Informatieclassificatie Vlaamse overheid (Vo-ICR)

Netwerken

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen netwerken. Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 2 delen. Eerst worden de minimale maatregelen besproken, alvorens in het 2de deel al de nodige aanvullende informatie ter beschikking wordt gesteld.

De organisatie van de maatregelen in het kader van informatieclassificatie wordt beschreven in het document 'Vo informatieclassificatie – Organisatie - Informatieclassificatieraamwerk'.

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

	Datum	Auteur	Opmerkingen
v.1.0	4 april 2019	Kristel VAN AKEN	Publicatie
v.1.1	16 April 2019	Kristel VAN AKEN	Versie gepubliceerd in pdf
v.1.2	1 oktober 2020	Kristel VAN AKEN	Integriteit toegevoegd
v.1.3	11 oktober 2021	Kristel VAN AKEN	Virtuele netwerken toegevoegd Beschikbaarheid toegevoegd
v.2.0	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid en document gesplitst in 'Netwerken' en 'ICT-systemen'' Geen inhoudelijke wijzigingen
v.2.1	17 oktober 2023	Nele Lowet	Update KSZ

Bronnen en verwijzingen

De inhoud van dit document werd samengesteld op basis van volgende documenten:

Documentverwijzingen:

- *Vo Informatieclassificatie – Organisatie Informatieveiligheid* (PDF)
- *Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk* (PDF)
- Vo Informatieclassificatie – Minimale maatregelen (PDF)
  - *Vo Informatieclassificatie - Minimale maatregelen – Cryptografie*
  - *Vo Informatieclassificatie - Minimale maatregelen - fysische maatregelen*
  - *Vo Informatieclassificatie - Minimale maatregelen – IAM*
  - *Vo Informatieclassificatie - Minimale maatregelen – PAM*
  - *Vo Informatieclassificatie - Minimale maatregelen – SIEM*
- Vo Informatieclassificatie – Overzicht baseline maatregelen (XLS) (Klik hier)

De laatste versies van deze documenten zijn te raadplegen op vlaanderen.be.

Inhoudsopgave

INLEIDING

Netwerken zijn niet meer weg te denken uit een organisatie. Netwerken zijn ontstaan uit de behoefte om informatie van de ene computer over te brengen op de andere. Daarnaast is het delen van randapparatuur zoals printers een belangrijke drijfveer voor het opzetten van netwerken.

De belangrijkste functies van een netwerk zijn:

- Uitwisselen en delen van informatie;
- Faciliteren van het centraal opslaan van informatie;
- Beveiligen van informatie tijdens het transport;
- Ter beschikking stellen van gedeelde apparatuur;
- Ter beschikking stellen van software; en
- Mogelijk maken van communicatie tussen gebruikers.

Er zijn verschillende criteria om een netwerk te definiëren:

- **Target**: Er kan sprake zijn van een intern netwerk, een extern netwerk of een hybride vorm van beide. Verschillende netwerken zijn vaak ook gekoppeld, waarbij men moet uitgaan van het laagste beveiligingsniveau. Zo zal een gebruikerscomputer als zwakste schakel in een anderzijds hoog beveiligd netwerk het uiteindelijke beveiligingsniveau bepalen. Daarnaast moet men ook rekening houden met de huidige trends van virtualisatie en gebruik van cloudoplossingen, waardoor fysieke grenzen vervagen. Waar voorheen fysieke beveiligingsmaatregelen een flink deel uitmaakten van het totaalpakket aan beveiliging, is dit niet meer afdoende aangezien grenzen meer en meer verdwijnen. Denk hierbij ook aan werken op afstand bijvoorbeeld telewerken en beheer op afstand,
- **Functioneel**: Verschillende netwerken of netwerkzones hebben verschillende functies. Vaak is er sprake van DMZ (*demilitarized zone*), segment voor de werkplek, het *serversegment*, segment voor IoT (*Internet of Things*), waar ook het printernetwerk en apparatuur voor beheer en beveiliging van gebouwen (bv. camera's, elektronische toegangspoorten, …) toe behoren, out-of-band-segment voor beheer van apparatuur, en
- **Fysiek**: netwerken worden bekabeld of draadloos opgezet. Van het laatste zijn wifi en bluetooth bekende voorbeelden.

