CyFun®

TLP:GREEN

The CyberFundamentals Framework 2025
CyFun® 2025 Kernmaatregelen

Een initiatief van het Centrum voor Cybersecurity België

Belgian Cybersecurity Certification Authority

Kernmaatregelen CyFun®

		CyFun® 2023	CyFun® 2025
Totaal aantal Kernmaatregelen	BASIC	13	13
Totaal aantal Kernmaatregelen	IMPORTANT	8	9
Totaal aantal Kernmaatregelen	ESSENTIAL	7	7
Totaal aantal Kernmaatregelen		**28**	**29**

Kernmaatregelen CyFun® Basic

	CyFun® 2023		CyFun® 2025
PR.AC-1.1	Identiteiten en referenties voor geautoriseerde apparaten en gebruikers moeten worden beheerd.	**PR.AA-01.1**	Identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware moeten worden beheerd.
PR.AC-3.2	De netwerken van de organisatie die op afstand toegankelijk zijn, moeten worden beveiligd, onder meer door middel van multifactorauthenticatie (MFA).	**PR.AA-03.2**	Multifactorauthenticatie (MFA) is vereist om op afstand toegang te krijgen tot de netwerken van de organisatie.
PR.AC-4.1	De toegangsrechten voor gebruikers tot de systemen van de organisatie moeten worden gedefinieerd en beheerd.	**PR.AA-05.1**	Toegangsrechten, machtigingen en autorisaties moeten worden vastgesteld, beheerd, gehandhaafd en periodiek herzien.
PR.AC-4.2	Er moet worden vastgesteld wie toegang moet hebben tot de bedrijfskritische informatie en technologie van de organisatie, en de middelen om die toegang te krijgen.	**PR.AA-05.2**	Er moet worden vastgesteld wie toegang nodig heeft tot de bedrijfskritische informatie en technologie van de organisatie, evenals op welke manier die toegang wordt verleend.
PR.AC-4.3	De toegang van werknemers tot gegevens en informatie moet worden beperkt tot de systemen en specifieke informatie die zij nodig hebben om hun werk te doen (het beginsel van “least privilege”).	**PR.AA-05.3**	Toegangsrechten, privileges en autorisaties moeten worden beperkt tot de systemen en specifieke informatie die nodig zijn om de taken uit te voeren (het principe van ‘Least Privilege’).
PR.AC-4.4	Niemand heeft beheerdersrechten voor dagelijkse taken.	**PR.AA-05.4**	Niemand mag beheerdersrechten hebben voor dagelijkse routinetaken.
PR.AC-5.1	Op alle netwerken van de organisatie moeten firewalls worden geïnstalleerd en geactiveerd.	**PR.IR-01.1**	Firewalls moeten worden geïnstalleerd, geconfigureerd en actief onderhouden op alle netwerken die door de organisatie worden gebruikt om bescherming te bieden tegen ongeoorloofde toegang en cyberdreigingen.
PR.AC-5.2	Waar nodig moet de netwerkintegriteit van de kritieke systemen van de organisatie worden beschermd door netwerksegmentatie en -scheiding.	**PR.IR-01.2**	Om kritieke systemen te beschermen, moeten organisaties netwerksegmentatie en -scheiding toepassen, afgestemd op zones met verschillend vertrouwensniveau en de kriticiteit van systemen, zodat dreigingen zich niet kunnen verspreiden en strikte toegangscontrole wordt afgedwongen.
PR.IP-4.1	Back-ups voor bedrijfskritische gegevens van de organisatie moeten worden uitgevoerd en opgeslagen op een ander systeem dan het apparaat waarop de oorspronkelijke gegevens zich bevinden.	**PR.DS-11.1**	Back-ups van de bedrijfskritieke gegevens van de organisatie moeten worden gemaakt en opgeslagen op een ander systeem dan het apparaat waarop de originele gegevens zich bevinden.
PR.MA-1.1	Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.	**ID.AM-08.2**	Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.
PR.PT-1.1	Logs worden bijgehouden, gedocumenteerd en geëvalueerd. Richtlijnen	**PR.PS-04.1**	Logbestanden moeten worden bijgehouden, gedocumenteerd en bewaakt.
DE.AE-3.1	De functionaliteit voor activiteitenregistratie (“activity logging”) van beschermings-/detectieapparatuur of -software (bv. firewalls, antivirus) moet worden ingeschakeld, er moet een back-up van worden gemaakt en deze moet worden nagezien.	**DE.AE-03.1**	De logfunctionaliteit van beschermings- en detectietools moet worden ingeschakeld. Logbestanden moeten worden geback-upt, gedurende een vooraf bepaalde periode bewaard en regelmatig gecontroleerd om ongebruikelijke of mogelijk schadelijke activiteiten te identificeren.
DE.CM-4.1	Anti-virus, -spyware, and other -malware programs shall be installed and updated.	**DE.CM-01.2**	Anti-virus, -spyware- en andere anti-malwareprogramma's moeten worden geïnstalleerd en bijgewerkt.

