Serverplatform

BIO Thema-uitwerking

Mei 2026 [versie 3.0 definitief]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.



©Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen (CC BY-NC-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl.

BIO Thema-uitwerking Serverplatform

Titel	BIO Thema-uitwerking Serverplatform
Datum	Mei 2026
Versie en status	3.0 definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	CIP-kernteamleden
Reviewers	Versie 1.0: Professionals uit het CIP-netwerk en het CIP-kernteam Versie 2.0: CIP-kernteam Versie 2.1: CIP-kernteam Versie 2.2: CIP-kernteam Versie 2.3: CIP-kernteam Versie 3.0: CIP-kernteam

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Wijzigingsbeheer

In de onderstaande tabel worden alle relevante wijzigingen in dit document bijgehouden, om eenvoudig inzicht te krijgen in de uitgevoerde aanpassingen.

Versie	Datum	Wijziging	Door
1.0	Februari 2019		CIP-kernteam
2.0	Maart 2021		CIP-kernteam
2.1	Oktober 2021		CIP-kernteam
2.2	Maart 2023		CIP-kernteam
2.3	November 2023	Tekstverbeteringen, BUC-afbeeldingen in tabelvorm, harde enters vervangen, doelstellingen en risico's geüniformeerd)	CIP-kernteam
3.0	Mei 2026	BIO2 1.3 verwerkt	CIP-kernteam

Leeswijzer

Voorafgaand aan hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein, de kern van dit document, heeft elke BIO Thema-uitwerking een inleiding met een standaard paragraafindeling.

Aanvullend geldt:

- Voor de aanduiding van personen wordt de mannelijke vorm aangehouden (hij/hem/zijn) ongeacht het geslacht.
- De controls en maatregelen vermeld in deze thema-uitwerking zijn in het beleids-, uitvoerings- en control-domein georganiseerd, waarmee ze bij de overeenkomstige functionarissen kunnen worden geadresseerd. Deze functionarissen zijn niet benoemd omdat dit organisatie-afhankelijk is.
- Van best practices (open standaarden al dan niet toegankelijk met een licentie) zijn de meest actuele versies afgekort vermeld, tenzij de actuele versie niet toereikend is.

Voor een overzicht van alle gebruikte best practices, afkortingen en begrippen en een generieke toelichting op de opzet van de thema-uitwerkingen, zie de Structuurwijzer BIO Thema-uitwerkingen.

Inhoudsopgave

Leeswijzer 3

1 Inleiding 7

1.1 Opzet BIO Thema-uitwerking 7

1.2 Scope en begrenzing serverplatform 7

1.3 Context serverplatform 8

2 Beveiligingsobjecten serverplatform 10

2.1 Vaststellen beveiligingsobjecten voor serverplatform 10

2.2 Globale relaties tussen beveiligingsobjecten 11

2.2.1 Beleidsdomein 11

2.2.2 Uitvoeringsdomein 11

2.2.3 Control-domein 11

3 Beleidsdomein 12

3.1 Doelstelling 12

3.2 Risico’s 12

3.3 Objecten, controls en maatregelen 12

3.3.1 B.01 Beleid voor beveiligde inrichting en onderhoud 13

Objectdefinitie 13

Objecttoelichting 13

3.3.2 B.02 Inrichtingsprincipes voor serverplatform 13

Objectdefinitie 13

Objecttoelichting 13

3.3.3 B.03 Serverplatform-architectuur 14

Objectdefinitie 14

Objecttoelichting 14

4 Uitvoeringsdomein 16

4.1 Doelstelling 16

4.2 Risico’s 16

4.3 Objecten, controls en maatregelen 16

4.3.1 U.01 Bedieningsprocedure 17

Objectdefinitie 17

Objecttoelichting 17
4.3.2 U.02 Standaarden voor serverconfiguratie 18
Objectdefinitie 18
Objecttoelichting 18
4.3.3 U.03 Malwareprotectie 18
Objectdefinitie 18
Objecttoelichting 18
4.3.4 U.04 Technische kwetsbaarhedenbeheer 19
Objectdefinitie 19
Objecttoelichting 19
4.3.5 U.05 Patchmanagement 21
Objectdefinitie 21
Objecttoelichting 21
4.3.6 U.06 Beheer op afstand 22
Objectdefinitie 22
Objecttoelichting 22
4.3.7 U.07 Server-onderhoud 24
Objectdefinitie 24
Objecttoelichting 24
4.3.8 U.08 Verwijderen of hergebruiken serverapparatuur 24
Objectdefinitie 24
Objecttoelichting 24
4.3.9 U.09 Hardenen server 25
Objectdefinitie 25
Objecttoelichting 25
4.3.10 U.10 Serverconfiguratie 26
Objectdefinitie 26
Objecttoelichting 26
4.3.11 U.11 Virtualisatie serverplatform 27
Objectdefinitie 27
Objecttoelichting 27
4.3.12 U.12 Beperking software-installatie 28

Objectdefinitie 28
Objecttoelichting 28
4.3.13 U.13 Kloksynchronisatie 29
Objectdefinitie 29
Objecttoelichting 29
4.3.14 U.14 Ontwerpdocument 29
Objectdefinitie 29
Objecttoelichting 29
5 Control-domein 31
5.1 Doelstelling 31
5.2 Risico's 31
5.3 Objecten, controls en maatregelen 31
5.3.1 C.01 Evaluatierichtlijn servers en serverplatforms 31
Objectdefinitie 31
Objecttoelichting 32
5.3.2 C.02 Beoordeling technische serveromgeving 32
Objectdefinitie 32
Objecttoelichting 32
5.3.3 C.03 Logbestanden beheerders 33
Objectdefinitie 33
Objecttoelichting 33
5.3.4 C.04 Logging 34
Objectdefinitie 34
Objecttoelichting 34
5.3.5 C.05 Monitoring 34
Objectdefinitie 34
Objecttoelichting 35
5.3.6 C.06 Beheersorganisatie servers en serverplatforms 35
Objectdefinitie 35
Objecttoelichting 36

1 Inleiding

Dit document bevat een referentiekader voor het thema Serverplatform. Het is geënt op de controls uit de Baseline Informatiebeveiliging Overheid (BIO2), die gebaseerd is op de NEN-ISO/IEC 27002:2022 (hierna genoemd ISO 27002). Er wordt ook gebruik gemaakt van andere best practices zoals: The Standard of Good Practice (SoGP) 2018 en van de National Institute en Standard and Technology (NIST).

Dit kader dient evenals andere BIO Thema-uitwerkingen als een toetsinstrument voor interne en externe leveranciers om inzicht te geven in het beveiligings- en beheersingsniveau van haar ICT-organisatie. Dit thema geeft tevens inzicht in de kwaliteitszorg die de leverancier dient toe te passen bij het opleveren van nieuwe infrastructuur.

1.1 Opzet BIO Thema-uitwerking

De inhoudelijke onderwerpen die besproken worden in deze BIO Thema-uitwerking (de objecten) zijn gestructureerd in een drietal domeinen: Beleid, Uitvoering en Control (BUC). Deze objecten vormen de onderwerpen die bij de verwerving en het beheer van serverplatforms van belang zijn. Per domein zijn ze uitgewerkt in de vorm van controls en onderliggende maatregelen.

Deze Thema-uitwerking volgt de standaard opzet voor BIO Thema-uitwerkingen:

- scope en begrenzing van het thema (zie paragraaf 1.2);
- context van het thema (zie paragraaf 1.3);
- beveiligingsobjecten en uitwerking van deze objecten op de BUC-lagen (zie paragraaf 2.1);
- globale relaties van de geïdentificeerde beveiligingsobjecten (zie paragraaf 2.2).