Vele maatregelen zijn inzetbaar op netwerkniveau én op systeemniveau (host). Zo zijn er *netwerk-firewalls* en *host-based-firewalls*, netwerk-IDS/IP*S* (*Intrusion Detection Systems*/ *Intrusion Prevention Systems*) en *host-based*-IDS/IPS. In dit document worden enkel netwerk gebaseerde oplossingen besproken, maar systeem gebaseerde maatregelen kunnen nodig zijn om restrisico's op het netwerk te mitigeren via de *host* (gastheer).

Meer informatie is te vinden in '[Vo Informatieclassificatie – minimale maatregelen – ICT-systemen]'.

1. MINIMALE MAATREGELEN

De minimale maatregelen voor netwerken hebben enkel betrekking op de netwerkcomponenten. We onderscheiden:

- **Passieve componenten**: deze componenten hebben geen elektrische stroom nodig om te kunnen functioneren, voorbeelden zijn een netwerkkabel, connector of *patch*-panelen;
- **Actieve componenten**: deze netwerkcomponenten kunnen enkel werken als ze voorzien zijn van elektrische stroom (aan het net geschakeld of via een batterij), voorbeelden zijn *switches*, *routers*, *hubs*, *repeaters*.
  - Intelligente actieve componenten: dit zijn alle componenten met ingebouwde rekencapaciteit, een processor zeg maar, waardoor ze geprogrammeerd kunnen worden om bepaalde taken uit te voeren. Deze categorie omvat de meeste hedendaagse netwerkcomponenten.
  - Niet-intelligente actieve componenten: deze componenten hebben geen processor en dus geen interne rekencapaciteit, voorbeelden zijn (niet-intelligente) *hubs* en *repeaters*.
  - Intelligente actieve componenten waarop een *security policy* wordt afgedwongen: deze componenten nemen acties op basis van een *security policy*, een set paramaters, vaak aangestuurd door een centrale *policy server* die bepaalt hoe de component handelt, voorbeelden zijn *firewalls*, *antimalware*.
- **Componenten voor beheerstaken**: dit zijn componenten, vaak geïnstalleerd op *servers* van waaruit centraal een aantal netwerk toestellen worden beheerd. Dit houdt taken in zoals configureren, uitvoeren van wijzigingen, opstellen en verspreiden van *policies*, beheren van loginformatie, installeren van *patches* en nieuwe versies, enz.

De minimale maatregelen in volgende hoofdstukken gelden dus enkel voor deze netwerkcomponenten, en niet voor de andere apparatuur die deel uitmaakt van een netwerk (gebruikersapparatuur zoals desktops en laptops, *servers* met zakelijke en andere toepassingen, enz.), behalve wanneer het gaat over de plaatsing van deze apparatuur in het netwerk of wanneer dit uitdrukkelijk is vermeld.

We onderscheiden publieke en niet-publieke netwerken:

- **Publieke netwerken**: deze netwerken bevatten datastromen die niet onder het beleid van de organisatie vallen. Voorbeelden zijn het internet, publieke *cloud*-netwerken, partner-netwerken. Het beheer van zulke netwerken kan eventueel uitbesteed worden; en
- **Niet-publieke netwerken**: deze netwerken vallen volledig onder het beleid van de organisatie, en enkel datastromen conform dit beleid zijn toegelaten. De organisatie is dan ook verantwoordelijk en aansprakelijk voor deze netwerken.

Dit document beschrijft enkel de maatregelen voor netwerken, ICT-systemen en gebruikersapparatuur zitten niet in de scope van dit document.