	CyFun® 2023	CyFun® 2025	Wijzigingen
Totaal aantal Kernmaatregelen	**13**	**13**	Geen nieuwe kernmaatregelen, verbetering van de uitvoerbaarheid, herformulering, hernummering

Kernmaatregelen CyFun® Important

	CyFun® 2023		CyFun® 2025
ID.AM-6.1	De rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatie- en cyberbeveiliging binnen de organisatie moeten worden gedocumenteerd, geëvalueerd, geautoriseerd en bijgewerkt en afgestemd op de andere interne rollen van de organisatie en die van externe partners.	**GV.RR-02.1**	De rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging en cyberbeveiliging voor werknemers, leveranciers, klanten en partners moeten worden gedocumenteerd, gecontroleerd, geautoriseerd, bijgewerkt, gecommuniceerd en intern en extern gecoördineerd.
PR.AC-3.3	Gebruiksbeperkingen, verbindingsvereisten, implementatierichtlijnen en autorisaties voor toegang op afstand tot de kritieke systeemomgeving van de organisatie moeten worden vastgesteld, gedocumenteerd en geïmplementeerd.	**PR.AA-03.3**	De organisatie moet gebruiksbeperkingen, verbindingsvereisten en autorisatieprocedures voor externe toegang tot haar kritieke systemen definiëren, documenteren en implementeren. Deze controles moeten ervoor zorgen dat alleen goedgekeurde gebruikers verbinding kunnen maken met behulp van veilige methoden, waarbij de toegang beperkt blijft tot wat nodig is voor hun functie.
PR.AC-5.3	Waar nodig moet de netwerkintegriteit van de kritieke systemen van de organisatie worden beschermd door (1) het identificeren, documenteren en controleren van verbindingen tussen systeemcomponenten en (2) het beperken van externe verbindingen met de kritieke systemen van de organisatie.	**PR.IR-01.3**	Om de operationele stabiliteit en veiligheid te waarborgen, moet de organisatie zonder uitzondering de verbindingen tussen de componenten van haar kritieke systemen identificeren, documenteren en controleren.
PR.AC-5.4	De organisatie moet verbindingen en communicatie aan de buitengrenzen en aan belangrijke interne grenzen binnen de kritieke systemen van de organisatie bewaken en controleren door waar nodig grensbeschermingsvoorzieningen te implementeren.	**PR.IR-01.4**	De organisatie moet passende grensbeveiligingsmaatregelen implementeren om de communicatie aan externe en belangrijke interne grenzen van haar kritieke systemen, zowel in IT- als OT-omgevingen, te monitoren en te controleren, om een veilige en betrouwbare werking te garanderen.
PR.IP-1.1	De organisatie moet voor haar bedrijfskritische systemen een basisconfiguratie ontwikkelen, documenteren en bijhouden.	**PR.PS-01.1**	De organisatie moet een basisconfiguratie voor haar bedrijfskritieke systemen ontwikkelen, documenteren en onderhouden.
PR.DS-5.1	De organisatie neemt passende maatregelen die leiden tot de bewaking van haar kritische systemen aan de buitengrenzen en kritische interne punten wanneer ongeoorloofde toegang en activiteiten, met inbegrip van het lekken van gegevens, worden ontdekt.	**RS.MI-01.2**	De organisatie moet ongeoorloofde toegang of gegevenslekken detecteren en passende maatregelen nemen om de schade te beperken, waaronder het monitoren van kritieke systemen aan de externe grenzen en op belangrijke interne punten.
DE.CM-1.2	De organisatie moet ongeoorloofd gebruik van haar bedrijfskritische systemen bewaken en vaststellen door het opsporen van ongeoorloofde lokale verbindingen, netwerkverbindingen en verbindingen op afstand.	**DE.CM-01.3**	De organisatie moet ongeoorloofd gebruik van haar bedrijfskritieke systemen monitoren en identificeren door het opsporen van ongeoorloofde lokale verbindingen, netwerkverbindingen en externe verbindingen.
RS.AN-5.1	De organisatie moet processen en procedures voor het beheer van kwetsbaarheden toepassen die het verwerken, analyseren en verhelpen van kwetsbaarheden uit interne en externe bronnen omvatten.	**ID.RA-08.1**	De organisatie moet een kwetsbaarheidsbeheerplan opstellen en implementeren om alle soorten kwetsbaarheden te identificeren, analyseren, beoordelen, beperken en communiceren, onder meer in de vorm van een gecoördineerde kwetsbaarheidsmelding (CVD) volgens de toepasselijke wettelijke modaliteiten.
		RS.CO-02.2	Cyberbeveiligingsincidenten worden binnen de in het incidentresponsplan vastgestelde termijnen gedeeld met relevante externe belanghebbenden, met inbegrip van het melden van belangrijke incidenten aan de autoriteiten, zoals wettelijk vereist.

