Serverplatform

BIO Thema-uitwerking

Maart 2021 [versie 2.0 definitief]

BIO Thema-uitwerking Serverplatform

Titel	BIO Thema-uitwerking Serverplatform
Datum	Maart 2021
Versie	2.0 definitief
Opdrachtgever	Voorzitter werkgroep BIO en directeur CIP
Regime	Becommentarieerde praktijk
Auteurs	Wiekram Tewarie (UWV/CIP) en Jaap van der Veen (CIP)
Reviewers	Versie 1.0: Jan Breeman (UWV), Paul Coret (Hoogheemraadschap Delfland), Peter van Dijk (VNG/IBD), Kees Hintzbergen (VNG/IBD), René Reith (Provincie Zuid-Holland) en Ton Voogt (ICT Architects) Versie 2.0: 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.

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

1	Inleiding	5
1.1	Opzet van het thema	5
1.2	Scope en begrenzing van serverplatform	5
1.3	Context van serverplatform	6
2	Beveiligingsobjecten serverplatform	8
2.1	Vaststellen beveiligingsobjecten voor serverplatform	8
2.2	Globale relaties tussen de beveiligingsobjecten	8
2.2.1	Beleidsdomein	9
2.2.2	Uitvoeringsdomein	9
2.2.3	Control-domein	9
3	Beleidsdomein	10
3.1	Doelstelling	10
3.2	Risico’s	10
3.3	Objecten, controls en maatregelen	10
3.3.1	B.01 Beleid voor beveiligde inrichting en onderhoud	11
3.3.2	B.02 Principes voor inrichten beveiligde servers	11
3.3.3	B.03 Serverplatform-architectuur	12
4	Uitvoeringsdomein	14
4.1	Doelstelling	14
4.2	Risico’s	14
4.3	Objecten, controls en maatregelen	14
4.3.1	U.01 Bedieningsprocedures	15
4.3.2	U.02 Standaarden voor serverconfiguratie	16
4.3.3	U.03 Malwareprotectie	16
4.3.4	U.04 Beheer serverkwetsbaarheden	17
4.3.5	U.05 Patchmanagement	19
4.3.6	U.06 Beheer op afstand	21
4.3.7	U.07 Server-onderhoud	22
4.3.8	U.08 Veilig serverapparatuur verwijderen of hergebruiken	22
4.3.9	U.09 Hardenen servers	23
4.3.10	U.10 Serverconfiguratie	24

4.3.11	U.11 Virtueel serverplatform	25
4.3.12	U.12 Beperking software-installatie	26
4.3.13	U.13 Kloksynchronisatie	27
4.3.14	U.14 Ontwerpdocumentatie	28
5	Control-domein	29
5.1	Doelstelling	29
5.2	Risico's	29
5.3	Objecten, controls en maatregelen	29
5.3.1	C.01 Evaluatierichtlijnen servers en serverplatforms	29
5.3.2	C.02 Beoordeling technische serveromgeving	30
5.3.3	C.03 Logbestanden beheerders	31
5.3.4	C.04 Registratie gebeurtenissen	32
5.3.5	C.05 Monitoring servers en serverplatforms	32
5.3.6	C.06 Beheersorganisatie servers en serverplatforms	33

1 Inleiding

Dit document bevat een referentiekader voor het thema Serverplatform. Het is geënt op de controls uit de Baseline Informatiebeveiliging Overheid (BIO), die gebaseerd is op de NEN-ISO/IEC 27002: 2017 (hierna genoemd ISO 27002). Er wordt ook gebruik gemaakt van andere best practices zoals: Standard of Good Practice (SoGP) en National Institute en Standard and Technology (NIST).

Dit kader dient evenals andere BIO-thema's als een toetsinstrument voor interne en externe leveranciers, om inzicht te geven over het beveiligings- en beheersingsniveau van haar ontwikkel- en onderhoudsorganisatie. Dit thema geeft tevens inzicht in de kwaliteitszorg die de leverancier dient toe te passen bij het opleveren van nieuwe infrastructuur.

1.1 Opzet van het thema

Het thema Serverplatform wordt achtereenvolgens uitgewerkt langs twee onderdelen: structuur en objecten. De structuur van dit themadocument bestaat uit een indeling op basis van Beleid, Uitvoering en Control (BUC). De objecten vormen de inhoudelijke onderwerpen die in de vorm van controls en onderliggende maatregelen zullen worden behandeld. De objecten en de bijbehorende maatregelen worden gestructureerd met een (BUC-)lagenstructuur.

Dit thema volgt de standaard opzet voor BIO-thema's:

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

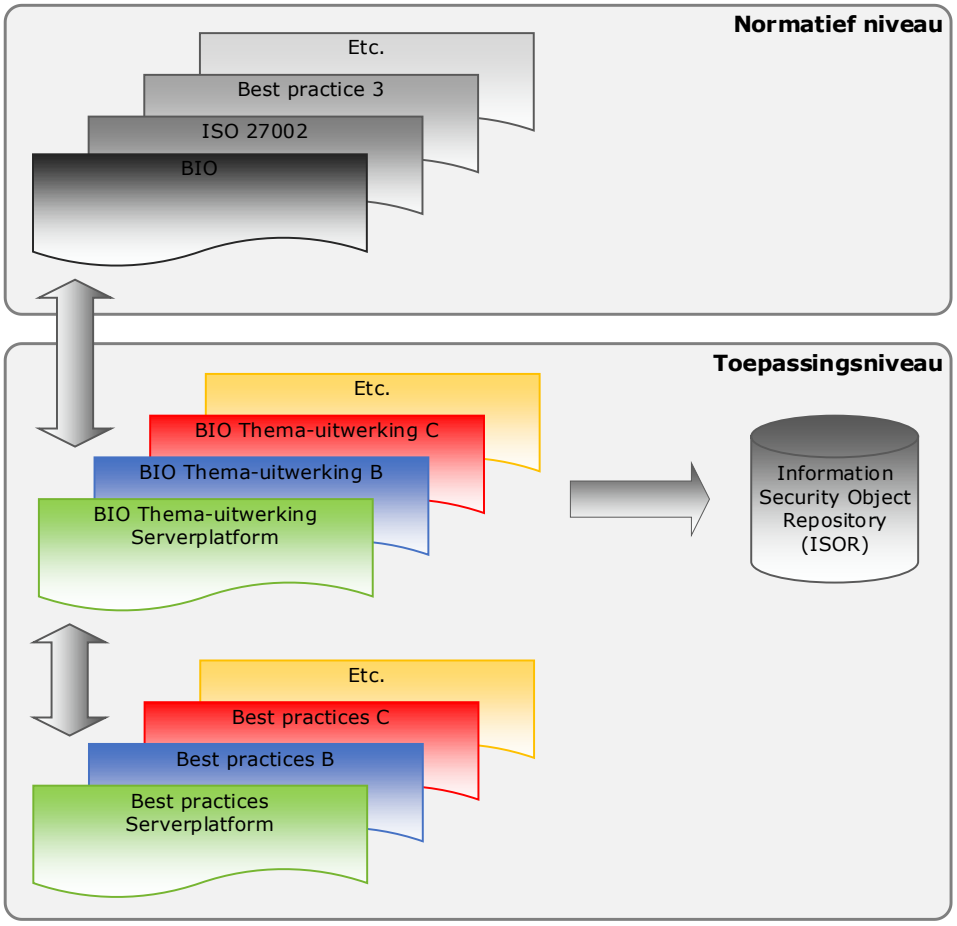
1.2 Scope en begrenzing van serverplatform