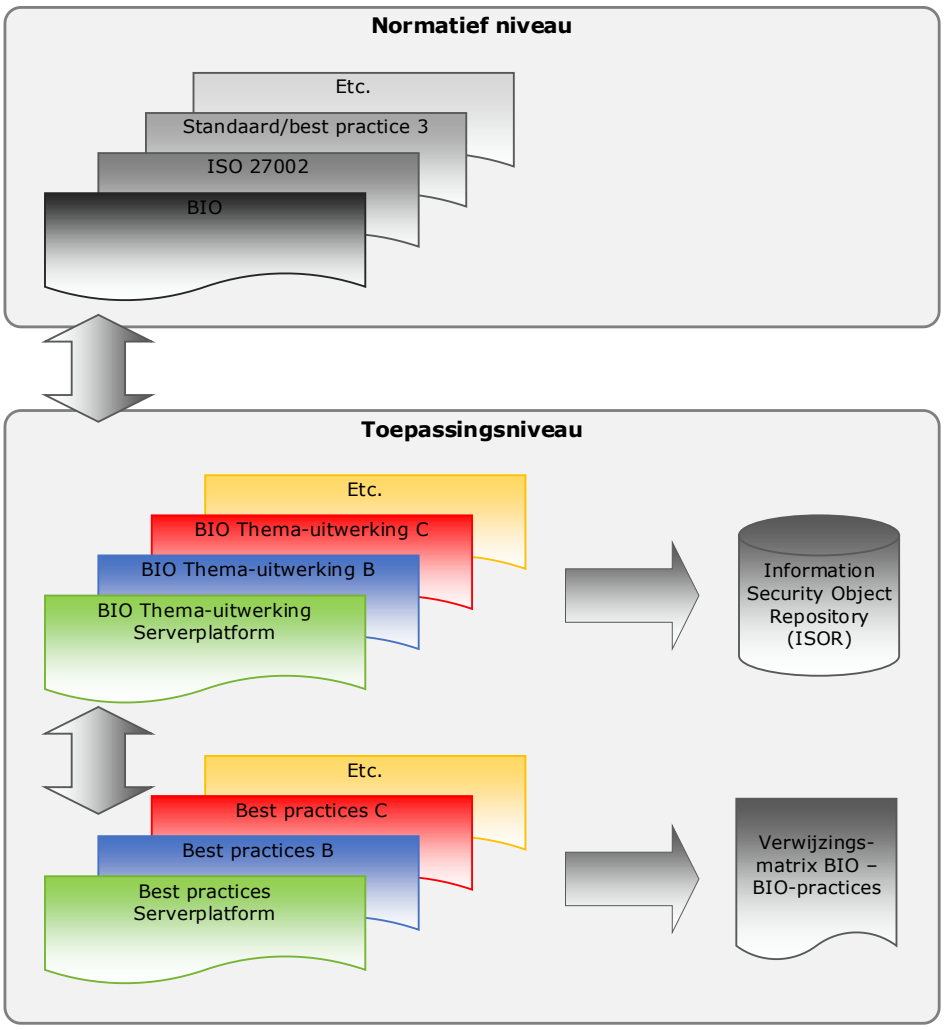
1.2 Scope en begrenzing serverplatform

In deze BIO Thema-uitwerking is de scope van het begrip serverplatform beperkt tot de basisfunctionaliteit en algemene onderwerpen die gerelateerd zijn aan serverplatforms. Enkele componenten van dit thema zijn: server-hardware, virtualisatietechnologie en besturingssysteem. Organisaties zullen met deze informatie hun eigen servers in hun omgeving moeten beoordelen en nagaan welke risico's aanvullend gemitigeerd moeten worden.

De thema-uitwerking beschrijft niet de kenmerken van specifieke typen servers, zoals: bestandserver, applicatieserver, webserver, mailserver of databaseserver.

De objecten voor serverplatform komen direct of indirect uit de BIO2 of uit andere best practices. In sommige gevallen zijn de teksten aangepast op het specifieke onderdeel serverplatform. Voorbeelden: de vertaling van de BIO-titel 'Beleid voor beveiligd ontwikkelen' (zie paragraaf 3.3.1) naar het overeenkomstige object voor serverplatforms, is 'Beleid voor beveiligde inrichting en onderhoud'; de BIO-titel 'Principes voor engineering van beveiligde systemen', is vertaald naar het object 'Inrichtingsprincipes voor serverplatform' (zie paragraaf 3.3.2).

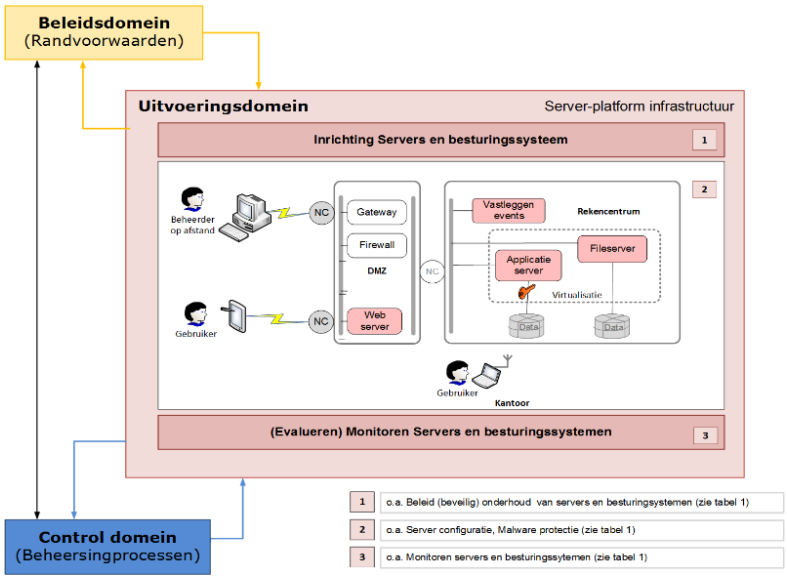
De begrenzing van dit document is weergegeven in afbeelding 1.



Afbeelding 1: Relatie BIO Thema-uitwerking Serverplatform met aanpalende documenten

1.3 Context serverplatform

Servers zijn computers, die via werkstations (clients), een of meerdere diensten aan eindgebruikers of aan andere computersystemen beschikbaar stellen. Voorbeelden van servers zijn: fileserver, database-server, mailserver, webserver en File Transfer Protocol (FTP)-server. Het kan ook gerelateerd zijn aan software die deze dienst mogelijk maakt, zoals een softwaremodule die verzoeken van gebruikers accepteert en verwerkt. Een server bedient een of meerdere clients. Afbeelding 2 geeft een globale context van enkele typen servers en schetst hoe ze in relatie staan met beleids- en beheersingsaspecten.



Afbeelding 2: Context van het thema Serverplatform

In de hier geschetste situatie logt de externe gebruiker (linksboven in het schema) aan op een webserver vanuit het internet. De webserver geeft de relevante gebruikersgegevens door aan een portal-toegangsserver, die op zijn beurt applicaties vanuit backoffice-servers beschikbaar stelt.

De gebruiker linksonder in afbeelding 2 is een medewerker van een vertrouwde partij, die via een semi-vertrouwd kanaal informatie zoekt op een webserver van de partnerorganisatie.

De interne gebruiker onderin het schema logt aan op z'n werkstation via het lokale netwerk.

In veel gevallen is er ook sprake van 'middleware', ofwel applicatiecode die bepaalde functies vervult tussen de gebruikersapplicatie en het besturingssysteem. Zie daarvoor de BIO Thema-uitwerking Middleware.

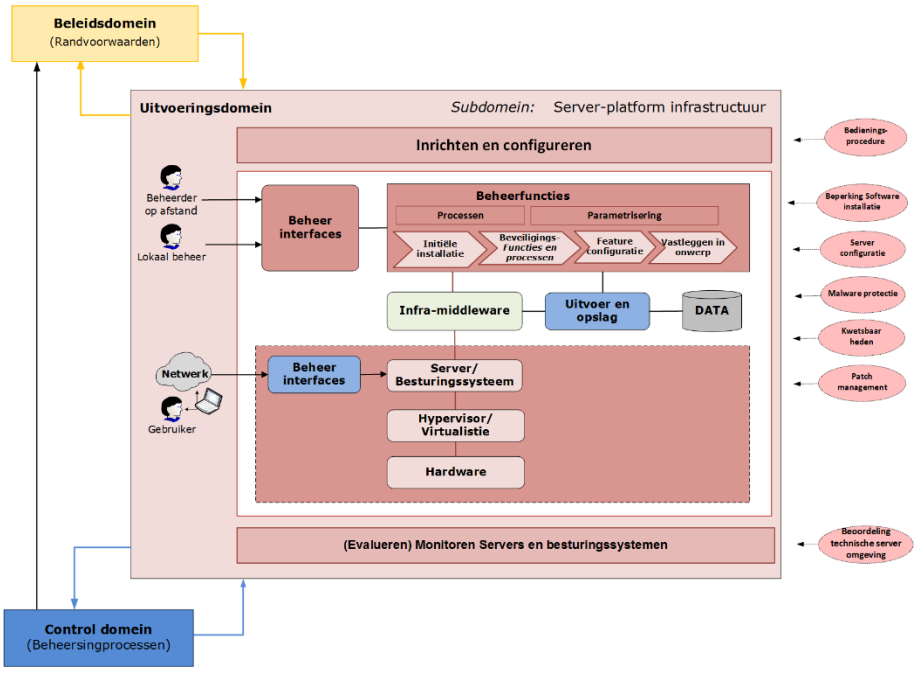
2 Beveiligingsobjecten serverplatform

Objecten worden geïdentificeerd met onderzoeksvragen en risicogebieden. De objecten, met hun uitwerking naar controls en maatregelen, hebben tot doel risico's te mitigeren. Ze zijn afgeleid vanuit de optiek van de kwaliteitscriteria: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid (BIVC), en vervolgens ingedeeld in het beleids-, uitvoerings- en control-domein.

De vragen die hierbij een rol spelen zijn:

- Beleidsdomein: Welke elementen spelen een rol bij de conditionering en sturing op de inrichting van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
- Uitvoeringsdomein: Welke elementen spelen een rol bij de inrichting van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
- Control-domein: Welke elementen spelen een rol bij de beheersing van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?

Afbeelding 3 geeft de positionering weer van servers binnen de lagenstructuur van het uitvoeringsdomein. De functieblokken bevatten op hun beurt beveiligingsobjecten waarvoor beveiligingsmaatregelen getroffen moeten worden.



Afbeelding 3: Gelaagdheid serverplatform met enkele beveiligingsobjecten

2.1 Vaststellen beveiligingsobjecten voor serverplatform

De tabellen 1, 2 en 3 uit hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein geven een overzicht van alle relevante beveiligingsobjecten voor het thema Serverplatform, afkomstig uit de BIO2.

Uit de contextuele analyse blijkt dat er enkele onderwerpen bestaan die niet in de BIO2 voorkomen. Voor deze onderwerpen, waarvoor de BIO2 geen control heeft geformuleerd, zijn controls uit andere

baselines geadopteerd, zoals: SoGP, NIST en ICT-Beveiligingsrichtlijnen voor Webapplicaties van het Nationaal Cyber Security Centrum (NCSC).