	CyFun® 2023	CyFun® 2025	Wijzigingen
Totaal aantal Kernmaatregelen	8	9	Verbetering van de uitvoerbaarheid, herformulering, hernummering 1 nieuwe kernmaatregel: RS.CO-02.2 → Ref. NIS2 voor belangrijke en essentiële entiteiten

Key Measures CyFun® Essential

	CyFun® 2023		CyFun® 2025
ID.SC-3.2	Er moeten contractuele vereisten inzake informatie- en cyberbeveiliging voor leveranciers en externe partners worden geïmplementeerd, om te zorgen dat er een controleerbaar proces is voor het verhelpen van gebreken, en om te waarborgen dat gebreken worden verholpen die worden vastgesteld tijdens informatie- en cyberbeveiligingstesten en evaluaties.	GV.SC-05.2	Contractuele informatie-/cyberbeveiligingseisen voor leveranciers en externe partners moeten worden geïmplementeerd om een verifieerbaar proces voor het oplossen van gebreken te waarborgen en om ervoor te zorgen dat tekortkomingen die tijdens informatie-/cyberbeveiligingstests en -evaluaties worden vastgesteld, worden verholpen.
ID.SC-3.3	De organisatie moet contractuele voorschriften vaststellen die haar in staat stellen de door leveranciers en externe partners geïmplementeerde programma's voor "informatiebeveiliging en cyberveiligheid" te evalueren.	GV.SC-05.3	De organisatie stelt contractuele vereisten vast die de organisatie in staat stellen de door leveranciers en externe partners geïmplementeerde informatie-/cyberbeveiligingsprogramma's te beoordelen.
PR.MA-1.5	De organisatie moet voorkomen dat onderhoudsapparatuur die kritieke systeeminformatie van de organisatie bevat, door onbevoegden wordt verwijderd.	ID.AM-08.7	De organisatie moet voorkomen dat onderhoudsapparatuur met kritieke systeeminformatie van de organisatie zonder toestemming wordt verwijderd.
PR.MA-1.6	Onderhoudsinstrumenten en draagbare opslagapparaten moeten worden geïnspecteerd wanneer zij de faciliteit worden binnengebracht en moeten worden beschermd door anti-malwareoplossingen, zodat zij worden gescand op kwaadaardige code voordat zij op de systemen van de organisatie worden gebruikt.	ID.AM-08.9	Onderhoudsgereedschap en draagbare opslagapparaten moeten worden geïnspecteerd wanneer ze de faciliteit binnenkomen en moeten worden beschermd door antimalwareoplossingen die ze scannen op kwaadaardige code voordat ze op de systemen van de organisatie worden gebruikt.
PR.MA-1.7	De organisatie moet na onderhoud of reparatie/patching van hardware en software de beveiligingscontroles nazien en de nodige maatregelen nemen.	ID.AM-08.10	De organisatie moet de beveiligingsmaatregelen na onderhoud of reparaties/patching controleren en indien nodig maatregelen nemen.
PR.PT-2.3	Draagbare opslagapparatuur die systeemgegevens bevat, moet tijdens transit en wanneer in opslag worden gecontroleerd en beschermd.	PR.DS-02.1	Draagbare opslagapparaten die systeemgegevens bevatten, moeten tijdens het transport en de opslag worden gecontroleerd en beschermd.
DE.AE-1.1	De organisatie moet ervoor zorgen dat een baseline van netwerkoperaties en verwachte gegevensstromen voor haar kritieke systemen wordt vastgesteld, gedocumenteerd en bijgehouden om gebeurtenissen te volgen.	ID.AM-03-3	De netwerkcommunicatie en externe gegevensstromen van de organisatie moeten in kaart worden gebracht, gedocumenteerd, geautoriseerd en bijgewerkt wanneer er wijzigingen optreden.