Classificatie netwerkcomponenten

Onafhankelijk van de classificatie van de informatie die doorheen de netwerkcomponent getransporteerd wordt, kunnen de componenten zelf ook in een klasse onderverdeeld worden:

Netwerkcomponent	***Voorbeelden***	***Minimale klasse vertrouwelijkheid***	***Minimale klasse integriteit***
Passieve componenten	Netwerkkabel, *connector*, *patch*-panelen	1	1
Niet-intelligente actieve componenten	*Hub*, *repeater*	1	1
Intelligente actieve componenten in eenzelfde zone	*Switches* en *routers* zonder *policies* of rapportering *Switches* of *routers* in IoT of bezoekersnetwerk	1	2
Intelligente actieve componenten die voor connectiviteit zorgen tussen verschillende zones		3	3
Intelligente actieve componenten waarop een security policy wordt afgedwongen	*Firewall*, IPS, *antimalware*	3	3
Componenten met SSL-inspectie/ *SSL offloading*		4	4
Componenten voor beheerstaken		3	4
Hypervisor	Virtuele machines	4	4

Uiteraard moet ook nog de classificatie van de informatie die over de netwerkcomponent gaat, in rekening gebracht worden. De hoogste klasse is dan ook bepalend: indien informatie van klasse 3 over een netwerkcomponent van klasse 1 gaat, zal de netwerkcomponent automatisch ook tot klasse 3 gerekend worden.

1.1. Minimale maatregelen in de DMZ

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 Er moet een DMZ opgezet worden voor ontsluiting naar publieke netwerken (zoals internet en derde partijen), componenten met rechtstreekse verbinding naar publieke netwerken moeten hierin geplaatst worden; 〉 Datastromen tussen verschillende organisaties worden van mekaar gescheiden door een DMZ. Organisaties kunnen enkel in hun eigen container (= eigen afschermings-*boundary*) onderling afspraken maken over de inrichting van de datastromen zonder DMZ; 〉 *Servers* in de DMZ hebben zo beperkt mogelijk toegang tot publieke netwerken; 〉 Indien aanwezig worden *proxy* (*forward* & *reverse*) en *mail relays* in de DMZ geplaatst; 〉 *Least privilege* wordt toegepast voor datastromen van en naar de DMZ; en 〉 DMZ mag fysiek niet toegankelijk zijn voor onbevoegden (niet door de organisatie geautoriseerde personen) en moet fysiek beveiligd zijn (zie ook document 'Vo Informatieclassificatie – minimale maatregelen – fysische maatregelen'). **Transportbeveiliging**: 〉 Versleutelde transportprotocollen of VPN voor beheerstaken die buiten de DMZ worden uitgevoerd. **IDS**: 〉 Wordt ingezet op alle datastromen van en naar de DMZ. **Inbraakpreventie**: 〉 Datastromen tussen DMZ en publieke netwerken worden geleid via een *firewall*, die voldoet aan goede praktijken zoals ISF *good practice for information security* of gelijkwaardig, rekening houdende met volgende criteria: ○ Filteren op basis van type datastromen; ○ Beperken of blokkeren van bepaalde datastromen; ○ *Stateful inspection* of gelijkwaardige technologie; ○ Werken vanuit *default deny*-principe; ○ Werken vanuit centraal opgestelde regels (*ruleset*); en ○ Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS moet de DMZ beveiligen tegen aanvallen vanuit publieke netwerken.

	Antimalware: 〉 Alle datastromen die de DMZ binnenkomen of verlaten, worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle 'aanvalsvectoren' met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; 〉 Beveiliging tegen *zero-day*-aanvallen; en 〉 Genereren van alarmen naar de *antimalware*-beheerders. ***Content/URL filtering***: 〉 Een *whitelist* wordt opgesteld en actief onderhouden op *serverniveau* voor uitgaande datastromen naar internet. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging***: 〉 Toegang van en naar DMZ moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Er wordt actief gecontroleerd op ongewenste patronen in datastromen; 〉 *Event logging* wordt opgezet op kritische netwerktoestellen in DMZ (o.a. *up*/*down* gaan van *switch*-poorten); 〉 Voor *logging* van toegangsbeheer: zie document 'Vo Informatieclassificatie – minimale maatregelen – PAM'; 〉 Zie ook document 'Vo Informatieclassificatie – minimale maatregelen – SIEM'.

