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.

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.

- **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.

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 Grundlage gängiger Arten von Cyberangriffen werden bestimmte Anforderungen als „**Schlüsselmaßnahmen**“ festgelegt. Diese müssen auf dieser Sicherheitsebene umgesetzt 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-03 Gesetzliche, behördliche und vertragliche Anforderungen an die Cybersicherheit werden verstanden und gemanagt

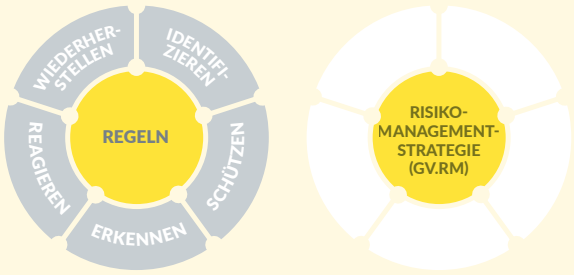
GV.OC-03.1 Gesetzliche und behördliche Anforderungen an die Informations- und Cybersicherheit werden ermittelt und umgesetzt.

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



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

GV.RM-03 Aktivitäten und Ergebnisse des Managements von Cybersicherheits-risiken 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.

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

GV.RR-04 Cybersicherheit ist Bestandteil der Personalpraxis

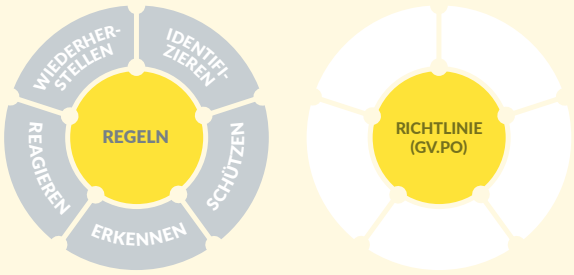
GV.RR-04.1 Mitarbeiter mit Zugang zu den kritischsten Informationen oder Technologien der Organisation werden authentifiziert.

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.



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

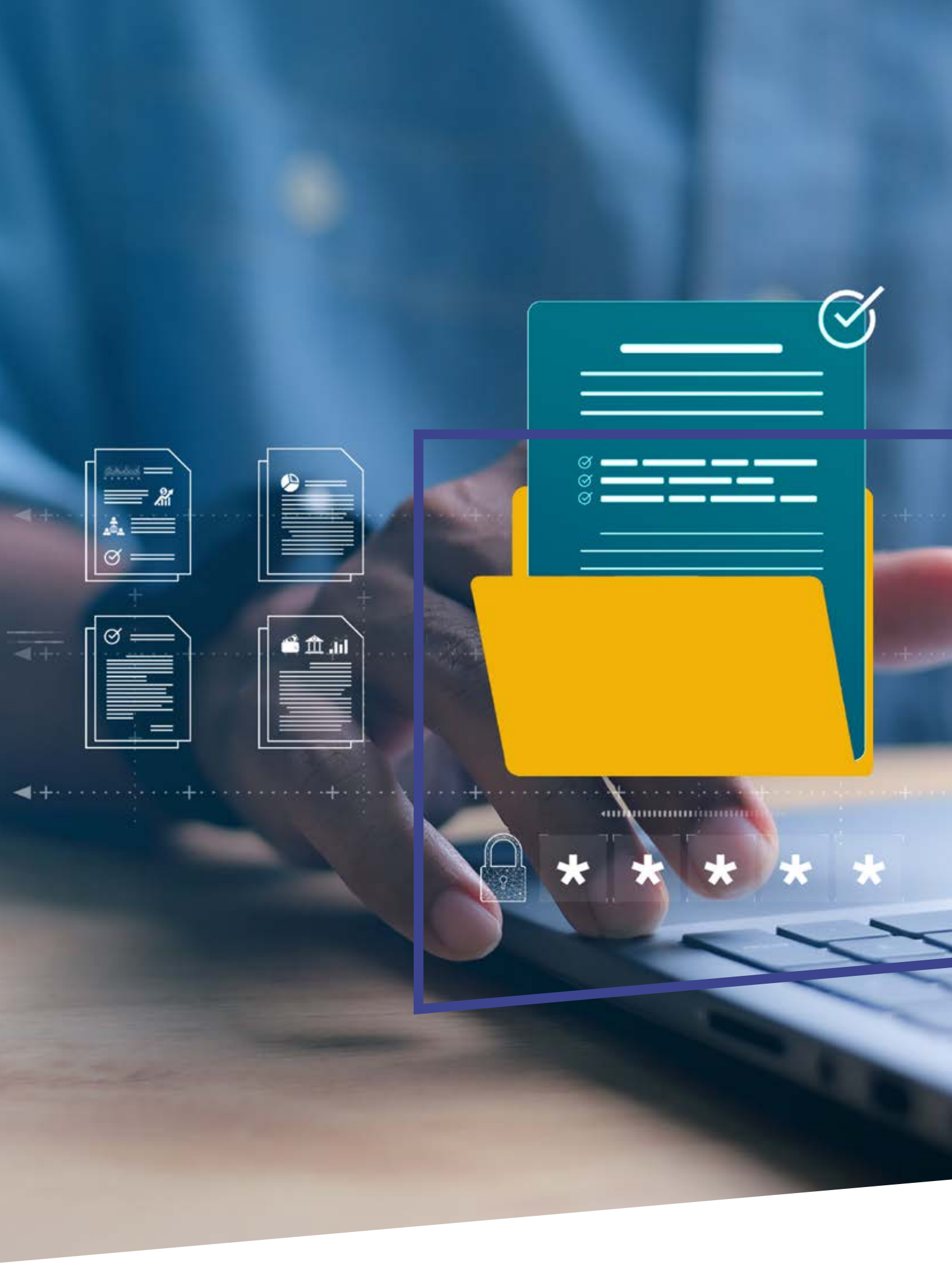
GV.PO-01.1 **Richtlinien und Verfahren für die Verwaltung von Informationen und Cybersicherheit werden erstellt, dokumentiert, überprüft, genehmigt, bei Änderungen aktualisiert, kommuniziert und durchgesetzt.**