	CyFun® 2023	CyFun® 2025	Wijzigingen
Totaal aantal Kernmaatregelen	7	7	Geen nieuwe kernmaatregelen, verbetering van de uitvoerbaarheid, herformulering, hernummering

Govern

CyFun®

KERNMAATREGEL

CyberFundamentals IMPORTANT

GV.RR-02.1

De rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging en cyberbeveiliging voor werknemers, leveranciers, klanten en partners moeten worden gedocumenteerd, gecontroleerd, geautoriseerd, bijgewerkt, gecommuniceerd en intern en extern gecoördineerd.

DOEL

Ervoor zorgen dat alle interne en externe partijen hun rollen, verantwoordelijkheden en bevoegdheden op het gebied van cyberbeveiliging begrijpen en nakomen, waardoor hiaten, overlappingen en vertragingen bij incidentrespons en naleving (‘compliance’) worden verminderd.

Govern

CyFun®

KERNMAATREGEL

CyberFundamentals ESSENTIAL

GV.SC-05.2

Contractuele eisen voor informatie- en cyberbeveiliging bij leveranciers en externe partners moeten worden geïmplementeerd om een controleerbaar proces voor het oplossen van kwetsbaarheden te waarborgen en om ervoor te zorgen dat tekortkomingen die tijdens testen en evaluaties worden vastgesteld, worden verholpen.

DOEL

Afdwingbare vereisten opnemen in contracten met leveranciers om te garanderen dat gebreken tijdig worden verholpen en cyberbeveiligingsproblemen die tijdens tests en evaluaties worden vastgesteld, worden opgelost.

Govern

CyFun®

KERNMAATREGEL

CyberFundamentals ESSENTIAL

GV.SC-05.3

De organisatie moet contractuele vereisten vaststellen die de organisatie in staat stellen om de door leveranciers en externe partners geïmplementeerde informatie-/cyberbeveiligingsprogramma's te beoordelen.

DOEL

Ervoor zorgen dat de organisatie de informatie/cyberbeveiligingspraktijken van leveranciers en externe partners kan beoordelen en verifiëren door middel van contractuele overeenkomsten.

Detect

CyFun®

KERNMAATREGEL

CyberFundamentals BASIC

DE.AE-03.1
De logfunctionaliteit van beschermings- en detectietools moet worden ingeschakeld. Logbestanden moeten worden geback-upt, gedurende een vooraf bepaalde periode bewaard en regelmatig gecontroleerd om ongebruikelijke of mogelijk schadelijke activiteiten te identificeren.

DOEL

Ervoor zorgen dat:

- beveiligingstools zijn ingesteld om logbestanden bij te houden,
- logbestanden gedurende een bepaalde tijd worden bewaard,
- logbestanden regelmatig worden gecontroleerd om ongebruikelijke of schadelijke activiteiten op te sporen.

Dit helpt om bedreigingen vroegtijdig te detecteren en maatregelen te nemen.

Voorbeelden van dergelijke tools zijn firewalls, antivirussoftware, eindpuntdetectie en inbraakdetectiesystemen.

Detect CyFun®

KERNMAATREGEL

CyberFundamentals BASIC

DE.CM-01.2
Anti-virus, -spyware- en andere anti-malwareprogramma's moeten worden geïnstalleerd en bijgewerkt.

DOEL

Ervoor zorgen dat alle apparaten van de organisatie (IT- en OT-middelen) worden beschermd tegen kwaadaardige software door antimalwaretools te implementeren en regelmatig bij te werken.

Detect

CyFun®

KERNMAATREGEL

CyberFundamentals IMPORTANT

DE.CM-01.3

De organisatie moet het ongeoorloofd gebruik van haar bedrijfskritieke systemen monitoren en identificeren door het detecteren van ongeautoriseerde lokale, netwerk- en externe verbindingen.