In dit thema 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 BIO of andere best practices. De vertaling van de BIO-titel Beleid voor beveiligd ontwikkelen (zie paragraaf 14.2.1) naar het object voor serverplatforms wordt Beleid voor beveiligde inrichting en onderhoud. De BIO-titel Principes voor engineering van beveiligde systemen wordt het object Principes voor inrichten beveiligde servers.

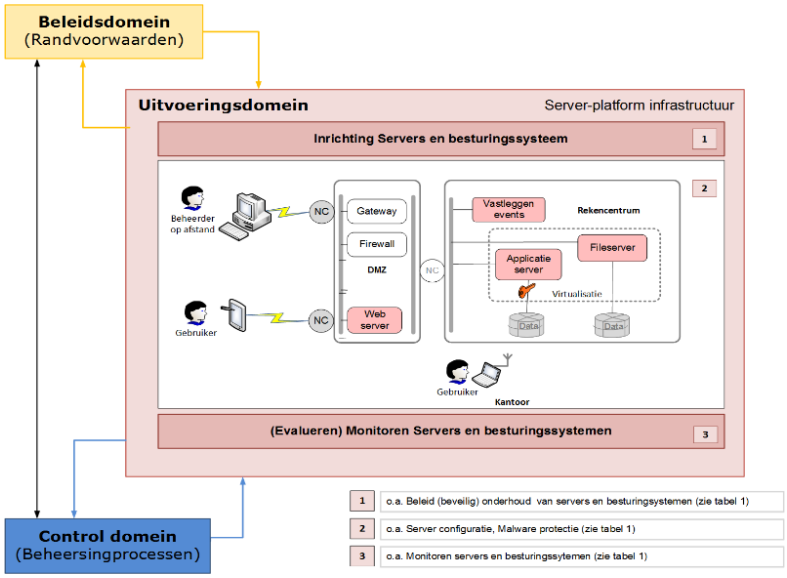
De begrenzing van dit document is in onderstaande afbeelding weergegeven.



Afbeelding 1: Relatie BIO Thema-uitwerking met aanpalende documenten

1.3 Context van 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: accepteert verzoeken van gebruikers en verwerkt deze. Aan een server hangt een of meerdere clients. Afbeelding 2 geeft een globale context van enkele typen servers en hoe ze in relatie staan met beleids- en beheersingsaspecten.



Afbeelding 2: Context van het thema Serverplatform

Een externe gebruiker logt bijvoorbeeld aan op een webserver vanuit het internet. Dit type server geeft de relevante gebruikersgegevens door aan een portal-toegangsserver, die op zijn beurt applicatieve diensten vanuit backoffice-servers beschikbaar stelt. De onderste gebruiker in de afbeelding is een medewerker van een vertrouwde partij en zoekt via een semi-vertrouwd kanaal informatie op een webserver van de partnerorganisatie. De interne gebruiker logt aan op z'n werkstation via het lokale netwerk. In veel gevallen is er ook sprake van 'middleware', oftewel applicatiecode die bepaalde functies vervult tussen de gebruikersapplicatie en het besturingssysteem.

2 Beveiligingsobjecten serverplatform

Objecten worden geïdentificeerd aan de hand van onderzoeksvragen en risicogebieden. De objecten zijn afgeleid vanuit de optiek van de kwaliteitscriteria: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid (BIVC), die vervolgens zijn ingedeeld in drie domein: beleid, uitvoering en control.

De vragen die hierbij een rol hebben gespeeld, zijn:

1. Welke randvoorwaardelijke elementen spelen een rol bij de inrichting van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
2. Welke elementen spelen een rol bij de inrichting van het serverplatform vanuit de optiek van BIVC en wat is de consequentie bij afwezigheid?
3. 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 binnen het uitvoeringsdomein. Die functieblokken bevatten op hun beurt beveiligingsmaatregelen, die vanuit de normatiek geduid worden als beveiligingsobjecten.