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.

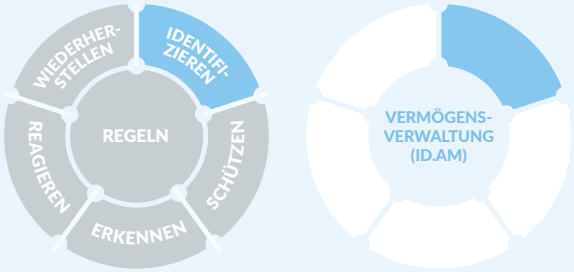
Um diese Kontrolle effektiv zu implementieren, sollten Sie die folgenden Praktiken beachten:

- 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.



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

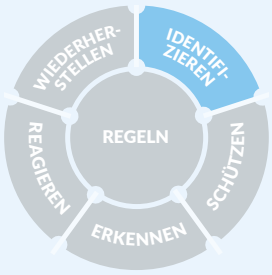
ID.AM-08.2 Patches und Sicherheitsupdates für Betriebssysteme und kritische Systemkomponenten werden installiert.

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.



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

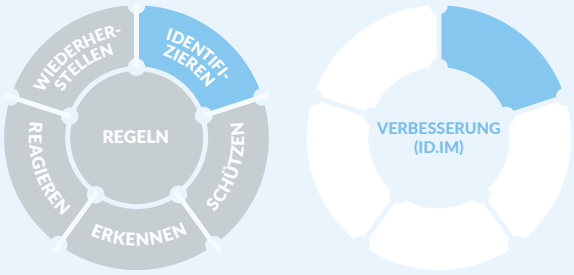
ID.RA-05.1 Die Organisation führt Risikobewertungen durch, bei denen das Risiko durch Bedrohungen, Schwachstellen und die Auswirkungen auf Geschäftsprozesse und Vermögenswerte bestimmt wird.

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.



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

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.