DOEL

Ervoor zorgen dat de organisatie ongeoorloofde toegang tot of misbruik van haar bedrijfskritieke systemen kan detecteren en hierop kan reageren. Dit omvat het identificeren van verdachte lokale, netwerk- of externe verbindingen die kunnen wijzen op een inbreuk op de beveiliging of misbruik van gevoelige systemen.

Identify CyFun®

KERNMAATREGEL

CyberFundamentals BASIC

ID.AM-08.2
Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.

DOEL

Ervoor zorgen dat besturingssystemen en kritieke systeemcomponenten veilig en up-to-date blijven door patches en beveiligingsupdates tijdig en op een gecontroleerde manier te installeren.

Identify CyFun®

KERNMAATREGEL

CyberFundamentals IMPORTANT

ID.RA-08.1

De organisatie moet een kwetsbaarheidsbeheerplan opstellen en implementeren om alle soorten kwetsbaarheden te identificeren, analyseren, beoordelen, mitigeren en communiceren, onder meer in de vorm van een gecoördineerde kwetsbaarheidsmelding (CVD) volgens de toepasselijke wettelijke modaliteiten.

DOEL

Ervoor zorgen dat alle soorten kwetsbaarheden systematisch worden geïdentificeerd, geanalyseerd, beoordeeld, beperkt en gecommuniceerd via een gedocumenteerd kwetsbaarheidsbeheerplan. Dit omvat het afhandelen van meldingen in overeenstemming met de praktijken voor gecoördineerde kwetsbaarheidsmeldingen (CVD) en de toepasselijke wettelijke vereisten.

KERNMAATREGEL

CyberFundamentals ESSENTIAL

ID.AM-03.3
De netwerkcommunicatie en externe gegevensstromen van de organisatie moeten in kaart worden gebracht, gedocumenteerd, geautoriseerd en bijgewerkt wanneer er wijzigingen optreden.

DOEL

Ervoor zorgen dat externe netwerkcommunicatie duidelijk wordt begrepen, gecontroleerd en gemonitord om het risico van ongeoorloofde toegang, gegevenslekken of dienstonderbrekingen in ICT- en OT-omgevingen te verminderen

KERNMAATREGEL

CyberFundamentals ESSENTIAL

ID.AM-08.7

De organisatie moet voorkomen dat onderhoudsapparatuur die kritieke systeeminformatie van de organisatie bevat, zonder toestemming wordt verwijderd.

DOEL

Het voorkomen van ongeoorloofde verwijdering van onderhoudsapparatuur die kritieke systeeminformatie kan bevatten, waardoor het risico op gegevenslekken of -diefstal wordt verminderd, met name in operationele technologie (OT)-omgevingen.

ID.AM-08.9

Onderhoudstools en draagbare opslagapparaten moeten worden geïnspecteerd wanneer ze de faciliteit binnenkomen en moeten worden beschermd door anti-malwareoplossingen die ze scannen op kwaadaardige code voordat ze op de systemen van de organisatie worden gebruikt.

DOEL

Het voorkomen van het binnendringen van kwaadaardige code in de systemen van de organisatie, door ervoor te zorgen dat alle onderhoudstools en draagbare opslagapparaten worden geïnspecteerd en gescand voordat ze worden gebruikt

KERNMAATREGEL

CyberFundamentals ESSENTIAL

ID.AM-08.10
De organisatie moet na onderhoud of reparaties/patches controleren of de beveiligingsmaatregelen correct functioneren en zo nodig passende acties ondernemen.

DOEL

Ervoor zorgen dat beveiligingsmaatregelen effectief blijven na onderhoud, reparaties of patching. In OT-omgevingen kunnen zelfs kleine configuratiewijzigingen aanzienlijke gevolgen hebben voor de veiligheid of de werking, waardoor verificatie na onderhoud van cruciaal belang is.

KERNMAATREGEL

CyberFundamentals BASIC

PR.AA-01.1
Identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware moeten worden beheerd.

DOEL

Ervoor zorgen dat identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware correct worden beheerd om ongeoorloofde toegang te voorkomen en veilige operaties in zowel ICT- als OT-omgevingen te ondersteunen.

