerksegmentierung und -trennung entsprechend den Vertrauensgrenzen und der Kritikalität der Ressourcen, wodurch die Ausbreitung von Bedrohungen begrenzt und eine strenge Zugriffskontrolle durchgesetzt wird.

Erkennen

DE.CM-01 Netzwerke und Netzwerkdienste werden überwacht, um potenziell unerwünschte Ereignisse zu erkennen

DE.CM-01.2 Antiviren-, Anti-Spyware- und andere Anti-Malware-Programme werden installiert und aktualisiert.

DE.AE-03 Informationen aus verschiedenen Quellen werden miteinander in Beziehung gesetzt

DE.AE-03.1 Die Protokollierungsfunktion von Schutz- und Erkennungstools wird aktiviert. Protokolle werden gesichert und für einen vordefinierten Zeitraum aufbewahrt sowie regelmäßig überprüft, um ungewöhnliche oder potenziell schädliche Aktivitäten zu identifizieren.

ANHANG B: LISTE ZUSÄTZLICHER SCHLÜSSEL-MASSNAHMEN FÜR DAS SICHERHEITSNIVEAU „IMPORTANT“

Die nachstehende Liste ergänzt die wichtigsten Maßnahmen für das Sicherheitsniveau „Basic“.

Regeln

GV.RR-02 Rollen, Verantwortlichkeiten und Befugnisse im Zusammenhang mit dem Management von Cybersicherheitsrisiken sind festgelegt, kommuniziert, verstanden und durchgesetzt

GV.RR-02.1 Rollen, Verantwortlichkeiten und Befugnisse im Bereich Informationssicherheit und Cybersicherheit für Mitarbeiter, Lieferanten, Kunden und Partner sind dokumentiert, überprüft, genehmigt, auf dem neuesten Stand gehalten, kommuniziert und intern und extern koordiniert.

Identifizieren

ID.RA-08 Prozesse für den Empfang, die Analyse und die Reaktion auf die Offenlegung von Schwachstellen sind eingerichtet

ID.RA-08.1 Die Organisation erstellt und implementiert einen Schwachstellenmanagementplan, um alle Arten von Schwachstellen zu identifizieren, zu analysieren, zu bewerten, zu mindern und zu kommunizieren, einschließlich in Form einer koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure, CVD) gemäß den geltenden rechtlichen Bestimmungen.

Schützen

PR.AA-03 Benutzer, Services und Hardware sind authentifiziert

PR.AA-03.3 Die Organisation definiert, dokumentiert und implementiert Nutzungsbeschränkungen, Verbindungsanforderungen und Autorisierungsverfahren für den Fernzugriff auf ihre kritischen Systeme. Diese Kontrollen stellen sicher, dass nur zugelassene Benutzer über sichere Methoden eine Verbindung herstellen können und der Zugang auf das für ihre Rolle erforderliche Maß beschränkt ist.

PR.PS-01 Konfigurationsmanagementverfahren sind eingeführt und werden angewendet

PR.PS-01.1 Die Organisation entwickelt, dokumentiert und pflegt eine Basiskonfiguration für ihre geschäftskritischen Systeme.

PR.IR-01 Netzwerke und Umgebungen sind vor unbefugtem logischem Zugriff und unbefugter Nutzung geschützt

PR.IR-01.3 Um die Betriebsstabilität und -sicherheit zu gewährleisten, identifiziert, dokumentiert und kontrolliert die Organisation ausnahmslos alle Verbindungen zwischen den Komponenten ihrer kritischen Systeme.

PR.IR-01.4 Die Organisation implementiert angemessene Maßnahmen zum Schutz der Grenzen, um die Kommunikation an den externen und wichtigen internen Grenzen ihrer kritischen Systeme sowohl in IT- als auch in OT-Umgebungen zu überwachen und zu kontrollieren und so einen sicheren und zuverlässigen Betrieb zu gewährleisten.