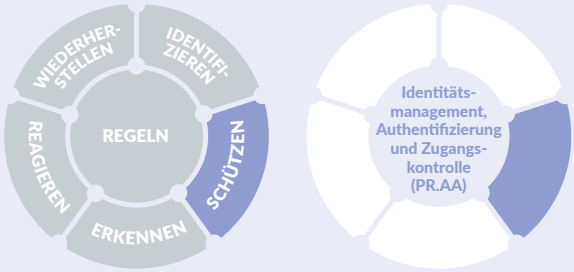
Um dieses Ziel zu erreichen, sollten folgende Punkte berücksichtigt werden:

- **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.


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

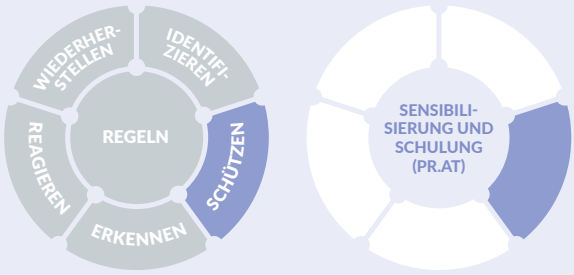
PR.AA-06.1 Der physische Zugang zu allen Einrichtungen der Organisation, einschließlich kritischer Bereiche, soll risikobasiert verwaltet, überwacht und durchgesetzt.

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.



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

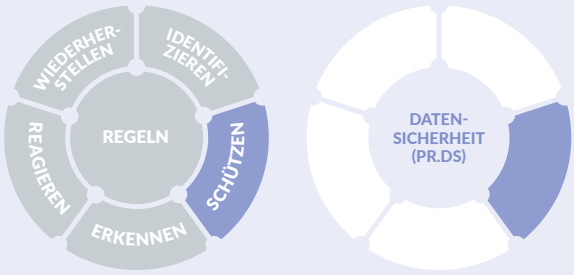
PR.AT-01.1 Die Organisation führt ein Programm zur Sensibilisierung und Schulung im Bereich Cybersicherheit ein und hält dieses aufrecht, um sicherzustellen, dass alle Mitarbeiter verstehen, wie sie ihre Aufgaben sicher und verantwortungsbewusst ausführen können.

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.



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-01.9 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-11 Backups von Daten werden erstellt, geschützt, gepflegt und getestet

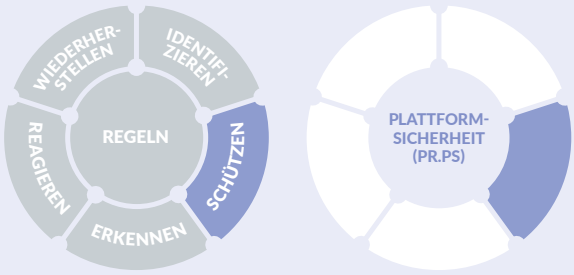
PR.DS-11.1 **Backups der geschäftskritischen Daten der Organisation werden auf einem anderen System durchgeführt und gespeichert als auf dem Gerät, auf dem sich die Originaldaten befinden.**

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.



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-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-05 Installation und Ausführung nicht autorisierter Software wird verhindert

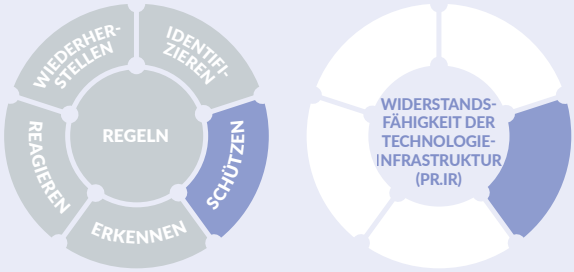
PR.PS-05.1 Web- und E-Mail-Filter werden installiert und verwendet.

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.



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.

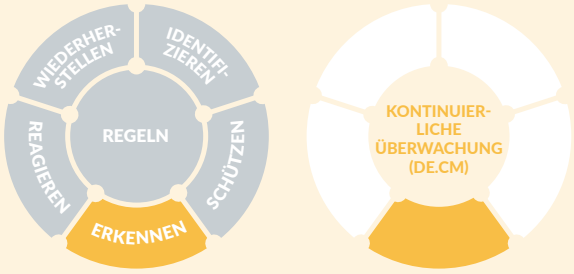
Um diese Kontrolle zu implementieren, sollten folgende Punkte berücksichtigt werden:

- **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.