PR.AA-03.2
Multifactorauthenticatie (MFA) is vereist om op afstand toegang te krijgen tot de netwerken van de organisatie.

DOEL

De netwerken van de organisatie te beschermen door multifactorauthenticatie (MFA) te vereisen voor alle externe toegang, waardoor het risico op ongeoorloofde toegang en aanvallen op basis van authenticatiemiddelen wordt verminderd.

KERNMAATREGEL

CyberFundamentals BASIC

PR.AA-05.1
Toegangsrechten, machtigingen en autorisaties moeten worden vastgesteld, beheerd, gehandhaafd en periodiek herzien.

DOEL

Ervoor zorgen dat toegangsrechten, machtigingen en autorisaties duidelijk worden vastgelegd, correct beheerd, consequent afgedwongen en regelmatig herzien, zodat systemen en gegevens beschermd blijven tegen ongeoorloofde toegang.

PR.AA-05.2

Er moet worden vastgesteld wie toegang nodig heeft tot de bedrijfskritische informatie en technologie van de organisatie, evenals op welke manier die toegang wordt verleend.

DOEL

Vaststellen wie toegang nodig heeft tot de bedrijfskritische informatie en technologie van de organisatie, en veilige methoden en procedures definiëren waarmee deze toegang wordt verleend.

PR.AA-05.3
Toegangsrechten, privileges en autorisaties moeten worden beperkt tot de systemen en specifieke informatie die nodig zijn om de taken uit te voeren (het principe van ‘least privilege’).

DOEL

Ervoor zorgen dat toegangsrechten, privileges en autorisaties beperkt blijven tot alleen de systemen en specifieke informatie die nodig zijn om de toegewezen taken uit te voeren, volgens het principe van minimale privileges.

PR.AA-05.4
Niemand mag beheerdersrechten hebben voor dagelijkse routinetaken.

DOEL

Het gebruik van beheerdersrechten voor routinematige, dagelijkse taken voorkomen, waardoor het risico op misbruik of exploitatie door aanvallers wordt verminderd.

KERNMAATREGEL

CyberFundamentals BASIC

PR.DS-11.1
Back-ups van de bedrijfskritieke gegevens van de organisatie moeten worden gemaakt en opgeslagen op een ander systeem dan het apparaat waarop de originele gegevens zich bevinden.

DOEL

Ervoor zorgen dat bedrijfskritieke gegevens regelmatig worden geback-upt en veilig worden opgeslagen op een apart systeem om ze te beschermen tegen gegevensverlies, systeemstoringen of cyberaanvallen zoals ransomware.

KERNMAATREGEL

CyberFundamentals BASIC

PR.IR-01.1

Firewalls moeten worden geïnstalleerd, geconfigureerd en actief onderhouden op alle netwerken die door de organisatie worden gebruikt om bescherming te bieden tegen ongeoorloofde toegang en cyberdreigingen.

DOEL

Ervoor zorgen dat alle netwerken die door de organisatie worden gebruikt, worden beschermd tegen ongeoorloofde toegang en cyberdreigingen door middel van de installatie, configuratie en actieve onderhoud van firewalls.

PR.IR-01.2

Om kritieke systemen te beschermen, moeten organisaties netwerksegmentatie en -scheiding toepassen, afgestemd op zones met verschillend vertrouwensniveau en de kriticiteit van systemen, zodat dreigingen zich niet kunnen verspreiden en strikte toegangscontrole wordt afgedwongen.

DOEL

De verspreiding van cyberdreigingen beperken en strikte toegangscontrole afdwingen door netwerksegmentatie en -segregatie te implementeren op basis van vertrouwensgrenzen en de kriticiteit van systemen.

KERNMAATREGEL

CyberFundamentals BASIC

PR.PS-04.1
Logbestanden moeten worden bijgehouden, gedocumenteerd en bewaakt.

DOEL

Ervoor zorgen dat logboeken consistent worden bijgehouden, gedocumenteerd en bewaakt om de zichtbaarheid, verantwoordingsplicht en vroege detectie van afwijkingen of bedreigingen te ondersteunen.

Protect CyFun®

KERNMAATREGEL

CyberFundamentals IMPORTANT

PR.AA-03.3
De organisatie moet gebruiksbeperkingen, verbindingsvereisten en autorisatieprocedures voor externe toegang tot haar kritieke systemen definiëren, documenteren en implementeren. Deze controles moeten ervoor zorgen dat alleen goedgekeurde gebruikers verbinding kunnen maken met behulp van veilige methoden, waarbij de toegang beperkt blijft tot wat nodig is voor hun functie.