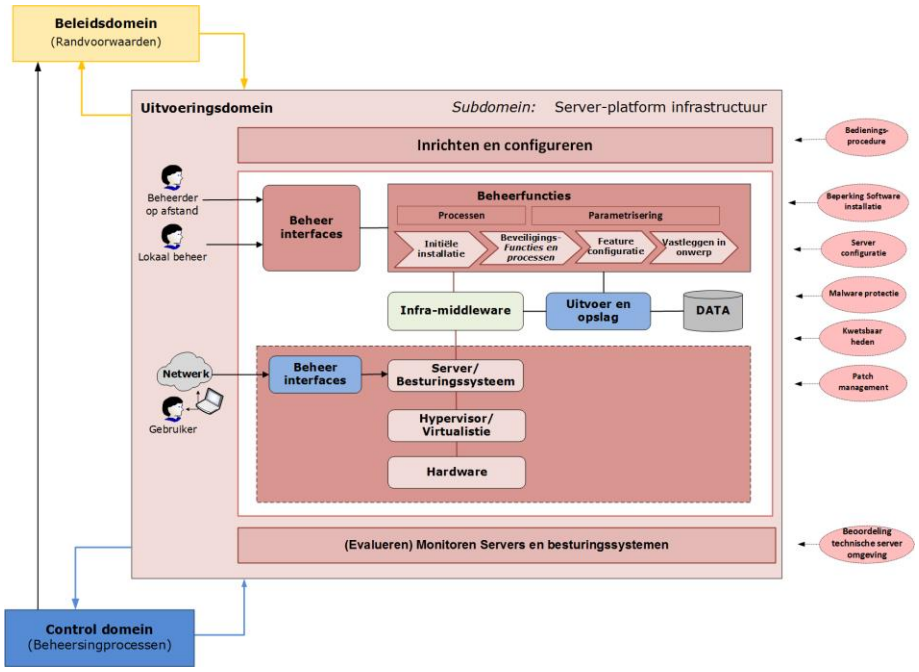
2.1 Vaststellen beveiligingsobjecten voor serverplatform

De afbeeldingen uit hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein geven een overzicht van alle relevante beveiligingsobjecten voor het thema Serverplatform, afkomstig uit de BIO die gebaseerd is op de ISO 27002. De BIO volgt dezelfde hoofdstukindeling en controlteksten.

Uit de contextuele analyse blijkt dat er enkele onderwerpen bestaan die niet in de BIO voorkomen. Voor deze onderwerpen, waarvoor de BIO geen control heeft geformuleerd, worden 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 de beveiligingsobjecten

Het thema Serverplatform omvat het geheel van beleid, richtlijnen, procedures, processen, mensen (actoren), middelen en registraties voor het betrouwbaar functioneren van serverplatforms die het fundament vormen voor 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. Moderne, gevirtualiseerde systeemomgevingen zien er mogelijk qua systeemtopologie geheel anders uit, maar de basiselementen die het fundament vormen voor informatiesystemen zijn niet anders.



Afbeelding 3: Gelaagdheid serverplatform met enkele beveiligingsobjecten

2.2.1 Beleidsdomein

Dit domein geeft de randvoorwaarden, conditionele aspecten en contraints waar de inrichting van het serverplatform aan moet voldoen.

2.2.2 Uitvoeringsdomein

De keuze van objecten uit de ISO 27002 voor het thema Serverplatform vloeit voort uit enkele uitgangspunten die gerelateerd zijn aan serverplatform:

- Initiële installatie
  De initiële installatie wordt uitgevoerd met 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 features. De beheerfunctie is gerelateerd aan enkele processen, zoals: server-onderhoud en beheer van kwetsbaarheden.
- Feature-configuratie
  Servers hebben verschillende features. Deze features moeten adequaat zijn geconfigureerd om het beveiligingsniveau te kunnen garanderen.
- Structuur en ontwerp
  De configuraties van servers en de koppelingen en relatie tussen verschillende servers moet in een ontwerpdocument worden vastgelegd.

2.2.3 Control-domein

Er zijn beoordelingsrichtlijnen vastgesteld voor het evalueren van de vastgestelde randvoorwaarden en de uitvoeringscomponenten.

3 Beleidsdomein

3.1 Doelstelling

De doelstelling van het beleidsdomein is de conditionele elementen te identificeren die randvoorwaardelijk zijn voor het inrichten, beveiligen en beheersen van de serverplatforms. De hiervoor van belang zijnde beveiligingsobjecten en de daaraan gerelateerde maatregel zijn opgenomen.

3.2 Risico's

Als de juiste beleidsaspecten voor de inrichting en het onderhoud van het serverplatform ontbreken, bestaat de kans 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 bestaat er een kans dat er datalekken optreden.

3.3 Objecten, controls en maatregelen

De onderwerpen die specifiek voor serverplatforms een rol spelen, zijn in onderstaande afbeelding vermeld. 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, in dit geval, ook voor in B.01 Beleid voor beveiligde inrichting en onderhoud. Vandaar dat ook in deze kolom geen objecten zijn vermeld.

Afbeelding 4: Overzicht serverplatform-objecten in het beleidsdomein

3.3.1 B.01 Beleid voor beveiligde inrichting en onderhoud

Definitie

Het resultaat van een besluitvorming over het onderhouden van serverplatforms waarin het verantwoordelijke management voor serverplatforms van een organisatie heeft vastgelegd op welke wijze serverplatforms onderhouden dienen te worden.

Toelichting

De ISO 27002 2017 formuleert 'beveiligd ontwikkelen' in paragraaf 14.2.1 'Beleid voor beveiligd ontwikkelen' als een eis voor het opbouwen van een beveiligde dienstverlening, software, systemen en architectuur.

In dit thema wordt bij het object 'Beleid voor beveiligde inrichting en onderhoud' inrichtings- en onderhoudsaspecten van serverplatform benadrukt. In het beleid worden onder andere standaarden en procedures beschreven voor het beveiligd inrichten en onderhouden van servers.

Doelstelling	Het beheersen van de beveiligde inrichting en onderhoud van het serverplatform.		
Risico	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.		BIO 2019: 14.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	De gangbare principes rondom 'security by design' zijn uitgangspunt voor het onderhouden van servers.	BIO 2019: 14.2.1.1
	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 Principes voor inrichten beveiligde servers

Definitie

Principiële uitgangspunten voor het inrichten van servers en serverplatforms, zoals:
'security by design' en 'defence in depth'.

Toelichting

Bij het inrichten van een beveiligde server behoren beveiligingsprincipes in acht te worden genomen. In de standaard ISO 27002 2017 zijn twee principes expliciet genoemd: 'security by design' en 'defence in depth'. 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.		BIO 2019: 14.2.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Principes	1.	De gangbare principes rondom 'security by design' zijn uitgangspunt voor het inrichten van servers.	BIO 2019: 14.2.1.1
	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

Definitie

Raamwerken of blauwdrukken waarmee wordt aangegeven op welke wijze serverplatforms zijn ingericht, samenhangen, beveiligd en beheerst.