Erkennen

DE.CM-01 Netzwerke und Netzwerkdienste werden überwacht, um potenziell unerwünschte Ereignisse zu erkennen

DE.CM-01.3 Die Organisation überwacht und identifiziert die unbefugte Nutzung ihrer geschäftskritischen Systeme durch die Erkennung unbefugter lokaler Verbindungen, Netzwerkverbindungen und Fernverbindungen.

Reagieren

RS.CO-02 Interne und externe Stakeholder werden über Vorfälle informiert

RS.CO-02.2 Cybersecurity-Vorfälle werden innerhalb der im Plan zur Reaktion auf Vorfälle festgelegten Fristen an die relevanten externen Beteiligten weitergegeben, einschließlich der gesetzlich vorgeschriebenen Meldung wichtiger Vorfälle an die Behörden.

RS.MI-01 Vorfälle werden eingedämmt

RS.MI-01.2 Die Organisation erkennt unbefugten Zugriff oder Datenlecks und ergreift geeignete Abhilfemaßnahmen, einschließlich der Überwachung kritischer Systeme an externen Grenzen und wichtigen internen Punkten.

ANHANG C: LISTE ZUSÄTZLICHER SCHLÜSSEL-MASSNAHMEN FÜR DAS SICHERHEITSNIVEAU „ESSENTIAL“

Die nachstehende Liste ergänzt die wichtigsten Maßnahmen für die Sicherheitsstufen „Basic“ und „Important“.

Regeln

GV.SC-05 Anforderungen zur Bewältigung von Cybersicherheitsrisiken in Lieferketten werden festgelegt, priorisiert und in Verträge und andere Arten von Vereinbarungen mit Lieferanten und anderen relevanten Drittparteien integriert

GV.SC-05.2 Vertragliche Informationen/Cybersicherheitsanforderungen für Lieferanten und externe Partner werden implementiert, um einen überprüfbaren Fehlerbehebungsprozess zu gewährleisten und sicherzustellen, dass Mängel, die bei Informations-/Cybersicherheitstests und -bewertungen festgestellt wurden, behoben werden.

GV.SC-05.3 Die Organisation legt vertragliche Anforderungen fest, die es ihr ermöglichen, die von Lieferanten und Drittpartnern implementierten Informations-/Cybersicherheitsprogramme zu überprüfen.

Identifizieren

ID.AM-03 Darstellungen der autorisierten Netzwerkkommunikation der Organisation sowie der internen und externen Netzwerkdatenflüsse werden gepflegt

ID.AM-03-3 Die Netzwerkkommunikation und die externen Datenflüsse der Organisation werden abgebildet, dokumentiert, genehmigt und bei Änderungen aktualisiert.

ID.AM-08 Systeme, Hardware, Software, Services und Daten werden während ihres gesamten Lebenszyklus verwaltet

ID.AM-08.7 Die Organisation soll die nicht autorisierte Entfernung von Wartungsgeräten, die kritische Systeminformationen der Organisation enthalten, verhindern.

ID.AM-08.9 Wartungstools und tragbare Speichergeräte werden bei ihrer Einbringung in die Einrichtung überprüft und durch Anti-Malware-Lösungen geschützt, die sie vor ihrer Verwendung in den Systemen der Organisation auf schädlichen Code scannen.

ID.AM-08.10 Die Organisation verifiziert die Sicherheitskontrollen nach Wartungs- oder Reparaturarbeiten/Patches und ergreift gegebenenfalls entsprechende Maßnahmen.

Schützen

PR.DS-02 Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bei der Übermittlung sind geschützt

PR.DS-02.1 Mobile Speichermedien, die Systemdaten enthalten, werden während des Transports und der Lagerung kontrolliert und geschützt.