2.2 Globale relaties tussen beveiligingsobjecten

Het thema Serverplatform omvat het geheel van beleid, richtlijnen, procedures, processen, mensen (actoren), middelen en registraties dat van belang is voor het betrouwbaar functioneren van serverplatforms, die het fundament vormen van informatiesystemen. De essentiële objecten voor serverplatforms worden ingedeeld naar de domeinen: beleid, uitvoering en control. Deze objecten worden in hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein verder toegelicht en uitgewerkt. Serverplatforms zijn er in zowel fysieke als gevirtualiseerde vormen. De basiselementen die bij de beveiliging een rol spelen zijn bij beide typen gelijk.

2.2.1 *Beleidsdomein*

Dit domein schetst de randvoorwaarden, conditionele aspecten en beperkingen, waaraan de inrichting van het serverplatform moet voldoen.

2.2.2 *Uitvoeringsdomein*

De keuze van objecten uit de BIO2 (en daarmee ook de ISO 27002) voor het thema Serverplatform vloeit voort uit enkele uitgangspunten die gerelateerd zijn aan serverplatform:

- Initiële installatie
  De initiële installatie wordt uitgevoerd op basis van richtlijnen en procedures, bijvoorbeeld: bedieningsprocedure (ISO 27002-terminologie).
- Beveiligings- en beheerfuncties
  De beveiligingsfunctie is gerelateerd aan protectiemechanismen die de beveiliging van de server moeten bevorderen, zoals malwareprotectie en hardenen van systeemfuncties. De beheerfunctie is gerelateerd aan processen als: server-onderhoud en beheer van kwetsbaarheden.
- Configuratie van systeemfuncties
  Servers hebben verschillende systeemfuncties, die adequaat moeten zijn geconfigureerd om het beveiligingsniveau te kunnen garanderen.
- Structuur en ontwerp
  De configuraties van servers en de koppelingen en relaties tussen verschillende servers moeten in een ontwerpdocument zijn vastgelegd.

2.2.3 *Control-domein*

Dit domein omvat beoordelingsrichtlijnen voor het evalueren van de vastgestelde randvoorwaarden en de uitvoeringscomponenten.

3 Beleidsdomein

3.1 Doelstelling

De doelstelling van het beleidsdomein is het identificeren en beschrijven van de conditionele elementen die voorwaardelijk zijn voor het inrichten, beveiligen en beheersen van serverplatforms. De hierbij van belang zijnde beveiligingsobjecten zijn uitgewerkt in controls en gerelateerde maatregelen.

3.2 Risico's

Als de juiste beleidsaspecten voor de inrichting en het onderhoud van het serverplatform ontbreken, is het risico dat onvoldoende sturing wordt gegeven aan een veilige inrichting en exploitatie van deze systemen. Daardoor komt de informatievoorziening van de organisatie als geheel in gevaar en kunnen er datalekken optreden.

3.3 Objecten, controls en maatregelen

De onderwerpen die specifiek voor serverplatforms een rol spelen, zijn vermeld in tabel 1. Is een objectblok geel gekleurd, dan komt de bijbehorende control voor in de BIO2. Betreft het een wit gemarkeerd objectblok, dan heeft de BIO geen control gedefinieerd, maar is dit object wel noodzakelijk voor deze BIO Thema-uitwerking.

Intentie	Functie	Gedrag	Structuur
B.01 Beleid voor beveiligde inrichting en onderhoud ((Operationeel) beleid	/	/	B.03 Serverplatform-architectuur (IT-architectuur)
B.02 Inrichtingsprincipes voor serverplatform ((Operationeel) beleid)	/	/	/

Tabel 1: Beleidsobjecten met basiselementen voor serverplatform per invalshoek

Binnen de kolom functies behoren objecten te worden opgenomen die voor serverplatforms gerelateerd zijn aan beveiligingsfuncties en beheerprocessen. Deze objecten hebben, in dit geval, echter meer een operationeel karakter. Daarom zijn functie-gerelateerde objecten in het uitvoeringsdomein opgenomen. De noodzakelijke beveiligingseisen voor functies op dit niveau zijn vermeld in paragraaf 3.3.1 B.01 Beleid voor beveiligde inrichting en onderhoud.

Binnen de gedragskolom zou een beleid voor configuratie, parametrisering en toegangsbeleid tot serverplatform opgenomen kunnen worden. Echter, dit soort beleidselementen komen eveneens voor in B.01 Beleid voor beveiligde inrichting en onderhoud. Vandaar dat ook in deze kolom geen objecten zijn vermeld.

3.3.1 *B.01 Beleid voor beveiligde inrichting en onderhoud*

Objectdefinitie

Resultaat van een besluitvorming over het onderhouden van serverplatforms.

Objecttoelichting

Dit object is ontleend aan de control 'Beleid voor beveiligd ontwikkelen' uit de ISO 27002:2022: 8.25, die betrekking heeft op het opbouwen van beveiligde dienstverlening, software, systemen en architectuur. Toegespitst naar serverplatforms als 'Beleid voor beveiligde inrichting en onderhoud' ziet dit object hier op standaarden en procedures voor inrichting en onderhoud van servers.

Doelstelling	Het beheersen van de beveiligde inrichting en onderhoud van het serverplatform.		
Risico	Er zijn onvoldoende mogelijkheden om sturing te geven aan de effectieve en betrouwbare inrichting van een serverplatform en hierover een verantwoordingsrapportage te laten afgeven.		
Control	Voor het beveiligd inrichten en onderhouden van het serverplatform behoren **regels** te worden vastgesteld en binnen de organisatie te worden toegepast.		ISO 27002:2022: 8.25
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	De gangbare principes rondom 'security by design' zijn uitgangspunt voor het onderhouden van servers.	ISO 27002:2022: 8.25
	2.	In het beleid voor beveiligd inrichten en onderhouden zijn de volgende aspecten in overweging genomen: • het toepassen van richtlijnen/standaarden voor de configuratie van servers en besturingssystemen; • het gebruik van hardeningsrichtlijnen; • het toepassen van standaard images; • het beperken van toegang tot krachtige faciliteiten en instellingen voor hostparameter; • het beschermen tegen ongeautoriseerde toegang.	SoGP 2018: SY1.2.1

3.3.2 *B.02 Inrichtingsprincipes voor serverplatform*

Objectdefinitie

Fundamentele uitgangspunten voor het veilig inrichten van een serverplatform.

Objecttoelichting

Bij het inrichten van servers en serverplatforms behoren beveiligingsprincipes in acht te worden genomen. Hierbij vormen 'security by design' en 'secure by default' het uitgangspunt. Daarnaast worden principes zoals defence in depth, least privilege en fail secure eveneens aanbevolen om toe te passen.. In andere baselines (zoals de SoGP) zijn verschillende andere van belang zijnde inrichtingsprincipes te vinden.

Doelstelling	Het zorgen dat servers betrouwbaar zijn gedurende alle inrichtingsverrichtingen van servers.

Risico	Bij de inrichting van servers zijn niet alle vereiste beveiligingsprincipes meegenomen.		
Control	**Principes** voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.		ISO 27002:2022: 8.27
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Principes	1.	De gangbare principes rondom 'security by design' en 'secure by default' zijn uitgangspunt voor het inrichten van servers.	BIO@: 8.27.01 ISO 27002:2022: 8.27
	2.	Voor het beveiligd inrichten van servers zijn de volgende beveiligingsprincipes van belang: • defence in depth (beveiliging op verschillende lagen); • secure by default; • least privilege (minimaal toegangsniveau); • fail secure, waarbij informatie door een systeemfout niet toegankelijk is voor onbevoegde personen en niet kan worden gemanipuleerd of gewijzigd; • eenduidige naamgevingsconventie; • minimalisatie van single points of failure.	SoGP 2018: SY1.1.3

3.3.3 *B.03 Serverplatform-architectuur*

Objectdefinitie

Modelmatige beschrijving van de wijze waarop serverplatforms zijn ingericht, samenhangen met andere systemen, zijn beveiligd en worden beheerst.

Objecttoelichting

De architectuur van een serverplatform geeft overzicht en inzicht in de wijze waarop de gebieden en objecten behoren te worden beveiligd. Architectuur geeft ook inzicht in de samenhang van beveiligingsmaatregelen. In de architectuur zijn gemaakte ontwerp- en inrichtingskeuzen gedocumenteerd en verantwoord en zijn de gemaakte keuzen onderbouwd.

Documentatie speelt ook een belangrijke rol bij het bepalen van de impact van wijzigingen en het voorkomen van ontwerpfouten. Documentatie moet dan ook na elke wijziging worden bijgewerkt; oude documentatie moet worden gearchiveerd.

Doelstelling	Het bieden van een landschap voor een serverplatform dat in samenhang beveiligd is en inzicht geeft in de inrichting van het serverplatform.	
Risico	Er is onvoldoende sturing op de inrichting van het serverplatform. Bedreigingen worden over het hoofd gezien.	
Control	De functionele eisen, beveiligingseisen en architectuurvoorschriften van het serverplatform zijn in samenhang in een **architectuurdocument** vastgelegd.	NIST SP 800-53 Rev. 5 2020: PL-8
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Architectuur-document	1.	Van het in te richten serverplatform is een actueel architectuurdocument opgesteld. Dit document: • heeft een eigenaar; • is voorzien van een datum en versienummer; • bevat een documenthistorie (wat is wanneer en door wie aangepast); • is actueel, juist en volledig; • is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd; • wordt actief onderhouden.	SoGP 2018: TS1.1.9a, c en d
	2.	In het architectuurdocument is vastgelegd welke uitgangspunten, principes, beveiligingsvoorschriften, eisen en overwegingen gelden voor het inrichten van serverplatforms.	SoGP 2018: TS1.1.5

4 Uitvoeringsdomein

4.1 Doelstelling

De doelstelling van het uitvoeringsdomein voor de inrichting en exploitatie van het serverplatform is het waarborgen dat de werkzaamheden plaatsvinden volgens specifieke beleidsuitgangspunten en dat de werking voldoet aan de eisen die door de klant (doelorganisatie) zijn gesteld.