Toelichting

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 en samenwerking van beveiligingsmaatregelen. In de architectuur zijn gemaakte ontwerp- en inrichtingskeuzen gedocumenteerd, 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 en oude documentatie moet worden gearchiveerd.

Doelstelling	Een landschap bieden voor een serverplatform dat in samenhang beveiligd is en inzicht geeft in de inrichting van het serverplatform.		
Risico	Onvoldoende sturing hebben 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 800-53 rev.5 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.

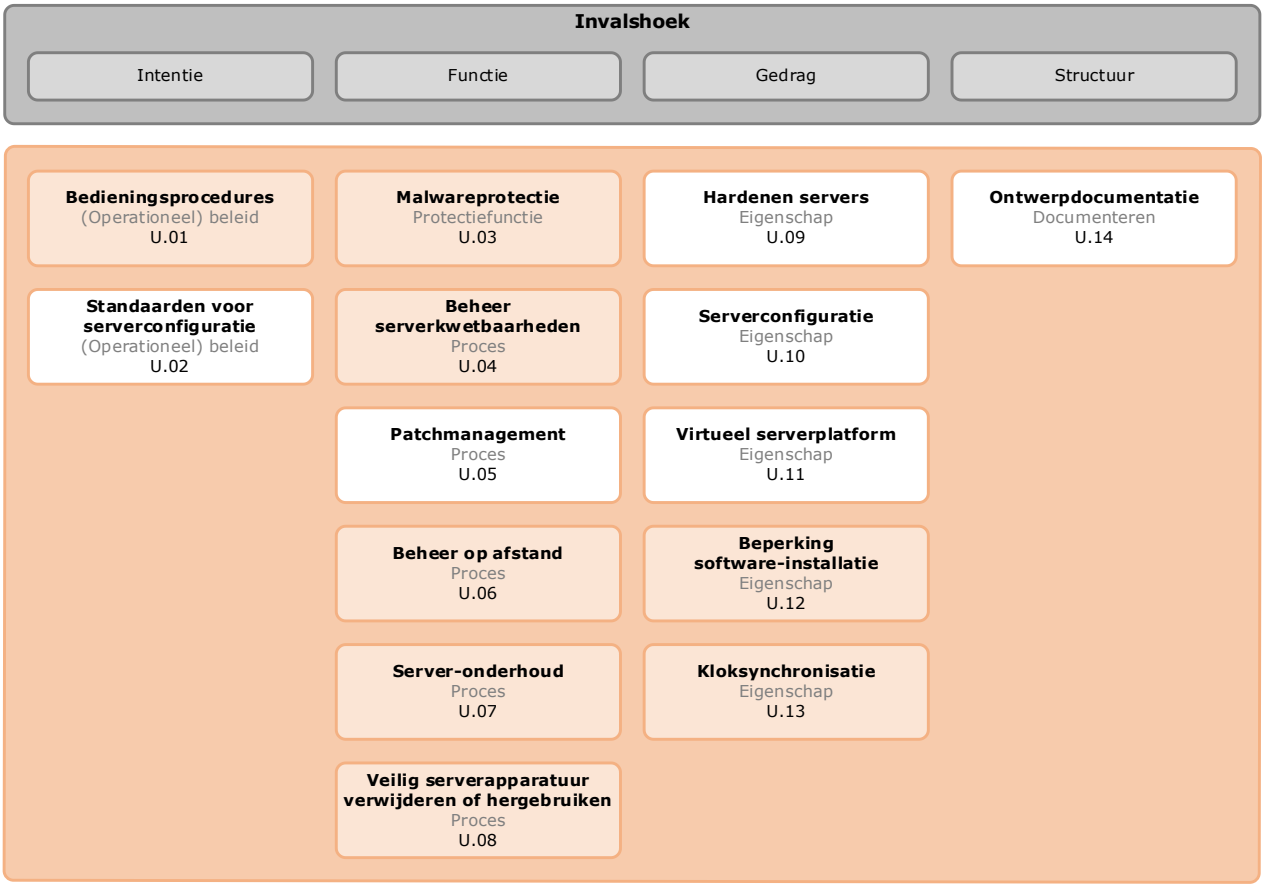
Wanneer meer functionaliteit is ingeschakeld dan nodig is voor de bedrijfsvoering nemen risico's van diefstal of inbreuk toe.

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

Hiaten 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 onderwerpen die specifiek voor het serverplatform een rol spelen, zijn in afbeelding 6 vermeld.



Afbeelding 5: Overzicht serverplatform-objecten in het uitvoeringsdomein

4.3.1 U.01 Bedieningsprocedures

Definitie

Een reeks verbonden taken of activiteiten die noodzakelijk zijn voor het beheren van serverplatforms.

Toelichting

Bedieningsprocedures zijn een reeks verbonden taken of activiteiten die noodzakelijk zijn voor het beheren van serverplatforms. De activiteiten kunnen gerelateerd zijn aan het starten en afsluiten van de computer, 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 en verlies van kennis voor het bedienen van serverplatforms.		
Control	**Bedieningsprocedures** behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.		BIO 2019: 12.1.1
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 2017: 12.1.1
	2.	Wijzigingen aan bedieningsprocedures voor systeemactiviteiten worden formeel door het hoger management goedgekeurd.	ISO 27002 2017: 12.1.1
	3.	In de bedieningsprocedures zijn de bedieningsvoorschriften opgenomen, onder andere voor: • de installatie en configuratie van systemen; • de verwerking en behandeling van informatie, zowel geautomatiseerd als handmatig; • de back-up; • de eisen voor de planning, met inbegrip van onderlinge verbondenheid met andere systemen; • de voorschriften voor de afhandeling van fouten of andere uitzonderlijke omstandigheden die tijdens de uitvoering van de taak kunnen optreden, waaronder beperkingen van het gebruik van systeemhulpmiddelen; • de ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten door onverwachte bedienings- of technische moeilijkheden; • het beheer van audit- en systeemlogbestandinformatie; • de procedures voor het monitoren van activiteiten.	ISO 27002 2017: 12.1.1a t/m f, i en j

4.3.2 U.02 Standaarden voor serverconfiguratie

Definitie

Documenten waarin afspraken zijn vastgelegd over configuraties en parametrisering van serverinstellingen.