ANHANG D: LISTE DER KONTROLLEN IN BEZUG AUF MANAGEMENTASPEKTE FÜR DAS SICHERHEITSNIVEAU ‘IMPORTANT’

Regeln

GV.RM-01 Die Risikomanagementziele sind festgelegt und von den Stakeholdern der Organisation gebilligt

GV.RM-01.1 Es werden Ziele für die Informationssicherheit/Cybersicherheit festgelegt, die von den Stakeholdern der Organisation vereinbart und von der Geschäftsleitung genehmigt werden

GV.RM 02 Erklärungen zur Risikobereitschaft und Risikotoleranz werden erstellt, kommuniziert und aufrechterhalten

GV.RM-02.1 Erklärungen zur Risikobereitschaft und Risikotoleranz werden definiert, dokumentiert, von der Geschäftsleitung genehmigt, kommuniziert und aufrechterhalten.

GV.RM 03 Aktivitäten und Ergebnisse des Managements von Cybersicherheitsrisiken sind in die Risikomanagementprozesse des Unternehmens integriert

GV.RM-03.2 Informations- und Cybersicherheitsrisiken werden im Rahmen der Risikomanagementprozesse des Unternehmens dokumentiert, von der Geschäftsleitung formell genehmigt und bei Änderungen aktualisiert.

GV.RR-02 Rollen, Verantwortlichkeiten und Befugnisse im Zusammenhang mit dem Management von Cybersicherheitsrisiken sind festgelegt, kommuniziert, verstanden und durchgesetzt.

GV.RR-02.1 Rollen, Verantwortlichkeiten und Befugnisse im Bereich Informationssicherheit und Cybersicherheit für Mitarbeiter, Lieferanten, Kunden und Partner werden dokumentiert, überprüft, genehmigt, auf dem neuesten Stand gehalten, kommuniziert und intern und extern koordiniert.

Identifizieren

ID.RA-05 Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen werden genutzt, um das inhärente Risiko zu verstehen und eine Priorisierung der Risikobewältigung vorzunehmen

ID.RA-05.2 Die Organisation führt Risikobewertungen durch und dokumentiert diese, wobei das Risiko anhand von Bedrohungen, Schwachstellen, Auswirkungen auf Geschäftsprozesse und Vermögenswerte sowie der Wahrscheinlichkeit ihres Eintretens bestimmt wird.

ID.RA-06 Risikobewältigungsmaßnahmen werden ausgewählt, nach Prioritäten geordnet, geplant, nachverfolgt und kommuniziert

ID.RA-06.1 Risikobewältigungsmaßnahmen werden ausgewählt, nach Prioritäten geordnet, geplant, nachverfolgt und kommuniziert

ID.IM-04 Pläne zur Reaktion auf Vorfälle und andere Cybersicherheitspläne, die sich auf den Betrieb auswirken, werden erstellt, kommuniziert, gepflegt und verbessert

ID.IM-04.1 Notfall- und Kontinuitätspläne werden erstellt, kommuniziert, gepflegt, getestet, validiert und verbessert.

Schützen

PR.IR-04 Eine angemessene Ressourcenkapazität zur Gewährleistung der Verfügbarkeit wird aufrechterhalten.

PR.IR-04.1 Eine angemessene Planung der Ressourcenkapazitäten stellt sicher, dass die Verfügbarkeit der kritischen Systeminformationen der Organisation in den Bereichen Informationsverarbeitung, Netzwerke, Telekommunikation und Datenspeicherung aufrechterhalten bleibt.

Wiederherstellen

RC.CO-03 Die Wiederherstellungsmaßnahmen und die Fortschritte bei der Wiederherstellung der Betriebsfähigkeit werden den benannten internen und externen Stakeholdern mitgeteilt

RC.CO-03.1 Wiederherstellungsmaßnahmen und Fortschritte bei der Wiederherstellung der Betriebsfähigkeit werden gemäß den festgelegten Kommunikationsverfahren an bestimmte interne und externe Stakeholder kommuniziert.