4.2 Risico's

Wanneer adequate protectiefuncties voor het serverplatform ontbreken, ontstaan er risico's op het gebied van virus- en malwarebesmetting, dataverlies of datalekken.

Wanneer meer functionaliteit is ingeschakeld dan nodig is voor de bedrijfsvoering nemen risico's van diefstal of inbreuk toe.

Wanneer er onvoldoende zoneringsfuncties zijn geactiveerd, kunnen invloeden van buitenaf de dienstverlening via computers of netwerken onmogelijk maken.

Kwetsbare plekken in de systeemketens zoals Single Points of Failure (SPoF) veroorzaken continuïteitsproblemen en maken 7x24 uur beschikbaarheidsgaranties praktisch onmogelijk.

4.3 Objecten, controls en maatregelen

De objecten die specifiek voor het serverplatform een rol spelen, zijn vermeld in tabel 1. De roodgekleurde objecten zijn afgeleid van de BIO2. De witte objecten zijn afgeleid van overige best practices.

Intentie	Functie	Gedrag	Structuur
U.01 Bedieningsprocedure ((Operationeel) beleid)	U.03 Malwareprotectie (Beschermingsfunctie)	U.09 Hardenen server (Eigenschap)	U.14 Ontwerpdocument (IT-architectuur)
U.02 Standaarden voor serverconfiguratie ((Operationeel) beleid)	U.04 Technische kwetsbaarhedenbeheer (Proces)	U.10 Serverconfiguratie (Eigenschap)	/
/	U.05 Patchmanagement (Proces)	U.11 Virtualisatie serverplatform (Eigenschap)	/
/	U.06 Beheer op afstand (Proces)	U.12 Beperking software-installatie (Eigenschap)	/
/	U.07 Server-onderhoud (Proces)	U.13 Kloksynchronisatie (Eigenschap)	/
/	U.08 Verwijderen of hergebruiken	/	/

	serverapparatuur (Proces)		

Tabel 2: Uitvoeringobjecten met basiselementen voor serverplatform per invalshoek

4.3.1 *U.01 Bedieningsprocedure*

Objectdefinitie

Vastgelegde manier van handelen voor het beheren van serverplatforms.

Objecttoelichting

Het betreft de beschrijving van taken/activiteiten zoals installatie en configuratie, starten en afsluiten, back-up en onderhoud van servers.

Doelstelling	Het waarborgen van een correcte en veilige bediening van serverplatforms.		
Risico	Het optreden van beveiligingsincidenten en/of datalekken. Kennis raakt verloren over het bedienen van serverplatforms.		
Control	**Bedieningsprocedures** behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.		ISO 27002:2022: 5.37
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Bedienings-procedures	1.	Voor bedieningsactiviteiten die samenhangen met informatieverwerking en communicatiefaciliteiten, zoals de procedures voor het starten en afsluiten van de computer, back-up, onderhoud van apparatuur, zijn gedocumenteerde procedures opgesteld.	ISO 27002:2022: 5.37
	2.	Gedocumenteerde bedieningsprocedures behoren te worden beoordeeld en zo nodig bijgewerkt. Wijzigingen in gedocumenteerde bedieningsprocedures voor systeemactiviteiten worden formeel door het hoger management goedgekeurd.	ISO 27002:2022: 5.37
	3.	In de bedieningsprocedures zijn de bedieningsvoorschriften opgenomen, onder andere voor: • verantwoordelijke personen en rollen; • beveiligde installatie en configuratie van systemen; • verwerking en behandeling van informatie (geautomatiseerd en handmatig); • back-up en herstel; • planning en onderlinge afhankelijkheden met andere systemen; • omgang met fouten en uitzonderlijke omstandigheden; • ondersteunings- en escalatiecontacten (inclusief externe partijen); • behandeling van opslagmedia; • herstart- en herstelprocedures bij storingen; • beheer van audit- en logbestanden; • monitoring van capaciteit, prestaties en beveiliging; • onderhoudsinstructies. •	ISO 27002:2022: 5.37.a t/m l

4.3.2 *U.02 Standaarden voor serverconfiguratie*

Objectdefinitie

Geheel van gedocumenteerde en erkende afspraken, specificaties of criteria, betreffende configuraties en parametrisering van serverinstellingen.

Objecttoelichting

De standaarden voor de configuratie van servers worden vastgelegd in documenten.

Doelstelling	Het zorgen voor een correcte werking van het serverplatform, met de vereiste beveiligingsinstellingen. Het voorkomen van onjuiste wijziging en wijziging door onbevoegden.		
Risico	De server is niet of onvoldoende geconfigureerd voor de functionaliteit binnen de IT-omgeving.		
Control	Het serverplatform is geconfigureerd volgens gedocumenteerde **standaarden**.		SoGP 2018: SY1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Standaarden	1.	De documentatie volgens de standaarden omvat: • het bieden van gestandaardiseerde firmwareconfiguraties; • het gebruik van gestandaardiseerde en vooraf bepaalde server-images voor het bouwen/configureren van servers; • het wijzigen van de standaardwaarden van leveranciers- en andere beveiligingsparameters; • het uitschakelen of beperken van onnodige functies en services; • het beperken van de toegang tot krachtige beheerhulpmiddelen en hostparameter-instellingen (bijvoorbeeld Windows 'Register-editor'); • het beschermen tegen ongeoorloofde toegang; • het uitvoeren van standaard beveiligingsbeheerpraktijken.	SoGP 2018: SY1.2.1

4.3.3 *U.03 Malwareprotectie*

Objectdefinitie

De continue bescherming van serverplatforms tegen schadelijke software.

Objecttoelichting

De organisatie maakt gebruik van malwareprotectie bij ingangs- en uitgangspunten van kritieke informatiesystemen (zoals firewalls, e-mailservers, webservers, proxyservers en servers met externe toegang), op werkstations, servers en mobiele computerapparatuur op het netwerk.

De organisatie gebruikt deze beschermingsmechanismen om haar servers te beschermen tegen schadelijke code en om schadelijke code te detecteren en te neutraliseren.

Doelstelling	Het zorgen dat informatie op servers wordt beschermd tegen malware.
Risico	Malware wordt niet opgespoord. Aangetroffen malware wordt niet of onvoldoende hersteld.

Control	Ter bescherming tegen malware behoren beheersmaatregelen voor **preventie**, **detectie** en **herstel** te worden geïmplementeerd, in combinatie met het stimuleren van een passend bewustzijn van gebruikers.		ISO 27002:2022: 8.7
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Preventie	1.	Het gebruik van niet-geautoriseerde software is formeel verboden in het informatiebeveiligingsbeleid. Er zijn regels en technische maatregelen om ongeautoriseerd gebruik te voorkomen of te detecteren.	ISO 27002:2022: 8.7, 8.19
	2.	Er zijn maatregelen om toegang tot bekende of verdachte kwaadaardige websites te blokkeren of te detecteren (bijv. blocklisting, web filtering).	ISO 27002:2022: 8.7.a, b
	3.	Gebruikers worden geïnformeerd en getraind over risico's van surfgedrag, klikken op onbekende links, downloads en bijlagen.	BIO2: 8.07.02 ISO 27002:2022: 6.3, 8.7.m
	4.	Het downloaden van bestanden en software van externe bronnen is beperkt en gebaseerd op risicoanalyse en het principe 'need-to-use'. De antimalware-software beoordeelt altijd alle downloads.	BIO2: 8.07.01 ISO 27002:2022: 8.7.e
Detectie	5.	Anti-malwaresoftware is geïnstalleerd en up-to-date op alle relevante systemen (servers, endpoints, mail- en webgateways). Reguliere scans worden uitgevoerd op alle binnenkomende data, downloads, bijlagen en webcontent voorafgaand aan executie of opslag.	BIO2: 8.07.04 ISO 27002:2022: 6.3, 8.7.f, g
	6.	Anti-malware- en herstelsoftware wordt periodiek geüpdatet en ondersteund door actuele dreigingsinformatie uit betrouwbare bronnen.	BIO2: 8.07.03 ISO 27002:2022: 8.7.n, o
Herstel	7.	Er is een procedure voor tijdelijke of permanente uitzonderingen op malwarebescherming, inclusief autorisatie, documentatie, onderbouwing en evaluatiedatum.	ISO 27002:2022: 8.7.l
	8.	Er zijn bedrijfscontinuïteitsplannen voorbereid voor herstel na malware-incidenten, inclusief back-up- en herstelprocedures voor data en software.	ISO 27002:2022: 8.7.j

4.3.4 *U.04 Technische kwetsbaarhedenbeheer*

Objectdefinitie

Instandhoudingsproces voor het onderzoek naar en het oplossen van technische kwetsbaarheden.

Objecttoelichting

Kwaadwillenden maken gebruik van kwetsbaarheden en zwakheden in software die op de servers zijn geïnstalleerd. Kwetsbaarhedenbeheer is een proactieve benadering van beveiliging door de kans te verminderen dat gebreken in software de beveiliging van een server in gevaar brengt.

Zonder inzicht in de actuele stand van zaken, kan de beheerder niet goed anticiperen op nieuwe ontwikkelingen. Vragen die hierbij een rol spelen:

- Hoe is de serveromgeving opgebouwd en geconfigureerd?

- Wat zijn bekende kwetsbaarheden en zwakheden?