Toelichting

Standaarden voor de configuratie van servers representeren documenten waarin afspraken zijn vastgelegd voor configuraties en parametrisering van serverinstellingen.

Doelstelling	Dat een serverplatform correct werkt met de vereiste beveiligingsinstellingen, dat de configuratie niet wordt gewijzigd door ongeautoriseerden en het voorkomen van onjuiste wijzigingen.		
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 conform 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

Definitie

Beschermingsmechanismen om servers te beschermen tegen schadelijke code en om schadelijke code te detecteren en te neutraliseren.

Toelichting

De organisatie maakt gebruik van malwareprotectie bij ingangs- en uitgangspunten van kritieke informatiesystemen (zoals firewalls, e-mailservers, webservers, proxyservers, servers met externe toegang) en op werkstations, servers of 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 en 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.		BIO 2019: 12.2.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Preventie	1.	Een formeel beleid wordt toegepast waarin het ongeautoriseerde gebruik van software is verboden.	ISO 27002 2017: 12.2.1a
	2.	Procedures zijn beschreven en verantwoordelijkheden benoemd voor de bescherming tegen malware.	ISO 27002 2017: 12.2.1h
	3.	Severs zijn voorzien van (actuele) software die malware opspoort en daartegen beschermt.	ISO 27002 2017: 12.2.1g
	4.	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	BIO 2019: 12.2.1.2
	5.	Het downloaden van bestanden is beheerst en beperkt op basis van een risicoanalyse en het principe 'need-of-use'.	BIO 2019: 12.2.1.1
Detectie	6.	Servers en hiervoor gebruikte media worden als voorzorgsmaatregel routinematig gescand op malware. De uitgevoerde scan omvat alle bestanden die op de server moeten worden opgeslagen.	BIO 2019: 12.2.1.4
	7.	De malware-scan wordt op alle omgevingen uitgevoerd.	BIO 2019: 12.2.1.5
Herstel	8.	De gebruikte anti-malwaresoftware en bijbehorende herstelsoftware zijn actueel en worden ondersteund door periodieke updates.	BIO 2019: 12.2.1.3

4.3.4 U.04 Beheer serverkwetsbaarheden

Definitie

Proactieve beveiliging van servers door het verwerven van inzicht in de kwetsbaarheden en zwakheden in de software die op de server zijn geïnstalleerd.

Toelichting

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 huidige stand van zaken, tast de beheerder in het duister en kan hij 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 12.6.1) behandelt wat betreft de maatregelen twee onderwerpen:

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

In dit thema worden deze twee onderwerpen apart beschreven.

Doelstelling	Het voorkomen van misbruik van technische kwetsbaarheden en bij blootstelling ervan tijdig passende maatregelen treffen.		
Risico	Kwetsbaarheden in servers worden niet opgemerkt, waardoor er misbruik van gemaakt kan worden.		
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.		BIO 2019: 12.6.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Technische serverkwets-baarheden	1.	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC-classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	BIO 2019: 12.6.1.1
	2.	Voor een doeltreffende kwetsbaarhedenanalyse van serverplatforms en servers is informatie aanwezig over beschikbaarheid van: • (onderlinge) afhankelijkheden; • software ten aanzien van versienummers en toepassingsstatus; • verantwoordelijken voor de software.	ISO 27002 2017: 12.6.1
	3.	Om een doeltreffend beheerproces voor technische kwetsbaarheden vast te stellen, zijn: • de rollen en verantwoordelijkheden in samenhang met beheer van technische kwetsbaarheden vastgesteld; • de middelen om technische kwetsbaarheden te bepalen, vastgesteld.	ISO 27002 2017: 12.6.1a
	4.	Voor de technische kwetsbaarheden zijn voor een doeltreffend beheerproces de activiteiten afgestemd op het incidentbeheerproces.	ISO 27002 2017: 12.6.1k

[1] Zie Handreiking: 4.42 Penetratietesten

	5.	Het kwetsbaarhedenbeheerproces wordt uitgevoerd voor: • de identificatie van bekende technische kwetsbaarheden; • een hoog-over-inzicht in de kwetsbaarheden in de technische infrastructuur van de organisatie; • de relevantie, gericht op de mate waarin het serverplatform en de servers kunnen worden blootgesteld aan bedreigingen; • het prioriteit geven aan herstel van onderkende kwetsbaarheden.	SoGP 2018: TM1.1.6
	6.	Technische kwetsbaarheden worden via de patchmanagementprocessen en/of het wijzigingsbeheer hersteld.	SoGP 2018: TM1.1.9
Geëvalueerd	7.	Het kwetsbaarhedenbeheerproces wordt regelmatig gemonitord en geëvalueerd.	ISO 27002 2017: 12.6.1i

4.3.5 U.05 Patchmanagement

Definitie

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.

Toelichting

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 software.

De noodzaak van het patchen staat vaak niet ter discussie. Vaak ontstaat echter wel discussie over de urgentie waarmee patches moeten worden uitgevoerd. De ernst van de kwetsbaarheid bepaalt de noodzaak om de tijdsduur tussen het uitkomen van een patch en het implementeren van een patch zo kort mogelijk te houden. Daarom is het van belang vast te stellen welke doelstelling en prioriteit met patchmanagement worden nagestreefd. 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, zodat inzicht bestaat over het al of niet uitvoeren van de patch op deze systemen.