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

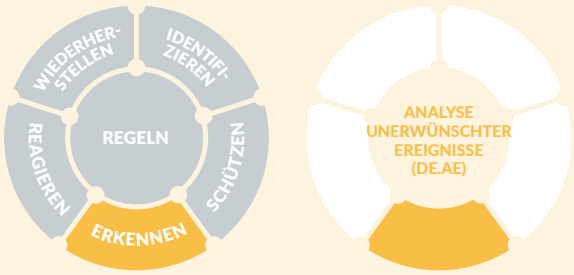
DE.CM-03-1 Es werden Endpunkt- und Netzschutzinstrumente zur Überwachung des Endnutzerverhaltens auf gefährliche Aktivitäten implementiert.

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.



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

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

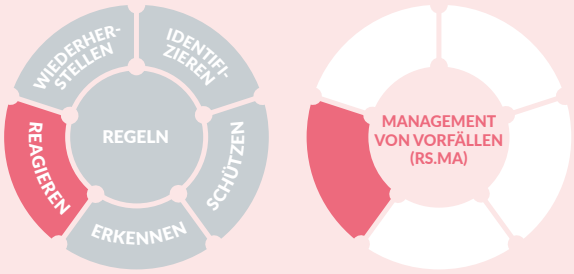
Ziel dieser Kontrolle ist es, sicherzustellen, dass die Sicherheitstools die Protokollierung aktiviert haben, die Protokolle für eine bestimmte Zeit aufbewahrt werden und regelmäßig auf ungewöhnliche oder schädliche Aktivitäten überprüft werden. Dies hilft dabei, Bedrohungen frühzeitig zu erkennen und 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.

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.

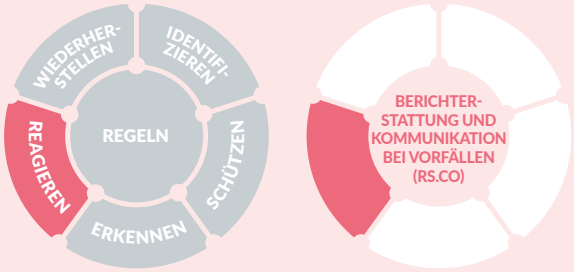
RS.MA-01.1 Während oder nach einem Cybersicherheitsvorfall, der die kritischen Systeme der Organisation betrifft, wird ein Plan zur Reaktion auf Vorfälle umgesetzt, der definierte Rollen, Verantwortlichkeiten und Befugnisse umfasst.

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.