Gerelateerd aan kwetsbaarhedenbeheer is het patchmanagementproces. Het ISO 27002-onderwerp 'Beheer van technische kwetsbaarheden' (in paragraaf 8.8) behandelt wat betreft de maatregelen twee onderwerpen:

Kwetsbaarhedenbeheer (vulnerability-management);
- Patchmanagement (zie paragraaf 4.3.5 U.05 Patchmanagement).

In deze BIO Thema-uitwerking worden deze twee onderwerpen apart beschreven.

Doelstelling	Het voorkomen van misbruik van technische kwetsbaarheden en het treffen van passende maatregelen bij blootstelling daaraan.		
Risico	Kwetsbaarheden in servers worden niet opgemerkt.		
Control	Informatie over **technische serverkwetsbaarheden**[1] behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden dient te worden **geëvalueerd** en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.		ISO 27002:2022: 8.8
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Technische serverkwets-baarheden	1.	Er is een beheersproces voor technische kwetsbaarheden vastgesteld, inclusief rollen, verantwoordelijkheden, middelen en een tijdsbestek voor reactie op kwetsbaarheidsmeldingen.	BIO2: 8.08.01 ISO 27002:2022: 8.8
	2.	Bij hoge kans op misbruik én hoge verwachte schade (volgens NCSC Inschalingsmatrix) worden mitigerende maatregelen zo snel mogelijk, maar uiterlijk binnen 1 week getroffen.	BIO2: 8.08.01
	3.	Op basis van een expliciete risicoafweging wordt bepaald op welke wijze (patchen, tijdelijke mitigerende maatregelen, compenserende controles) kwetsbaarheden worden aangepakt. Als installatie binnen een week niet mogelijk is, worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	BIO2: 8.08.02, 03
	4.	Informatiesystemen (met name internetfacing) worden waar mogelijk continu of minimaal jaarlijks getest op zwakheden en kwetsbaarheden (kwetsbaarheidsanalyse, penetratietesten, red teaming), om de technische naleving van beveiligingsnormen en risico's van de feitelijke veiligheid te waarborgen.	BIO2: 8.08.04, 05
	5.	Bij nieuwe releases of major updates van internetfacing systemen wordt waar mogelijk een geautomatiseerde penetratietest uitgevoerd. Bij kritieke bevindingen die niet anders gemitigeerd kunnen worden, mag het systeem niet in productie.	BIO2: 8.08.05

[1] Zie Handreiking: 4.42 Penetratietesten

Geëvalueerd	6.	Het kwetsbaarhedenbeheersproces wordt periodiek gemonitord en geëvalueerd. Wijzigingen aan patches en mitigerende maatregelen worden getest en geautoriseerd via het wijzigingsbeheerproces.	ISO 27002:2022: 8.8, 8.32

4.3.5 *U.05 Patchmanagement*

Objectdefinitie

Besturingsproces voor het verwerven, testen en installeren van patches op een computersysteem.

Objecttoelichting

Patchmanagement is het proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen ter opheffing van bekende beveiligingsproblemen in de code) op (verschillende softwarecomponenten van) een computersysteem. Een solide updatemechanisme is essentieel om voldoende beschermd te zijn tegen bekende beveiligingsproblemen in de software.

De noodzaak van het patchen staat vaak niet ter discussie. Vaak ontstaat echter wel discussie over de urgentie waarmee patches moeten worden uitgevoerd. Hoe ernstiger de kwetsbaarheid, hoe noodzakelijker het is om de tijdsduur tussen het uitkomen van een patch en het implementeren ervan, kort te houden. Het kan voorkomen dat systemen die niet meer ondersteund worden, (tijdelijk) operationeel gehouden moeten worden. In dat geval is het van belang om te weten welke systemen dat zijn en welke aanvullende maatregelen getroffen zijn om deze systemen voor het uitbuiten van kwetsbaarheden te behoeden.

Doelstelling	Het zorgen dat kwetsbaarheden tijdig en effectief worden aangepakt, om een stabiele omgeving te creëen.		
Risico	Servers zijn niet stabiel en betrouwbaar.		
Control	Patchmanagement is **procesmatig** en **procedureel** opgezet en wordt ondersteund door **richtlijnen** zodat het zodanig kan worden uitgevoerd dat op de servers de laatste (beveiligings)patches tijdig zijn geïnstalleerd.		NCSC 2015: C.09
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procesmatig	1.	Het patchmanagementproces is beschreven, goedgekeurd door het management en toegekend aan een verantwoordelijke functionaris.	NCSC 2015: C.09.01
	2.	Een technisch mechanisme zorgt voor (semi-)automatische updates.	CIP-netwerk
	3.	Configuratiebeheer geeft het inzicht waarmee servers worden gepatcht.	CIP-netwerk

	4.	Het patchbeheerproces bevat methoden om: • Alleen patches van legitieme en geautoriseerde bronnen worden gebruikt en toegepast; • Patches in overeenstemming met het wijzigingsbeheerproces worden geïnstalleerd. Bij hoge urgentie wordt het wijzigingsproces gevolgd of (indien nodig) de incidentresponsprocedure; • Voor systemen waar automatische updates beschikbaar zijn, wordt bewust besloten of deze functionaliteit wordt ingeschakeld; • Van alle patchactiviteiten (inclusief testresultaten, implementatiedatum en status) wordt een auditbare registratie bijgehouden.	ISO 27002:2022: 8.8.b, c, e
Procedureel	5.	De patchmanagementprocedure is actueel en beschikbaar.	CIP-netwerk
	6.	De rollen en verantwoordelijkheden voor patchmanagement zijn vastgesteld.	NCSC 2015: C.09.03
	7.	De volgende aspecten van een patch worden geregistreerd: • de beschikbare patches; • hun relevantie voor de systemen/bestanden; • het besluit tot wel/niet uitvoeren; • de testdatum en het resultaat van de patchtest; • de datum van implementatie; • het patchresultaat.	NCSC 2015: C.09.04
Richtlijnen	8.	Ter ondersteuning van de patchactiviteiten is op het juiste (organisatorische) niveau een opgestelde patchrichtlijn vastgesteld en geaccordeerd.	NCSC 2015: C.09.05
	9.	Alleen beschikbare patches van een legitieme (geautoriseerde) bron mogen worden geïmplementeerd.	CIP-netwerk
	10.	Patches worden getest en geëvalueerd voordat ze in productie worden geïnstalleerd, waarbij de risico's van de kwetsbaarheid worden afgewogen tegen de risico's van de patch zelf.	ISO 27002:2022: 8.8.d
	11.	Wanneer een patch niet beschikbaar of niet toepasbaar is, worden passende alternatieve maatregelen overwogen en gedocumenteerd (bijv. tijdelijke compenserende controles).	ISO 27002:2022: 8.8.l

4.3.6 *U.06 Beheer op afstand*

Objectdefinitie

Instandhoudingsproces van servers vanuit een externe, niet-vertrouwde omgeving.

Objecttoelichting

Toegang tot de servers is beperkt tot geautoriseerde personen en informatiesystemen.

Onder bepaalde voorwaarden is het beheerders toegestaan om servers te benaderen van buiten de door de organisatie beheerde netwerken.

Doelstelling	Het voorkomen van verlies, schade, diefstal of in gevaar brengen van informatie en andere bijbehorende assets en van onderbreking van de activiteiten van de organisatie.		
Risico	De server is onbetrouwbaar. Hij functioneert niet naar behoren.		
Control	**Richtlijnen** en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.		ISO 27002:2022: 6.7
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Richtlijnen	1.	Toegang tot kritieke systemen voor beheer op afstand door externe personen wordt beheerd door: • het definiëren en overeenkomen van de doelstellingen en reikwijdte van de geplande werkzaamheden; • het autoriseren van individuele sessies; • het beperken van toegangsrechten (binnen doelstellingen en reikwijdte); • het loggen van alle ondernomen activiteiten; • het gebruiken van unieke authenticatiereferenties voor elke implementatie; • het toewijzen van toegangsreferenties aan individuen in plaats van gedeeld; • het intrekken van toegangsrechten en het wijzigen van wachtwoorden onmiddellijk nadat het overeengekomen onderhoud is voltooid; • het uitvoeren van een onafhankelijke beoordeling van onderhoudsactiviteiten op afstand.	SoGP 2018: NC1.6.1
	2.	Het op afstand onderhouden van servers wordt strikt beheerd door: • het verifiëren van de bron van de verbinding op afstand; • het bepalen van de toestemming voordat toegang wordt verleend voor de connectiviteit; • het beperken van het aantal gelijktijdige externe verbindingen; • het bewaken van activiteiten gedurende de gehele duur van de verbinding; • het uitschakelen van de verbinding zodra de geautoriseerde activiteit voltooid is.	SoGP 2018: NC1.6.4
	3.	Het serverplatform is zodanig ingericht, dat dit op afstand kan worden geconfigureerd en beheerd en dat automatisch kan worden gecontroleerd of vooraf gedefinieerde parameters en drempelwaarden worden aangetast of overschreden.	SoGP 2018: SY1.1.2c
	4.	Handmatige interventie wordt niet toegepast, tenzij geautoriseerd en gedocumenteerd.	CIP-netwerk
	5.	Alle externe toegang tot servers vindt versleuteld plaats.	CIP-netwerk

4.3.7 *U.07 Server-onderhoud*

Objectdefinitie

Geheel van activiteiten voor de instandhouding van de adequate werking en het beveiligingsniveau van een serverplatform.

Objecttoelichting

In deze BIO Thema-uitwerking wordt het begrip 'apparatuur' in ISO 27002 2022 opgevat als de infrastructuurcomponent 'server', die periodiek onderhouden dient te worden. Het onderhoud behoort plaats te vinden binnen een tijdsinterval. Servers worden correct onderhouden door bevoegd personeel om te zorgen dat de beschikbaarheid van de dienstverlening en de integriteit hiervan gegarandeerd is.