Doelstelling	Het zekerstellen dat kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Risico	De stabiliteit en betrouwbaarheid van servers komt in gevaar.	
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
	3.	Configuratiebeheer geeft het inzicht waarmee servers worden gepatcht.	CIP
	4.	Het patchbeheerproces bevat methoden om: • patches te testen en te evalueren voordat ze worden geïnstalleerd; • patches te implementeren op servers die niet toegankelijk zijn via het bedrijfsnetwerk; • om te gaan met mislukte of niet uitgevoerde patches; • te rapporteren over de status van het implementeren van patches; • acties te bepalen als een technische kwetsbaarheid niet met een patch kan worden hersteld of een beschikbare patch niet kan worden aangebracht.	ISO 27002 2017: 12.6.1g SoGP 2018: TM1.1.10
Procedureel	5.	De patchmanagementprocedure is actueel en beschikbaar.	CIP
	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
	10.	De risico's die verbonden zijn aan het installeren van de patch worden beoordeeld (de risico's die worden gevormd door de kwetsbaarheid worden vergeleken met het risico van het installeren van de patch).	ISO 27002 2017: 12.6.1d
	11.	Wanneer voor een gepubliceerde technische kwetsbaarheid geen patch beschikbaar is, worden andere beheersmaatregelen overwogen, zoals: • het uitschakelen van functionaliteit of diensten; • het aanpassen of toevoegen van toegangsbeveiligingsmaatregelen, bijvoorbeeld firewalls, rond de grenzen van netwerken; • het vaker monitoren om de werkelijke aanvallen op te sporen; • het kweken van bewustzijn over de kwetsbaarheid.	ISO 27002 2017: 12.6.1g

4.3.6 U.06 Beheer op afstand

Definitie

Het beheer van servers door beheerders vanuit een niet-vertrouwde omgeving.

Toelichting

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

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

Doelstelling	Voorkomen van verlies, schade, diefstal of in gevaar brengen van informatie en andere bijbehorende assets en onderbreking van de activiteiten van de organisatie.		
Risico	De server is onbetrouwbaar en functioneert niet naar behoren.		
Control	**Richtlijnen** en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.		BIO 2019: 6.2.2
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
	5.	Alle externe toegang tot servers vindt versleuteld plaats.	CIP

4.3.7 U.07 Server-onderhoud

Definitie

Het actualiseren van configuraties van een serverplatform binnen een tijdsinterval.

Toelichting

In dit thema wordt apparatuur vanuit de ISO 27002 2017 opgevat als het 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 continue beschikbare en integere servers.		
Risico	Aantasting van de beschikbaarheid en integriteit van servers.		
Control	Servers behoren correct te worden **onderhouden** om de continue beschikbaarheid en integriteit te waarborgen.		BIO 2019: 11.2.4
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Onderhouden	1.	Het onderhoud van servers wordt uitgevoerd met richtlijnen die invulling geven aan de volgende eisen: • Onderhoud wordt uitgevoerd volgens de door de leverancier aanbevolen intervallen voor servicebeurten. • Alleen bevoegd onderhoudspersoneel voert reparaties en onderhoudsbeurten uit. • Van alle vermeende en daadwerkelijke fouten en van al het preventieve en correctieve onderhoud wordt een registratie bijgehouden. • Voor onderhoud vanuit interne of externe locaties worden passende maatregelen getroffen. • Voordat servers na onderhoud weer in bedrijf worden gesteld, vindt een inspectie plaats om te waarborgen dat niet is geknoeid met de server en dat deze nog steeds of weer goed functioneert.	ISO 27002 2017: 11.2.4a t/m d en f

4.3.8 U.08 Veilig serverapparatuur verwijderen of hergebruiken

Definitie

Het opschonen van apparatuur en het veilig stellen van data op de apparatuur.

Toelichting

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

Doelstelling	Het waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.		
Risico	Informatie met een vertrouwelijk karakter komt in handen van onbevoegden.		
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.		BIO 2019: 11.2.7
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Opslagmedia	1.	Van de server(s): • wordt informatie die niet meer nodig is, vernietigd door verwijderen of overschrijven, gebruikmakend van technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen; • worden opslagmedia die niet meer nodig zijn en die vertrouwelijke of door auteursrecht beschermde informatie bevatten fysiek vernietigd.	ISO 27002 2017: 11.2.7
Geverifieerd	2.	Voorafgaand aan verwijdering of hergebruik van servers wordt gecontroleerd of de server opslagmedia bevat en of de informatie is vernietigd.	ISO 27002 2017: 11.2.7

4.3.9 U.09 Hardenen servers

Definitie

Het proces van het uitschakelen of verwijderen van overbodige en/of niet gebruikte functies, services en accounts, waarmee de beveiliging wordt verbeterd.

Toelichting

De standaardconfiguratie van de meeste besturingssystemen is niet ontworpen met beveiliging als de 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	Misbruik van overbodige en/of niet gebruikte functies, services en accounts.

Control	Voor het beveiligen van servers 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.	Servers zijn 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.	Servers zijn 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.	Servers worden beschermd tegen ongeoorloofde toegang doordat:
		• onnodige of onveilige gebruikersaccounts zijn verwijderd;
		• belangrijke beveiliging gerelateerde parameters 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

Definitie

Het configureren van verschillende features van een server of serverplatform.

Toelichting

Serverplatforms hebben verschillende features en bieden een veelheid van functies om services te kunnen leveren. Om serverplatforms veilig te laten functioneren, behoort elk serverplatform conform 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 Virtueel serverplatform

Definitie

Het beschikbaar stellen van een of meer gescheiden 'logische' omgevingen op één fysieke server of serverplatform.

Toelichting

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	Dat onbevoegden inzicht krijgen 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 vertrouwelijkheidseisen en om te voorkomen dat informatie wordt uitgewisseld tussen discrete omgevingen; • de communicatie tussen virtuele servers te coderen; • de toegang te beperken tot een beperkt aantal geautoriseerde personen; • de rollen van hypervisoradministrators te scheiden.	SoGP 2018: SY1.3.5
Virtuele servers	3.	Virtuele servers worden ingezet, geconfigureerd en onderhouden conform standaarden en procedures, die de bescherming omvat 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

Definitie

Het stellen van regels aan het installeren van servers en serverplatforms.

Toelichting

Voor het gebruik van software (door een beheerder) op een server zijn regels opgesteld.