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

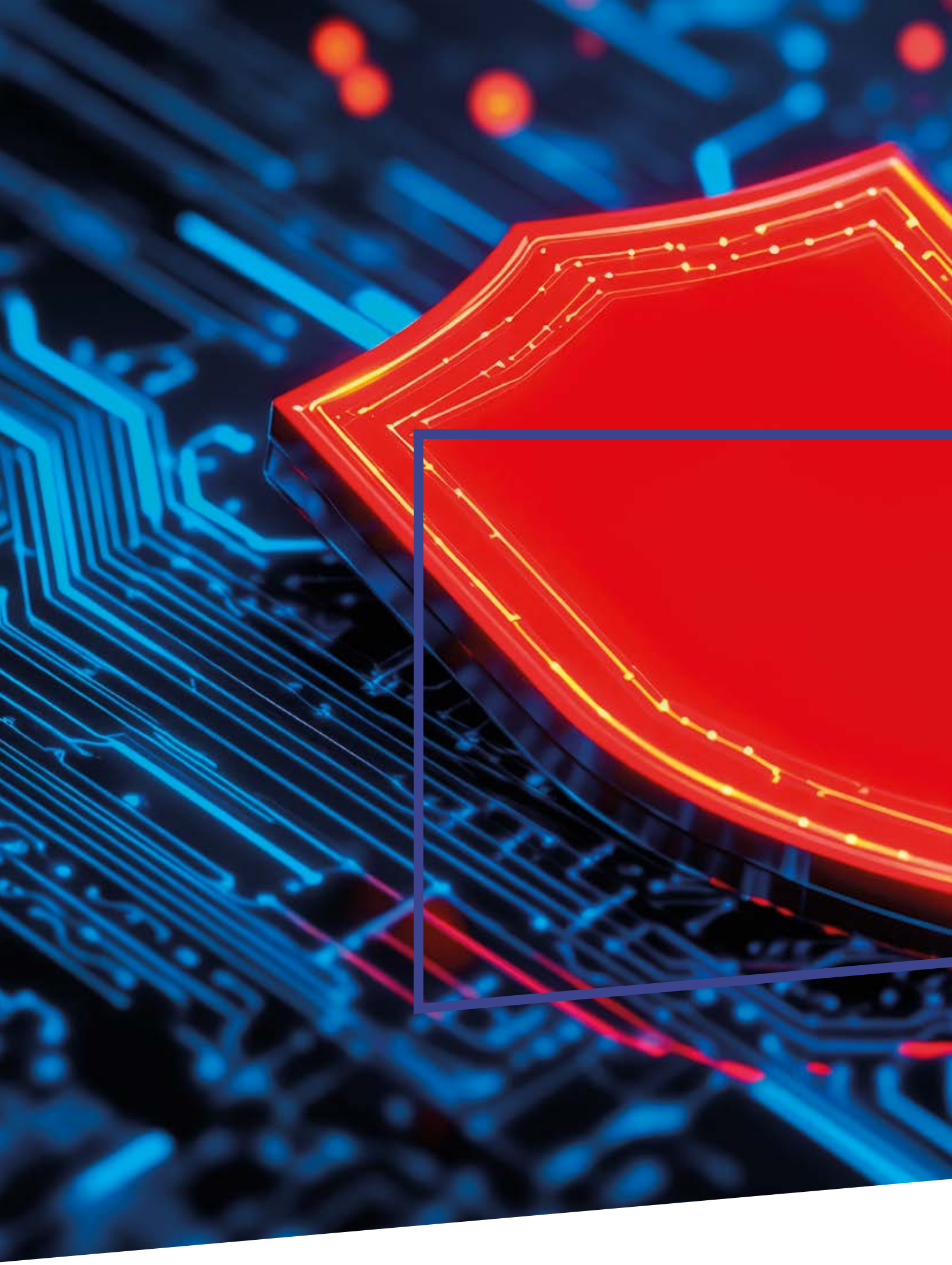
RS.CO-02.1 Informationen über Vorfälle im Bereich der Cybersicherheit werden den Mitarbeitern in einer klaren und leicht verständlichen Weise mitgeteilt.

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.

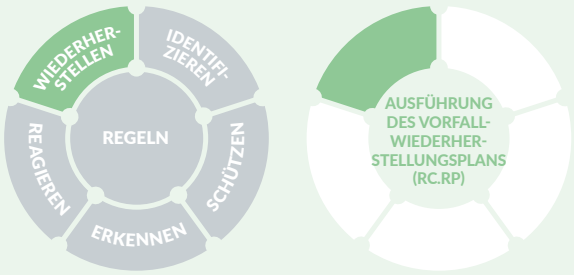
Um dies zu erreichen:

- 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.



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.

ANHANG

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.

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.

Alle Texte, Layouts, Designs und sonstigen Elemente dieses Dokuments sind **urheberrechtlich** geschützt. Die Vervielfältigung von Auszügen aus diesem Dokument ist nur für nichtkommerzielle Zwecke und unter Angabe der Quelle gestattet.