Doelstelling	Het waarborgen van continu beschikbare en integere servers.		
Risico	De beschikbaarheid en integriteit van servers zijn aangetast.		
Control	Servers behoren correct te worden **onderhouden** om de continue beschikbaarheid en integriteit te waarborgen.		ISO 27002:2022: 7.13
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Onderhouden	1.	Het onderhoud van servers wordt uitgevoerd met richtlijnen die invulling geven aan de volgende eisen: • Apparatuur wordt in overeenstemming met de door de leverancier aanbevolen frequentie voor servicebeurten en voorschriften onderhouden; • Reparaties en onderhoudsbeurten aan apparatuur worden alleen uitgevoerd door bevoegd onderhoudspersoneel, waarbij toezicht wordt gehouden op onderhoudspersoneel tijdens het uitvoeren van onderhoud ter plaatse; • Passende beheersmaatregelen worden geïmplementeerd wanneer onderhoud van apparatuur is gepland, rekening houdend met of dit onderhoud wordt uitgevoerd door personeel ter plaatse of door extern personeel, waarbij het onderhoudspersoneel gehouden is aan een passende geheimhoudingsovereenkomst. De toegang voor onderhoud op afstand wordt op basis van autorisaties toegestaan en beveiligd; • Voordat apparatuur na onderhoud weer in bedrijf wordt gesteld, wordt een inspectie uitgevoerd om te waarborgen dat niet met de apparatuur geknoeid is en dat deze naar behoren functioneert.	ISO 27002:2022: 7.13.a t/m j

4.3.8 *U.08 Verwijderen of hergebruiken serverapparatuur*

Objectdefinitie

Veilig verwijderen of hergebruiken van serverapparatuur.

Objecttoelichting

Opslagmedia van apparatuur bevat vaak vertrouwelijke informatie. Wanneer servers buiten gebruik worden gesteld of opnieuw worden ingezet, moet deze informatie veilig verwijderd zijn.

Doelstelling	Het waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.		
Risico	Onbevoegden beschikken over informatie met een vertrouwelijk karakter.		
Control	Alle onderdelen van servers die **opslagmedia** bevatten, behoren te worden **geverifieerd** om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.		ISO 27002:2022: 7.14
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Opslagmedia	1.	Servers die vertrouwelijke informatie bevatten, worden niet met de standaard delete-functie gewist, maar fysiek vernietigd of onherstelbaar gewist met gevalideerde technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen.	ISO 27002:2022 7.14
Geverifieerd	2.	Voorafgaand aan verwijdering, hergebruik of afvoer van servers, wordt gecontroleerd of alle gevoelige informatie veilig is verwijderd of onherstelbaar gewist.	ISO 27002:2022 7.14

4.3.9 *U.09 Hardenen server*

Objectdefinitie

Proces van het uitschakelen van overbodige functies van een server.

Objecttoelichting

De standaardconfiguratie van de meeste besturingssystemen is niet ontworpen met beveiliging als primaire focus. In plaats daarvan zijn standaardinstellingen meer gericht op bruikbaarheid, communicatie en functionaliteit.

Hardening is het proces van het uitschakelen of verwijderen van overbodige en/of niet gebruikte functies, services en accounts, waarmee de beveiliging wordt verbeterd. Ook servers behoren te worden gehardend. Alle overbodige en niet gebruikte functies, services en accounts behoren van de server(s) te worden verwijderd of te worden uitgeschakeld.

Doelstelling	Het verbeteren van de beveiliging van servers.		
Risico	Er wordt misbruik gemaakt van overbodige en/of niet gebruikte functies, services en accounts.		
Control	Voor het beveiligen van een server worden overbodige **functies** en ongeoorloofde **toegang** uitgeschakeld.		SoGP 2018: SY1.2.5 SoGP 2018: SY1.2.8
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Functies	1.	Een server is zodanig geconfigureerd dat onderstaande functies zijn verwijderd of uitgeschakeld: • niet-essentiële en overbodige (redundant) services; • het kunnen uitvoeren van gevoelige transacties en scripts; • krachtige beheer-hulpmiddelen; • het 'run'-commando en 'command'-processors; • de 'auto-run'-functie.	SoGP 2018: SY1.2.5

	2.	Een server is zodanig geconfigureerd dat gebruik van onderstaande functies wordt beperkt: • communicatiediensten die inherent vatbaar zijn voor misbruik; • communicatieprotocollen die gevoelig zijn voor misbruik.	SoGP 2018: SY1.2.5

Toegang	3.	Een server wordt beschermd tegen ongeoorloofde toegang doordat:
		• onnodige of onveilige gebruikersaccounts zijn verwijderd;
		• belangrijke beveiliging gerelateerde parameters in 'veilige stand' zijn gewijzigd;
		• time-out faciliteiten worden gebruikt, die:
		  ○ automatisch na een vooraf bepaalde periode van inactiviteit sessies sluiten en een blanco scherm tonen op de beheerschermen;
		  ○ vereisen dat opnieuw wordt ingelogd voordat een beheerscherm zich herstelt.
			SoGP 2018: SY1.2.8

4.3.10 *U.10 Serverconfiguratie*

Objectdefinitie

Instelling van systeemfuncties van een serverplatform.

Objecttoelichting

Serverplatforms hebben verschillende systeemfuncties en bieden een veelheid aan functies om services te kunnen leveren. Om ze veilig te laten functioneren, behoort elk serverplatform volgens bepaalde standaarden en procedures te zijn geconfigureerd.

Doelstelling	Het veilig laten functioneren van serverplatforms.		
Risico	Serverplatforms functioneren niet zoals vereist en zijn niet/onvoldoende beschermd tegen ongeautoriseerd en incorrecte updates.		
Control	Serverplatforms behoren zo **geconfigureerd** te zijn, dat zij functioneren zoals het vereist is en zijn beschermd tegen **ongeautoriseerd** en incorrecte updates.		SoGP 2018: SY1.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Geconfigu-reerd	1.	De servers zijn geconfigureerd volgens gedocumenteerde standaarden/procedures die betrekking hebben op: • het inrichten van standaard firmware-configuraties; • het gebruik van gestandaardiseerde vooraf bepaalde serverimages voor het bouwen/configureren van servers; • het wijzigen van de standaardwaarden en andere beveiligingsparameters van de leverancier(s); • het verwijderen, uitschakelen en/of beperken van onnodige functies en services; • het beperken van de toegang tot krachtige beheerhulpmiddelen en host-parameterinstellingen; • het beschermen tegen ongeoorloofde toegang; • het uitvoeren van standaard beveiligingsbeheerpraktijken.	SoGP 2018: SY1.2.1

	2.	De servers zijn geconfigureerd volgens een gestandaardiseerde en vooraf bepaald serverimage.	SoGP 2018: SY1.2.3
Ongeautori-seerd	3.	Toegang tot serverparameterinstellingen en krachtige beheerinstrumenten zijn: • beperkt tot een gelimiteerd aantal geautoriseerde personen; • beperkt tot specifiek omschreven situaties; • gekoppeld aan specifieke en gespecificeerde autorisatie.	SoGP 2018: SY1.2.7

4.3.11 *U.11 Virtualisatie serverplatform*

Objectdefinitie

Logische, softwarematig gecreëerde serveromgeving.

Objecttoelichting

Servervirtualisatie stelt een organisatie in staat om een of meer gescheiden logische omgevingen te creëren op één fysieke server. Bij virtualisatie zijn drie soorten componenten betrokken: een fysieke server, een hypervisor en een of meerdere virtuele servers.

De hypervisor alloceert resources van de fysieke server naar elke onderliggende virtuele server, inclusief Central Processing Unit (CPU), geheugen, harddisk of netwerk. Hiermee zijn de virtuele servers in staat simultaan of geïsoleerd van elkaar te opereren. Deze drie componenten moeten voldoen aan specifieke eisen.

Doelstelling	Het in voldoende mate beveiligen van gevoelige informatie op een virtueel serverplatform.		
Risico	Onbevoegden krijgen inzicht in gevoelige informatie.		
Control	Virtuele servers behoren goedgekeurd te zijn en toegepast te worden op robuuste en veilige **fysieke servers** (bestaande uit **hypervisors** en **virtuele servers**) en behoren zodanig te zijn geconfigureerd dat gevoelige informatie in voldoende mate is beveiligd.		SoGP 2018: SY1.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Fysieke servers	1.	Fysieke servers die worden gebruikt om virtuele servers te hosten, worden beschermd tegen: • onbeheerde en ad hoc-inzet van virtuele servers (zonder juiste procedures aanvraag, creëren en schonen); • overbelasting van resources ((CPU), geheugen en harde schijf) door het stellen van een limiet voor het aanmaken van het aantal virtuele servers op een fysieke host server.	SoGP 2018: SY1.3.4
Hypervisors	2.	Hypervisors worden geconfigureerd om: • virtuele servers onderling (logisch) te scheiden met het oog op vertrouwelijkheid en ter voorkoming dat informatie wordt uitgewisseld tussen discrete omgevingen; • de communicatie tussen virtuele servers te coderen; • de toegang te beperken tot een gelimiteerd aantal geautoriseerde personen; • de rollen van hypervisoradministrators te scheiden.	SoGP 2018: SY1.3.5

Virtuele servers	3.	Virtuele servers worden ingezet, geconfigureerd en onderhouden volgens standaarden en procedures, ter bescherming van: • fysieke servers die worden gebruikt voor het hosten van virtuele servers; • hypervisors die zijn geassocieerd met virtuele servers; • virtuele servers die op een fysieke server worden uitgevoerd.	SoGP 2018: SY1.3.1 SoGP 2018: SY1.3.2
	4.	Virtuele servers worden beschermd met standaard beveiligingsmechanismen op hypervisors, waaronder: • het toepassen van standaard beveiligingsrichtlijnen voor fysieke en logische toegang; • het hardenen van de fysieke en virtuele servers; • het wijzigingsbeheer en de malwareprotectie; • het toepassen van monitoring en van netwerk gebaseerde beveiliging.	SoGP 2018: SY1.3.6 SoGP 2018: SY1.3.7

4.3.12 *U.12 Beperking software-installatie*

Objectdefinitie

Systematisch ontwikkelde aanbevelingen ter beperking van het installeren van programmatuur door eindgebruikers.