Doelstelling	Het voorkomen dat er software wordt geïnstalleerd die schade kan veroorzaken, zoals het weglekken van informatie, verlies van integriteit, andere informatiebeveiligingsincidenten of het schenden van intellectuele-eigendomsrechten.
Risico	Het introduceren van kwetsbaarheden.

Control	Voor het door gebruikers (beheerders) installeren van software behoren **regels** te worden vastgesteld en te worden geïmplementeerd.		BIO 2019: 12.6.2
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels	1.	Gebruikers (beheerders) kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	BIO 2019: 12.6.2.1
	2.	De organisatie past een strikt beleid toe voor het installeren en gebruiken van software.	ISO 27002 2017: 12.6.2
	3.	Het principe van least-privilege wordt toegepast.	ISO 27002 2017: 12.6.2
	4.	De rechten van beheerders worden verleend op basis van rollen.	ISO 27002 2017: 12.6.2

4.3.13 U.13 Kloksynchronisatie

Definitie

Het gelijkrichten van klokken op verschillende servers.

Toelichting

Om gebeurtenissen uit verschillende componenten te correleren, worden de klokken van de verschillende systemen gelijkgericht en waarmee de timestamps van gebeurtenissen zijn gesynchroniseerd. Dit synchroniseren is het effect van de juiste instelling van tijd op betreffende componenten.

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	Om de correlatie en analyse van beveiligingsgerelateerde gebeurtenissen en andere geregistreerde gegevens mogelijk te maken en om onderzoeken naar informatiebeveiligingsincidenten te ondersteunen.		
Risico	Onnauwkeurige auditlogbestanden niet kunnen onderzoeken of als bewijs in juridische of disciplinaire zaken belemmeren en de geloofwaardigheid van dat bewijsmateriaal schaden.		
Control	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden **gedocumenteerd** en **gesynchroniseerd** met één referentietijdbron.		BIO 2019: 12.4.4
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gedocumen-teerd	1.	De systemen zijn met een standaard referentietijd voor gebruik geconfigureerd, zodanig dat gebruik gemaakt wordt van een consistente en vertrouwde datum- en tijdbron en dat gebeurtenislogboeken nauwkeurige tijdstempels gebruiken.	ISO 27002 2017: 12.4.4 SoGP 2018: TM1.2.3
Gesynchroni-seerd	2.	De interne en externe eisen voor weergave, synchronisatie en nauwkeurigheid van tijd en de aanpak van de organisatie om een referentietijd met externe bron(nen) te verkrijgen en hoe de interne klokken betrouwbaar te synchroniseren zijn gedocumenteerd.	ISO 27002 2017: 12.4.4

4.3.14 U.14 Ontwerpdocumentatie

Definitie

Een document waarin de relatie tussen servers en de instellingen van configuraties zijn vastgelegd.

Toelichting

De relatie tussen servers en de instellingen van configuraties moet zijn vastgelegd in een ontwerpdocument.

Doelstelling	Het hebben van een middel waarmee de vereiste acties genomen kunnen worden in de volgende fase, de inrichting van de server en het serverplatform. Inzichtelijk is waar wel en niet rekening mee is gehouden in het ontwerp.		
Risico	De inrichting van de server en het serverplatform wijkt af van wat vooraf nodig is geacht.		
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 beschreven is: • dat in het ontwerp rekening is gehouden met de principes van de beveiligingsarchitectuur en beveiligingsvereisten; • dat in het ontwerp rekening is gehouden met 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

Doelstelling van het control-domein is om vast te stellen of:

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

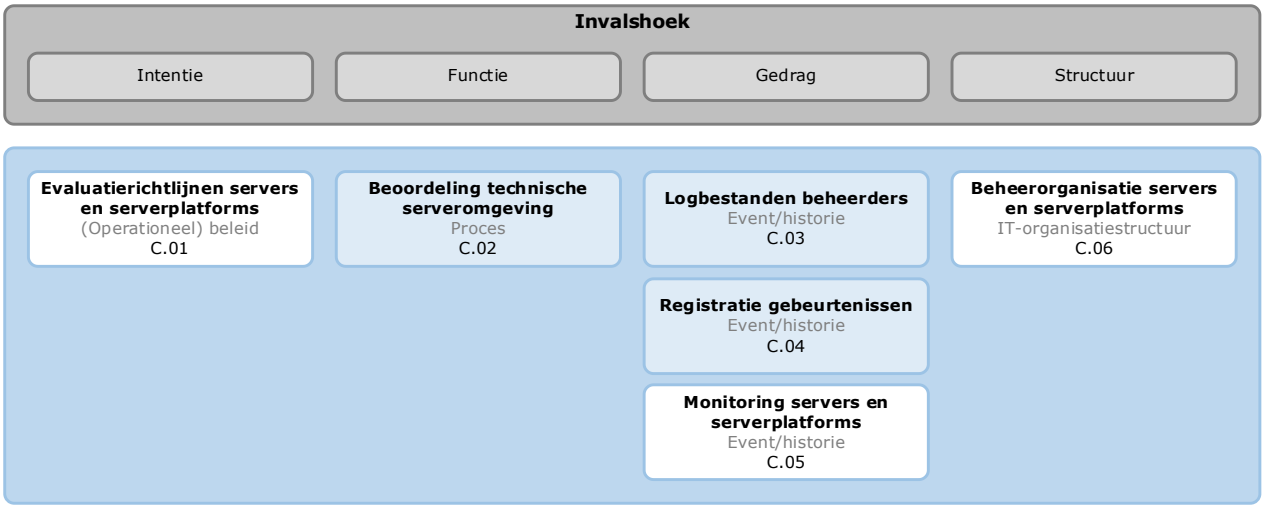
Dit houdt onder meer in dat binnen de organisatie een adequate beheerorganisatie moet zijn ingericht, waarin beheerprocessen zijn vormgegeven.

5.2 Risico's

Door het ontbreken van noodzakelijke maatregelen binnen de organisatie van de IT-leverancier is het niet zeker of de ontwikkel- en onderhoudsadministratie aan de beoogde organisatorische en beveiligingsvoorwaarden voldoet 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 in onderstaande afbeelding vermeld.