DOEL

Ervoor zorgen dat externe toegang tot kritieke systemen streng wordt gecontroleerd door middel van gedefinieerde gebruiksbeperkingen, veilige verbindingsmethoden en formele autorisatieprocedures

KERNMAATREGEL

CyberFundamentals IMPORTANT

PR.IR-01.3

Om de operationele stabiliteit en veiligheid te waarborgen, moet de organisatie zonder uitzondering alle verbindingen tussen onderdelen van haar kritieke systemen identificeren, documenteren en beheersen.

DOEL

Het handhaven van operationele stabiliteit en veiligheid door ervoor te zorgen dat alle verbindingen tussen componenten van kritieke systemen bekend zijn, gedocumenteerd worden en actief worden beheerd.

KERNMAATREGEL

CyberFundamentals IMPORTANT

PR.IR-01.4

De organisatie moet passende maatregelen nemen om communicatie te bewaken en te controleren aan externe en belangrijke interne grenzen van kritieke systemen, inclusief de verbindingen tussen IT- en OT-domeinen, om veilige en betrouwbare werking te garanderen .

DOEL

Veilige en betrouwbare activiteiten garanderen door actief toezicht te houden op en controle uit te oefenen op de communicatie aan belangrijke netwerkgrenzen, met name waar kritieke systemen in contact staan met externe netwerken of minder betrouwbare interne zones.

KERNMAATREGEL

CyberFundamentals IMPORTANT

PR.PS-01.1
De organisatie moet een basisconfiguratie voor haar bedrijfskritieke systemen ontwikkelen, documenteren en onderhouden.

DOEL

Ervoor zorgen dat alle bedrijfskritieke systemen in een bekende, veilige en goedgekeurde staat functioneren. Een basisconfiguratie definieert de standaardopstelling voor deze systemen, waardoor ongeoorloofde wijzigingen kunnen worden opgespoord, beveiligingsbeleid kan worden gehandhaafd en consistente bedrijfsvoering kan worden ondersteund.

PR.DS-02.1
Draagbare opslagapparaten die systeemgegevens bevatten, moeten tijdens transport en opslag worden bewaakt en beschermd.

DOEL

Ongeoorloofde toegang, manipulatie of verlies van kritieke systeemgegevens voorkomen wanneer draagbare opslagapparaten tussen locaties worden verplaatst of buiten beveiligde omgevingen worden opgeslagen.

Respond CyFun®

NEW

KERNMAATREGEL

CyberFundamentals IMPORTANT

RS.CO-02.2
Cyberbeveiligingsincidenten moeten binnen de in het incidentresponsplan vastgestelde termijnen worden gedeeld met relevante externe belanghebbenden, met inbegrip van het melden van belangrijke incidenten aan de bevoegde autoriteiten zoals wettelijk vereist.

DOEL

Ervoor zorgen dat alle relevante externe partijen tijdig, veilig en op gepaste wijze worden geïnformeerd over cyberbeveiligingsincidenten, zodat het vertrouwen behouden blijft en aan wettelijke en contractuele verplichtingen wordt voldaan.

Respond CyFun®

KERNMAATREGEL

CyberFundamentals IMPORTANT

RS.MI-01.2

De organisatie moet ongeautoriseerde toegang of datalekken detecteren en passende maatregelen nemen om deze te beperken, waaronder het monitoren van kritieke systemen aan externe grenzen en op belangrijke interne punten.

DOEL

Ongeoorloofde toegang en gegevenslekken tijdig te detecteren en passende maatregelen te nemen om de schade te beperken.

CyFun®

Thank you

CCB Certification Authority (NCCA)

Certification@ccb.belgium.be

Centre for Cybersecurity Belgium

Rue de la Loi / Wetstraat 18 – 1000 Brussels

www.ccb.belgium.be

What does TLP Green mean?

TRAFFIC LIGHT PROTOCOL (TLP)

Green (TLP GREEN)

Limited disclosure, recipients can spread this within their community.

Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.

Recipients may share TLP:GREEN information with peers and partner organisations within their community, but not via publicly accessible channels (e.g. websites, LinkedIn…). TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.