Objecttoelichting

Veel misbruik van systemen is het gevolg van kwetsbaarheden in software. Het is daarom van belang dat alleen door de organisatie toegestane en gevalideerde software wordt toegelaten op de technische infrastructuur. Voor de installatie en het gebruik van software op servers moeten derhalve regels worden opgesteld en nagevolgd.

Doelstelling	Het voorkomen dat software wordt geïnstalleerd die schade kan veroorzaken, zoals het weglekken van informatie, verlies van integriteit, andere informatiebeveiligingsincidenten of het schenden van intellectuele-eigendomsrechten.		
Risico	Kwetsbaarheden worden geïntroduceerd.		
Control	Er behoren **procedures en maatregelen** te worden geïmplementeerd om het installeren van software op operationele systemen op beveiligde wijze te beheren.		ISO 27002:2022: 8.19
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Procedures en maatregelen	1.	Installatie en updates op operationele systemen mogen alleen door opgeleide beheerders met passende rechten worden uitgevoerd. Gebruikers mogen geen niet-geautoriseerde software installeren.	BIO2: 8.19.01 ISO 27002:2022: 8.19.a
	2.	Uitsluitend goedgekeurde uitvoerbare code mag worden geïnstalleerd. Ontwikkelcode, compilers en andere ontwikkelhulpmiddelen zijn uitgesloten.	ISO 27002:2022: 8.19.b
	3.	Software wordt pas geïnstalleerd of geüpdatet na uitgebreide en geslaagde tests. Bijbehorende programmabronbibliotheken worden meegeüpdatet. Een roll-backstrategie wordt vooraf gedefinieerd.	ISO 27002:2022: 8.19.c, d, f

	4.	Een configuratiebeheersysteem beheert operationele software en documentatie. Van alle wijzigingen wordt een auditlog bijgehouden. Oude versies worden gearchiveerd zolang nodig voor gegevensherstel.	ISO 27002:2022: 8.19.e, g, h

4.3.13 *U.13 Kloksynchronisatie*

Objectdefinitie

Gelijke tijdsinstelling van systeemklokken op verschillende servers.

Objecttoelichting

Om gebeurtenissen uit verschillende systeemcomponenten te correleren, worden de klokken van de verschillende servers gelijkgericht, waarmee de timestamps van gebeurtenissen op de verschillende omgevingen zijn gesynchroniseerd.

Met het Network Time Protocol (NTP) wordt bereikt dat de tijd op alle servers en andere componenten overeenkomt (zie paragraaf 10.10.6 'Synchronisatie van systeemklokken' in de ISO 27002 2007).

Doelstelling	Mogelijk maken van correlatie en analyse van registraties van beveiligingsgerelateerde gebeurtenissen en van onderzoek naar informatiebeveiligingsincidenten.		
Risico	Auditlogbestanden bieden onvoldoende basis voor een onderzoek. Ze kunnen niet worden ingezet als steekhoudend bewijs in juridische of disciplinaire zaken.		
Control	De klokken van alle informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden **gedocumenteerd** en **gesynchroniseerd** met goedgekeurde referentietijdbronnen.		ISO 27002:2022: 8.17
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gedocumenteerd	1.	De interne en externe eisen voor weergave, synchronisatie en nauwkeurigheid van tijdsinstellingen, alsmede de aanpak voor het verkrijgen van een referentietijd van een externe bron, alsook de wijze waarop interne klokken betrouwbaar worden gesynchroniseerd, zijn gedocumenteerd.	ISO 27002:2022: 8.17 SoGP 2018: TM1.2.3
Gesynchroniseerd	2.	De systemen zijn met een standaard referentietijd geconfigureerd, waarbij gebruik wordt gemaakt van een consistente en vertrouwde datum- en tijdbron, zodat gebeurtenislogboeken nauwkeurige tijdstempels gebruiken.	ISO 27002:2022: 8.17

4.3.14 *U.14 Ontwerpdocument*

Objectdefinitie

Document waarin de inrichting van de server en de configuratie-instellingen zijn vastgelegd.

Objecttoelichting

De vastlegging van de inrichting van de server en de instellingen biedt het overzicht en de transparantie, die benodigd zijn voor deugdelijk beheer en onderhoud.

Doelstelling	Het creëren van een gedocumenteerde basis voor het onderhoud en het beheer van de inrichting van het serverplatform en de (beveiligings)instellingen.		
Risico	De inrichting van de server en het serverplatform wijkt af van wat vooraf nodig is geacht en/of onduidelijkheden bij het beheer en onderhoud.		
Control	Het **ontwerp** van een serverplatform behoort te zijn gedocumenteerd.		SoGP 2018: SY1.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Ontwerp	1.	Het ontwerp van elk serverplatform en elke server is gedocumenteerd, waarbij onder andere is beschreven hoe rekening gehouden is met: • de principes van de beveiligingsarchitectuur en beveiligingsvereisten; • de risico's van voorzienbare ontwikkelingen in het gebruik van IT door de organisatie.	SoGP 2018: SY1.1.1

5 Control-domein

5.1 Doelstelling

Het doel van het control-domein voor deze BIO Thema-uitwerking is vast te stellen in hoeverre:

- de controls voldoende zijn ingericht en functioneren om de beoogde beschikbaarheid, integriteit en vertrouwelijkheid van het serverplatform te garanderen;
- de infrastructurele diensten functioneel en technisch op het juiste niveau worden gehouden en de beveiliging ervan kan worden gegarandeerd.

Dit houdt onder meer in dat binnen de organisatie een adequate beheerorganisatie moet zijn ingericht, waarin de beheerprocessen zijn vormgegeven.

5.2 Risico's

Bij het ontbreken van de noodzakelijke control-maatregelen binnen de organisatie van de IT-leverancier is het niet zeker of de inrichting en exploitatie van deze systemen aan de beoogde organisatorische en beveiligingsvoorwaarden voldoen en dat de governance van deze omgeving toereikend is ingericht. Tevens kan dan niet vastgesteld worden dat de gewenste maatregelen worden nageleefd.

5.3 Objecten, controls en maatregelen

De objecten die specifiek voor het serverplatform een rol spelen, zijn vermeld in tabel 3. De blauwgekleurde objecten zijn afgeleid van de BIO. De witte objecten zijn afgeleid van overige best practices.

Intentie	Functie	Gedrag	Structuur
C.01 Evaluatierichtlijn servers en serverplatforms ((Operationeel) beleid	C.02 Beoordeling technische serveromgeving (Proces)	C.03 Logbestanden beheerders (Event/historie)	C.06 Beheersorganisatie servers en serverplatforms (IT-organisatiestructuur)
/	/	C.04 Logging (Event/historie)	/
/	/	C.05 Monitoring (Event/historie)	/

Tabel 3: Control-objecten met basiselementen voor serverplatform per invalshoek

5.3.1 *C.01 Evaluatierichtlijn servers en serverplatforms*

Objectdefinitie

Vastgestelde richtlijn voor de uitvoering van evaluatieactiviteiten van een serverplatform.

Objecttoelichting

Binnen de infrastructuur bevinden zich verschillende servers en besturingssystemen die het fundament vormen voor applicaties. Deze servers en besturingssystemen moeten daarom continu worden onderhouden, gehardend en op een veilige wijze geconfigureerd. In het kader van risicomanagement is het van groot belang dat deze servers en besturingssystemen, periodiek geëvalueerd worden. De evaluatie-activiteiten dienen uitgevoerd te worden volgens evaluatierichtlijnen, procedures en instructies, waarmee wordt bevorderd dat de evaluatieresultaten voldoen aan de verwachte eisen.

Doelstelling	Het adequaat uitvoeren van controle-activiteiten en opstellen van rapportages, gericht op de implementatie en beveiliging van servers en besturingssystemen.		
Risico	De resultaten van de controle-activiteiten voldoen niet aan de verwachte eisen. Het management stuurt niet op afwijkingen.		
Control	**Richtlijnen** behoren te worden vastgesteld om de implementatie en beveiliging van servers en besturingssystemen te controleren waarbij de bevindingen tijdig aan het management worden gerapporteerd.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Richtlijnen	1.	De organisatie beschikt over richtlijnen voor het beoordelen van de technische omgeving van servers en besturingssystemen.	CIP-netwerk
	2.	De organisatie beschikt over geautomatiseerde middelen voor effectieve ondersteuning van de controle-activiteiten.	CIP-netwerk
	3.	De organisatie beschikt over richtlijnen voor het uitvoeren van registratie, statusmeting, analyse, rapportage en evaluatie.	CIP-netwerk
	4.	De organisatie heeft de taken, verantwoordelijkheden en bevoegdheden van controle-functionarissen vastgelegd.	CIP-netwerk

5.3.2 *C.02 Beoordeling technische serveromgeving*

Objectdefinitie

Evaluatie van de mate waarin de serveromgeving voldoet aan de vooraf gestelde technische eisen.