Afbeelding 6: Overzicht serverplatform-objecten binnen het control-domein

5.3.1 C.01 Evaluatierichtlijnen servers en serverplatforms

Definitie

Richtlijnen die evaluatie-activiteiten van servers en serverplatforms ondersteunen.

Toelichting

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. Het is van groot belang dat deze servers en besturingssystemen vanwege risicomanagement, periodiek geëvalueerd worden. De evaluatie-activiteiten dienen ondersteund te worden met evaluatierichtlijnen, procedures en instructies. Anders bestaat het risico dat de resultaten van deze controle-activiteiten niet voldoen aan de verwachte eisen. De beheerorganisatiestructuur geeft de samenhang van de ingerichte processen weer.

Doelstelling	Het adequaat controle-activiteiten en rapportages opstellen 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.		ISO 27002 2007: 10.10.2
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
	2.	De organisatie beschikt over geautomatiseerde middelen voor effectieve ondersteuning van de controle-activiteiten.	CIP
	3.	De organisatie beschikt over richtlijnen voor het uitvoeren van registratie, statusmeting, analyse, rapportage en evaluatie.	CIP
	4.	De organisatie heeft de taken, verantwoordelijkheden en bevoegdheden van controle-functionarissen vastgelegd.	CIP

5.3.2 C.02 Beoordeling technische serveromgeving

Definitie

Het proces van evalueren van de serveromgeving.

Toelichting

Het is noodzakelijk om de technische omgeving regelmatig te beoordelen om de beveiliging doeltreffend te kunnen beheersen. Hiertoe dienen periodiek zowel de organisatorische als technische aspecten beoordeeld te worden, zoals: de toepassing van het geformuleerd inrichtingsbeleid voor servers, serverplatformarchitectuur, taken en verantwoordelijkheden, gebruik van technische middelen, frequentie, controle aanpak en 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.		BIO 2019: 18.2.3
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Naleving	1.	Technische naleving wordt bij voorkeur beoordeeld met geautomatiseerde instrumenten die technische rapporten vervaardigen en geïnterpreteerd door een technisch specialist.	ISO 27002 2017: 18.2.3
	2.	Periodiek worden, na verkregen toestemming van het management, penetratietests of kwetsbaarheidsbeoordelingen uitgevoerd.	ISO 27002 2017: 18.2.3
	3.	De uitvoering van dergelijke tests worden gepland en gedocumenteerd en zijn herhaalbaar.	ISO 27002 2017: 18.2.3
	4.	Beoordeling van technische naleving wordt uitsluitend uitgevoerd door competente en bevoegde personen of onder toezicht van het management.	ISO 27002 2017: 18.2.3

5.3.3 C.03 Logbestanden beheerders

Definitie

Bestanden waarin de activiteiten van beheerders worden vastgelegd.

Toelichting

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

Doelstelling	Achteraf kunnen fouten en/of onrechtmatigheden in het gebruik van waaronder ongeautoriseerde toegangspogingen tot technische componenten vroegtijdig worden gesignaleerd.		
Risico	Schade door het niet opmerkingen van fouten en/of onrechtmatigheden in het gebruik van 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.		BIO 2019: 12.4.3
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.	ISO 27002 2017: 12.4.3

	2.	Speciale gebruikers geven rekenschap over de door hun uitgevoerde beheeractiviteiten.	ISO 27002 2017: 12.4.3

5.3.4 C.04 Registratie gebeurtenissen

Definitie

Het proces van registreren van gebeurtenissen op een server vanuit beveiligingsoptiek.

Toelichting

Op de servers en besturingssystemen vinden automatische en handmatige activiteiten plaats. Vanuit beveiligingsoptiek is het van belang om deze activiteiten te registreren in logboeken 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. Bij wel opmerken, is er geen bewijs voorhanden.		
Control	**Logbestanden** van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.		BIO 2019: 12.4.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Logbestanden	1.	Logbestanden van gebeurtenissen bevatten, voor zover relevant: • gebruikersidentificaties; • systeemactiviteiten; • data, tijdstippen en details van belangrijke gebeurtenissen zoals de registratie van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem en tot bronnen van informatie; • identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie; • systeemconfiguratieveranderingen; • gebruik van speciale bevoegdheden; • alarmen die worden afgegeven door het toegangsbeveiligingssysteem; • activering en de-activering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen; • verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd.	ISO 27002 2017: 12.4.1a t/m e, g, h, l, m en n

5.3.5 C.05 Monitoring servers en serverplatforms

Definitie

Het proces van bewaken, reviewen en analyseren van vastgelegde gebeurtenissen en het rapporteren hierover.

Toelichting

Onder monitoren wordt verstaan: reviewen, analyseren en rapporteren. Het monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot servers en serverplatforms tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringsfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris. Monitoring vindt mede plaats met 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 waarmee het management tijdig kan bijsturen.		
Risico	Onvoldoende mogelijkheden om tijdig bij te sturen om organisatorisch en technisch te (blijven) voldoen aan de doelstellingen.		
Control	De organisatie **reviewt/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
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Reviewt/ 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 verantwoordelijk management.	NCSC 2015: C.07.09
	6.	De eindrapportage bevat, op basis van analyses, verbetervoorstellen.	CIP

5.3.6 C.06 Beheersorganisatie servers en serverplatforms

Definitie

Een organisatorische eenheid die verantwoordelijk is voor de beheersing van de servers en serverplatformomgeving en die adequaat is gepositioneerd.

Toelichting

Voor het adequaat beheersen en beheren van servers en serverplatforms zou een beheersorganisatiestructuur moeten zijn vastgesteld, waarin de verantwoordelijkheden voor de beheersprocessen met toereikende bevoegdheden zijn uitgedrukt en op het juiste niveau zijn gepositioneerd.

Doelstelling	Het invullen, coördineren en borgen van de beheersing van servers en serverplatforms.		
Risico	De beheersorganisatie is niet effectief ingericht waardoor servers en serverplatforms onvoldoende zijn 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
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
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