ANHANG E: LISTE DER KONTROLLEN IN BEZUG AUF MANAGEMENTASPEKTE FÜR DAS SICHERHEITSNIVEAU ‘ESSENTIAL’

Regeln

GV.RR-02 Rollen, Verantwortlichkeiten und Befugnisse im Zusammenhang mit dem Management von Cybersicherheitsrisiken sind festgelegt, kommuniziert, verstanden und durchgesetzt

GV.RR-02.2 Die Organisation ernennt einen leitenden Informationssicherheitsbeauftragten.

GV.SC-01 Ein Programm zum Cybersicherheitsrisikomanagement in der Lieferkette, eine diesbezügliche Strategie, Ziele, Richtlinien und Prozesse sind etabliert und von den organisatorischen Stakeholdern akzeptiert

GV.SC-01.1 Ein Programm zum Cybersicherheitsrisikomanagement in der Lieferkette, eine diesbezügliche Strategie, Ziele, Richtlinien und Prozesse werden dokumentiert, überprüft, bei Veränderungen aktualisiert und von den organisatorischen Stakeholdern akzeptiert.

Identifizieren

ID.RA-05 Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen werden genutzt, um das inhärente Risiko zu verstehen und eine Priorisierung der Risikobewältigung vorzunehmen

ID.RA-05.3 Die Ergebnisse der Risikobewertung werden an die relevanten Stakeholder weitergegeben.

ID.IM-03 Bei der Durchführung von betrieblichen Prozessen, Verfahren und Aktivitäten werden Verbesserungen festgestellt

ID.IM-03.9 Die Organisation führt spezialisierte Bewertungen durch, einschließlich eingehender Überwachung, Schwachstellen-Scans, Tests auf böswillige Benutzer, Bewertung von Insider-Bedrohungen, Leistungs-/Lasttests sowie Verifikations- und Validierungstests für die kritischen Systeme der Organisation.

ID.IM-04 Pläne zur Reaktion auf Vorfälle und andere Cybersicherheitspläne, die sich auf den Betrieb auswirken, werden erstellt, kommuniziert, gepflegt und verbessert.

ID.IM-04.2 Die Organisation koordiniert die Entwicklung und das Testen von Plänen zur Reaktion auf Vorfälle und anderen Cybersicherheitsplänen, die sich auf den Betrieb auswirken, mit den Stakeholdern, um sicherzustellen, dass diese Pläne mit den allgemeinen Organisationszielen übereinstimmen und die Widerstandsfähigkeit verbessern.

Erkennen

DE.AE-04 Die geschätzten Auswirkungen und das Ausmaß von unerwünschten Ereignissen sind bekannt

DE.AE-04.1 Die Organisation bewertet die negativen Auswirkungen festgestellter Ereignisse auf ihre Betriebsabläufe, Vermögenswerte und Personen und setzt diese Auswirkungen in Beziehung zu den Ergebnissen ihrer Risikobewertungen.

Haftungsausschluss

Dieses Dokument und seine Anhänge wurden vom Zentrum für Cybersicherheit Belgien (CCB) erstellt, einer föderalen Behörde, die durch königlichen Erlass vom 10. Oktober 2014 gegründet wurde und dem Premierminister untersteht.

Dieses Dokument enthält technische Informationen in englischer Sprache. Die Informationen zur Sicherheit von Netzwerken und Informationssystemen richten sich an IT-Dienstleister, die englische Computerterminologie verwenden.

Das CCB übernimmt **keine Haftung für den Inhalt** dieses Dokuments.
Die bereitgestellten Informationen:

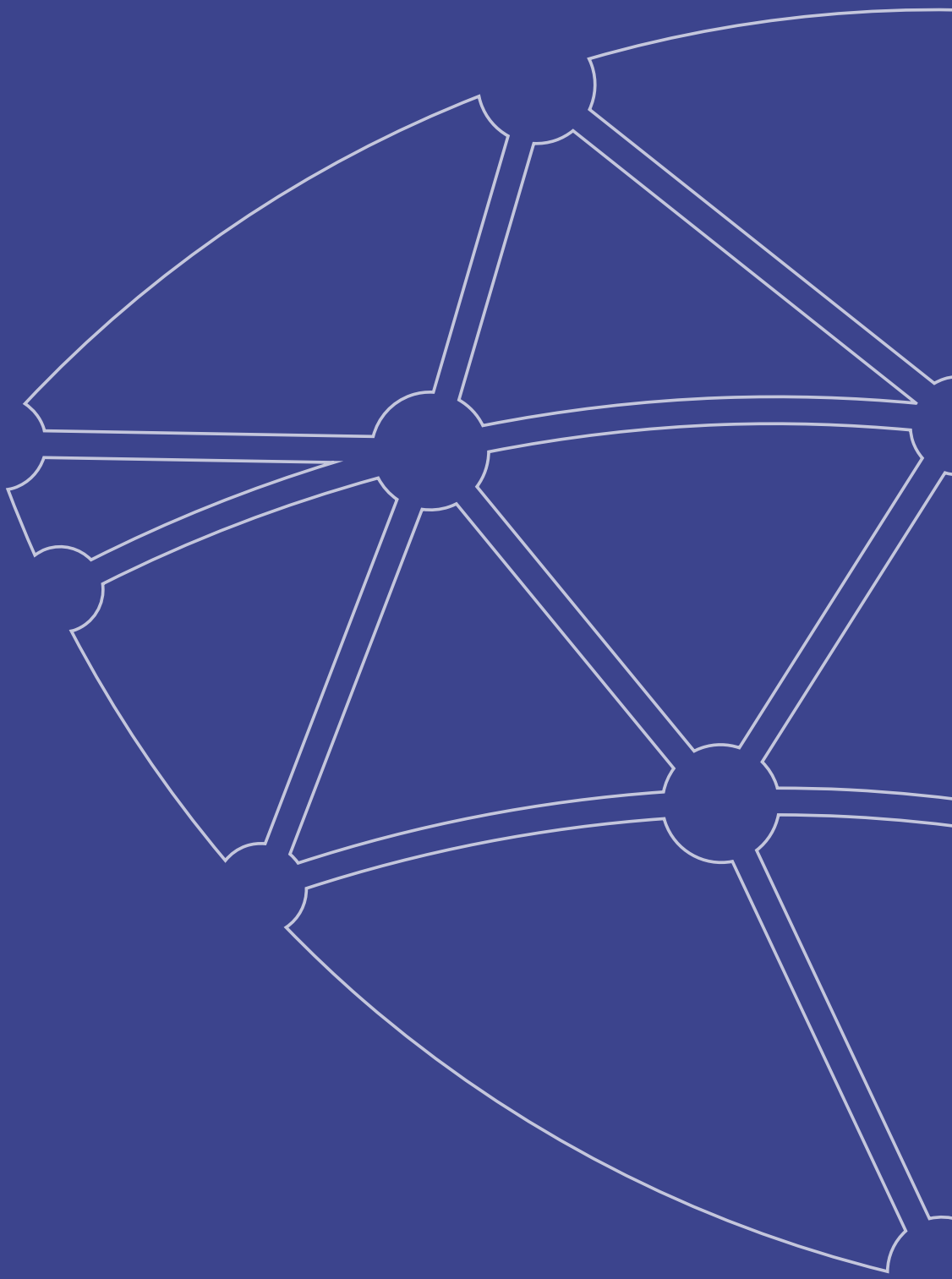
- sind allgemeiner Natur und decken nicht alle spezifischen Situationen ab.
- sind nicht notwendigerweise vollständig, präzise oder in jeder Hinsicht aktuell."

Verantwortlicher Herausgeber

Zentrum für Cybersicherheit Belgien
M. De Bruycker, Generaldirektor
Wetstraat 18
1000 Brüssel

Juristisches Depot

D/2025/14828/010



Zentrum für Cybersicherheit Belgien

Wetstraat 18

1000 Brüssel