Objecttoelichting

Voor het doeltreffend kunnen beheersen van de beveiliging, is het noodzakelijk de technische omgeving regelmatig te beoordelen. Hiertoe dienen periodiek zowel de organisatorische als de technische aspecten beoordeeld te worden. Het betreft dan onder andere:

- de toepassing van het geformuleerde inrichtingsbeleid voor servers,
- de serverplatformarchitectuur,
- de taken en verantwoordelijkheden,
- het gebruik van technische middelen,
- de controle aanpak
- het inschakelen van externe specialisten.

Als resultaat dient een rapportage van bevindingen aan het management te worden uitgebracht.

Doelstelling	Het vaststellen of de technische serveromgevingen voor servers en besturingssystemen afdoende zijn beveiligd.		
Risico	Kwetsbaarheden in technische serveromgevingen voor servers en besturingssystemen worden niet opgemerkt.		
Control	Technische serveromgevingen behoren regelmatig te worden beoordeeld op **naleving** van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.		ISO 27002:2022: 5.36, 8.8
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Naleving	1.	Voor serverplatforms en servers bepalen managers en eigenaren hoe de naleving van informatiebeveiligingseisen (beleid, regels, normen en technische standaarden) wordt gecontroleerd en beoordeeld.	ISO 27002:2022: 5.36
	2.	Technische naleving van servers en serverplatforms wordt bij voorkeur beoordeeld met geautomatiseerde instrumenten. Bevindingen worden tijdig gerapporteerd aan het management.	ISO 27002:2022: 5.36
	3.	Bij geconstateerde niet-naleving worden oorzaken onderzocht, corrigerende maatregelen vastgesteld en uitgevoerd, en de effectiviteit ervan gecontroleerd. Alle stappen worden geregistreerd.	ISO 27002:2022: 5.36, 8.8
	4.	Corrigerende maatregelen worden tijdig afgerond op basis van het risico. Niet-afgeronde maatregelen worden meegenomen in de volgende beoordelingsronde.	ISO 27002:2022: 5.36

5.3.3 *C.03 Logbestanden beheerders*

Objectdefinitie

In logbestanden vastgelegde beheeractiviteiten.

Objecttoelichting

Logging is het proces voor het registreren van technische activiteiten en gebeurtenissen. Hiermee kunnen achteraf fouten of onrechtmatigheden in het gebruik (waaronder ongeautoriseerde toegangspogingen tot technische componenten) vroegtijdig worden gesignaleerd. Het loggen van activiteiten spitst zich toe op de bewaking van rechtmatigheid van toegekende rechten en het gebruik hiervan.

Doelstelling	Het vroegtijdig achteraf signaleren van fouten en/of onrechtmatigheden in het gebruik, waaronder ongeautoriseerde toegangspogingen tot technische componenten.	
Risico	Er ontstaat schade, waaronder ongeautoriseerde toegangspogingen tot technische componenten.	
Control	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de **logbestanden** behoren te worden beschermd en regelmatig te worden beoordeeld.	ISO 27002:2022: 8.15
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Logbestanden	1.	De logbestanden worden beschermd tegen ongeautoriseerd manipuleren en worden beoordeeld om vast te stellen wie welke activiteit heeft uitgevoerd.	BIO2: 8.15.01, 06 ISO 27002:2022: 8.15
	2.	Speciale gebruikers (beheerders/operators) geven rekenschap over de door hun uitgevoerde beheeractiviteiten en kunnen hun eigen activiteiten niet verwijderen of deactiveren.	BIO2: 8.15.05 ISO 27002:2022: 8.15

5.3.4 *C.04 Logging*

Objectdefinitie

Vastlegging van informatiebeveiliging-gerelateerde gebeurtenissen.

Objecttoelichting

Op de servers en besturingssystemen vinden automatische en handmatige activiteiten plaats. Vanuit beveiligingsoptiek is het van belang om deze activiteiten te registreren in logbestanden en te controleren.

Doelstelling	Het verzamelen van bewijs om achteraf te kunnen beoordelen of er ongeoorloofde acties hebben plaatsgevonden op servers en besturingssystemen.		
Risico	Ongeoorloofde acties op servers en besturingssystemen worden niet opgemerkt. Wordt het wel opgemerkt, dan is er geen bewijs voorhanden.		
Control	Er behoren **logbestanden** waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, te worden geproduceerd, opgeslagen, beschermd en geanalyseerd.		ISO 27002:2022: 8.15
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Logbestanden	1.	Logbestanden van gebeurtenissen bevatten, voor zover relevant: • Actie: de gebeurtenis of handeling die heeft plaatsgevonden. • Object: waarop de gebeurtenis of handeling effect had (bijvoorbeeld welk bestand, proces of server). • Resultaat: het resultaat van de gebeurtenis of handeling. • Oorsprong: het apparaat of de netwerklocatie van waaruit de gebeurtenis of handeling in gang is gezet. • Actor: identificatie van de persoon die of het proces dat de gebeurtenis in gang heeft gezet. • Tijdstempel: datum en tijdstip waarop de gebeurtenis of handeling plaatsvond. • Nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden. •	BIO2: 8.15.01, 02

5.3.5 *C.05 Monitoring*

Objectdefinitie

Bewaking en onderkenning van afwijkingen op het verwachtte gebruikspatroon van servers.

Objecttoelichting

Onder monitoren wordt verstaan: bewaken, analyseren en rapporteren. Het monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot servers en serverplatforms tijdig te signaleren en, proportioneel aan de ernst ervan, acties te ondernemen. De monitoringsfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris. Monitoring vindt mede plaats op basis van geregistreerde gegevens (logging). De geregistreerde gegevens dienen te worden geanalyseerd en te worden gerapporteerd (alerting). Alerting kan ook geautomatiseerd plaats vinden op basis van vastgestelde overschrijding van drempelwaarden.

Doelstelling	Het vaststellen van onjuist gebruik en verdachte activiteiten op servers en besturingssystemen op basis waarvan het management tijdig kan bijsturen.		
Risico	Er zijn onvoldoende mogelijkheden om tijdig bij te sturen om organisatorisch en technisch te (blijven) voldoen aan de doelstellingen.		
Control	De organisatie **analyseert** regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten op servers en besturingssystemen vast te stellen en bevindingen aan het management te **rapporteren**.		NCSC 2015: C.07 ISO 27002:2022: 8.16
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Analyseert	1.	De verantwoordelijke functionaris analyseert periodiek: • de gelogde gebruikers- en activiteitengegevens van servers en serverplatforms; • het optreden van verdachte gebeurtenissen en mogelijke schendingen van de beveiligingseisen; • eventuele ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden.	NCSC 2015: C.07.03
	2.	De verzamelde log-informatie wordt in samenhang geanalyseerd.	NCSC 2015: C.07.05
	3.	Periodiek worden de geanalyseerde en beoordeelde gelogde (gesignaleerde) gegevens aan de systeemeigenaren en/of aan het management gerapporteerd.	NCSC 2015: C.07.08
	4.	De rapportages uit de beheerdisciplines compliancy-management, vulnerability assessment, penetratietest en logging en monitoring worden op aanwezigheid van structurele risico's geanalyseerd en geëvalueerd.	NCSC 2015: C.07.09
Rapporteren	5.	De analyserapportage bevat informatie over kwetsbaarheden, zwakheden en misbruik en wordt gecommuniceerd met het verantwoordelijke management.	NCSC 2015: C.07.09
	6.	De eindrapportage bevat op analyses gebaseerde verbetervoorstellen.	CIP-netwerk

5.3.6 *C.06 Beheersorganisatie servers en serverplatforms*

Objectdefinitie

Doelgerichte bundeling van kennis en vaardigheden tussen personen met taken, verantwoordelijkheden en bevoegdheden voor de beheersing van de serverplatformomgevingen.

Objecttoelichting

Voor het adequaat beheersen en beheren van servers en serverplatforms moet een beheersorganisatiestructuur zijn vastgesteld, waarin de verantwoordelijkheden voor de beheersprocessen, voorzien van toereikende bevoegdheden, zijn vastgelegd en op het juiste niveau zijn gepositioneerd.

Doelstelling	Het invullen, coördineren en borgen van de beheersing van servers en serverplatforms.		
Risico	Servers en serverplatforms zijn onvoldoende beveiligd.		
Control	Binnen de beheerorganisatie is een **beveiligingsfunctionaris** benoemd die de organisatie ondersteunt in de vorm van het bewaken van **beveiligingsbeleid** en die inzicht verschaft in de inrichting van de servers en het serverplatform.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligings-functionaris	1.	De beveiligingsfunctionaris zorgt onder andere voor: • de actualisatie van beveiligingsbeleid voor servers en besturingssystemen; • de afstemming van het beveiligingsbeleid in de afgesloten overeenkomsten met onder andere de ketenpartijen; • de evaluatie van de effectiviteit van de beveiliging van de ontwikkelde systemen; • de evaluatie van de beveiligingsmaatregelen ten aanzien van de bestaande risico's; • de bespreking van beveiligingsissues met ketenpartijen; • het verschaffen van inzicht in de afhankelijkheden tussen servers binnen de infrastructuur.	CIP-netwerk
Beveiligings-beleid	2.	Het beveiligingsbeleid geeft onder andere inzicht in: • inrichtings-, onderhouds- en beheervoorschriften (procedureel en technisch); • specifieke beveiligings- en architectuurvoorschriften; • afhankelijkheden tussen servers binnen de infrastructuur.	CIP-netwerk