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:

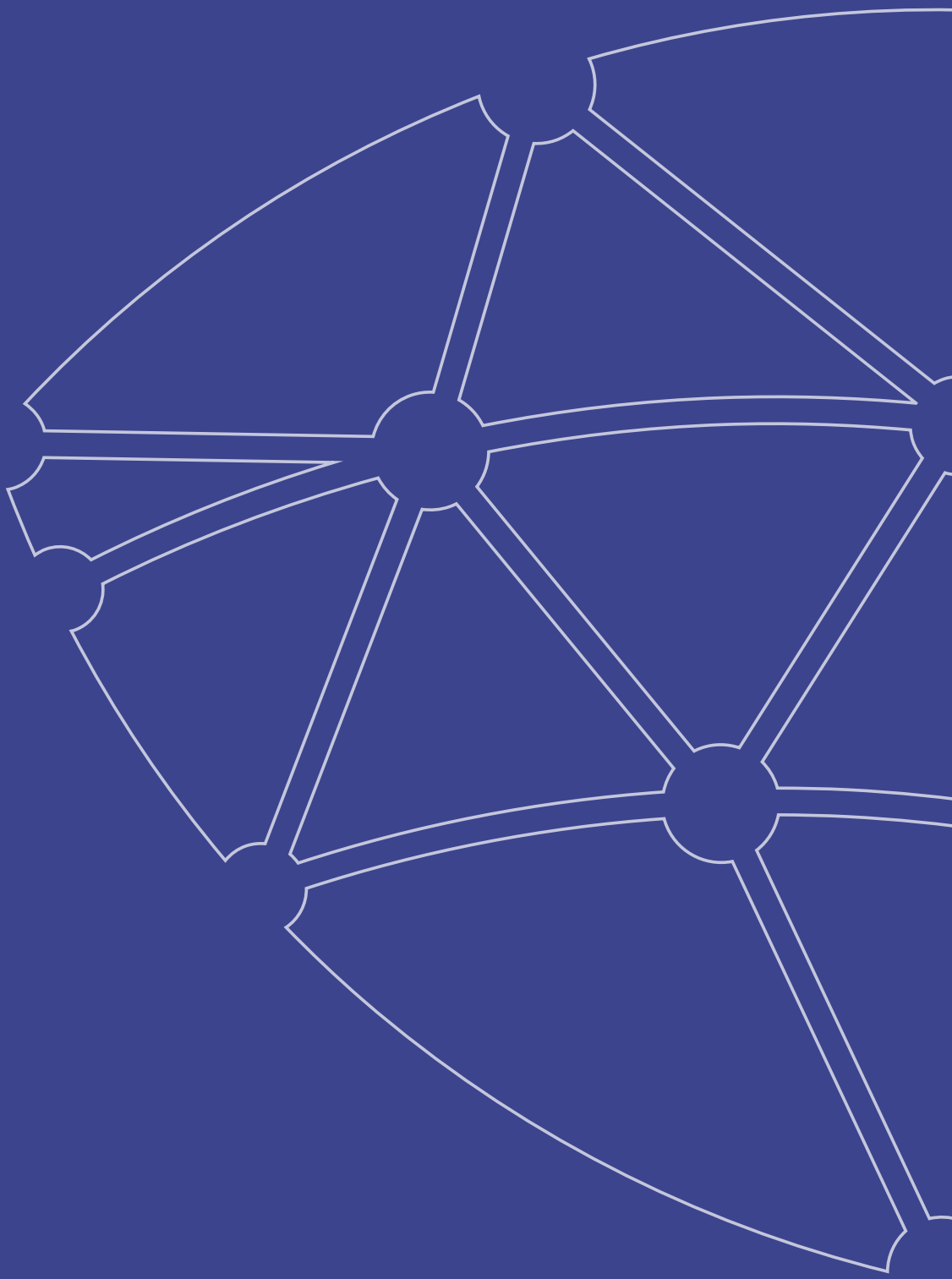
- sind allgemeiner Natur und decken nicht alle spezifischen Situationen ab.
- sind nicht notwendigerweise vollständig, präzise oder in jeder Hinsicht aktuell."

Verantwortlicher Herausgeber

Zentrum für Cybersicherheit Belgien
M. De Bruycker, Generaldirektor
Wetstraat 18
1000 Brüssel

Juristisches Depot

D/2025/14828/008



Zentrum für Cybersicherheit Belgien

Wetstraat 18

1000 Brüssel