	Klasse 3, Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 Out-of-Band opzetten voor beheerstaken. **Transportbeveiliging**: 〉 Binnen de DMZ wordt enkel gebruik gemaakt van versleutelde protocollen. ***Cloud*-omgeving**: 〉 Sleutelbeheer buiten de *cloud provider* (eigen organisatie of *trusted partner*); 〉 Geen *cloud provider* kiezen zonder vestiging in de EU; en 〉 Auditeerbaarheid contractueel afdwingen. ***Content/URL filtering***: 〉 Inspectie op alle datastromen die naar buiten gaan. ***Logging***: 〉 *Event logging* wordt opgezet voor alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.

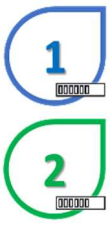
Integriteit

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 Er moet een DMZ opgezet worden voor ontsluiting naar publieke netwerken (zoals internet en derde partijen), componenten met rechtstreekse verbinding naar publieke netwerken moeten hierin geplaatst worden; 〉 Datastromen tussen verschillende organisaties worden van mekaar gescheiden door een DMZ. Organisaties kunnen enkel in hun eigen container (= eigen afschermings-*boundary*) onderling afspraken maken over de inrichting van de datastromen zonder DMZ; 〉 *Servers* in de DMZ hebben zo beperkt mogelijk toegang tot publieke netwerken; 〉 Indien aanwezig worden *proxy* (*forward* & *reverse*) en *mail relays* in de DMZ geplaatst; 〉 *Least privilege* wordt toegepast voor datastromen van en naar de DMZ; en

	〉 DMZ mag fysiek niet toegankelijk zijn voor onbevoegden (niet door de organisatie geautoriseerde personen) en moet fysiek beveiligd zijn (zie ook document 'Vo informatieclassificatie – minimale maatregelen – fysieke beveiliging'). **Transportbeveiliging**: 〉 Versleutelde transportprotocollen (bv. https, sftp) worden ingezet voor informatie die ontsloten is naar het internet (integriteitsbewaking); en 〉 Versleutelde transportprotocollen of VPN voor beheerstaken die buiten de DMZ worden uitgevoerd. **IDS**: 〉 Wordt ingezet op alle datastromen van en naar de DMZ. **Inbraakpreventie**: 〉 Datastromen tussen DMZ en publieke netwerken worden geleid via een *firewall*, die voldoet aan goede praktijken zoals ISF *good practice for information security* of gelijkwaardig, rekening houdende met volgende criteria: 〉 Filteren op basis van type datastromen; 〉 Beperken of blokkeren van bepaalde datastromen; 〉 *Stateful inspection* of gelijkwaardige technologie; 〉 Werken vanuit *default deny*-principe; 〉 Werken vanuit centraal opgestelde regels (*ruleset*); en 〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS moet de DMZ beveiligen tegen aanvallen vanuit publieke netwerken. ***Antimalware***: 〉 Alle datastromen die de DMZ binnenkomen of verlaten, worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; 〉 Beveiliging tegen *zero-day*-aanvallen; en 〉 Genereren van alarmen naar de *antimalware*-beheerders. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*.

	Logging* en *monitoring: 〉 Toegang van en naar DMZ moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Er wordt actief gecontroleerd op ongewenste patronen in datastromen; 〉 *Event logging* wordt opgezet op kritische netwerktoestellen in DMZ (o.a. *up/down* gaan van *switch*-poorten); 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 Out-of-Band opzetten voor beheerstaken. **Transportbeveiliging**: 〉 Binnen de DMZ wordt enkel gebruik gemaakt van versleutelde protocollen (integriteitsbewaking). ***Cloud*-omgeving**: 〉 Sleutelbeheer buiten de *cloud provider* (eigen organisatie of *trusted partner*); 〉 Geen *cloud provider* kiezen zonder vestiging in de EU; en 〉 Auditeerbaarheid contractueel afdwingen. ***Logging* en *monitoring***: 〉 *Event logging* wordt opgezet voor alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.

Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 Er moet een DMZ opgezet worden voor ontsluiting naar publieke netwerken (zoals internet en derde partijen), componenten met rechtstreekse verbinding naar publieke netwerken moeten hierin geplaatst worden; 〉 Datastromen tussen verschillende organisaties worden van mekaar gescheiden door een DMZ. Organisaties kunnen enkel in hun eigen container (= eigen afschermings-*boundary*) onderling afspraken maken over de inrichting van de datastromen zonder DMZ; 〉 *Servers* in de DMZ hebben zo beperkt mogelijk toegang tot publieke netwerken;

	〉 Indien aanwezig worden *proxy* (*forward* & *reverse*) en *mail relays* in de DMZ geplaatst; 〉 *Least privilege* wordt toegepast voor datastromen van en naar de DMZ; 〉 DMZ mag fysiek niet toegankelijk zijn voor onbevoegden (niet door de organisatie geautoriseerde personen) en moet fysiek beveiligd zijn (zie ook document 'Vo informatieclassificatie – minimale maatregelen – fysische maatregelen'). **IDS**: 〉 Wordt ingezet op alle datastromen van en naar de DMZ. **Inbraakpreventie**: 〉 Datastromen tussen DMZ en publieke netwerken worden geleid via een *firewall*, die voldoet aan goede praktijken zoals ISF *good practice for information security* of gelijkwaardig, rekening houdende met volgende criteria: 〉 Filteren op basis van type datastromen; 〉 Beperken of blokkeren van bepaalde datastromen; 〉 *Stateful inspection* of gelijkwaardige technologie; 〉 Werken vanuit *default deny*-principe; 〉 Werken vanuit centraal opgestelde regels (*ruleset*); en 〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS moet de DMZ beveiligen tegen aanvallen vanuit publieke netwerken. ***Antimalware***: 〉 Alle datastromen die de DMZ binnenkomen of verlaten, worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; 〉 Beveiliging tegen *zero-day*-aanvallen; en 〉 Genereren van alarmen naar de *antimalware*-beheerders. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* in het kader van beschikbaarheid**: 〉 Toegang van en naar DMZ moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Er wordt actief gecontroleerd op ongewenste patronen in datastromen;

	〉 *Event logging* wordt opgezet op kritische netwerktoestellen in DMZ (o.a. *up*/*down* gaan van *switch*-poorten); 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'. ***High-availability***: 〉 Het voorzien van reserve-onderdelen en reservecomponenten volstaat. ***Cloud*-omgeving**: 〉 Auditeerbaarheid contractueel afdwingen; en 〉 Exit procedure (opnemen in contract).
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 Out-of-Band opzetten voor beheerstaken. ***Logging* en *monitoring* in het kader van beschikbaarheid**: 〉 *Event logging* wordt opgezet voor alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM. ***High-availability***: 〉 *High-availability*-infrastructuur implementeren (*loadbalancing*, *clustering*, *safe failover*, …).
 	Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + ***Cloud provider***: 〉 Back-up van data bij een andere partij dan de *cloud provider* (om *vendor lock-in* te vermijden).

1.2. Minimale maatregelen in de gebruikerszone

Vertrouwelijkheid

IC klasse	Minimale maatregelen

 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen:
	
	Netwerkzonering:
	〉 *Least privilege* wordt toegepast op datastromen van en naar de gebruikerszone;
	〉 De datastromen voor beheer moeten gescheiden zijn van gebruikersdatastromen;
	〉 Er moet een logische scheiding zijn tussen gebruikers- en datazone;
	〉 Er moet een logische scheiding zijn tussen organisatie eigen gebruikerszones en publieke gebruikerszones (bv. *guest*);
	〉 *Outbound web*-datastromen worden ontsloten via *proxyservers* waarbij de *proxy* controleert op juist protocolgebruik; en
	〉 Bijkomende maatregelen moeten worden genomen op niveau gebruikersapparatuur
	
	IDS:
	〉 Wordt ingezet op alle datastromen van en naar de gebruikerszone.
	
	Transportbeveiliging:
	〉 Versleutelde transportprotocollen of VPN voor beheerstaken die buiten de gebruiker zone worden uitgevoerd.
	
	Inbraakpreventie:
	〉 Datastromen tussen gebruikerszone en publieke netwerken worden geleid via een *firewall* in de DMZ, die voldoet aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria:
	  〉 Filteren op basis van type datastromen;
	  〉 Beperken of blokkeren van bepaalde datastromen;
	  〉 *Stateful inspection* of gelijkwaardige technologie;
	  〉 Werken vanuit *default deny*-principe;
	  〉 Werken vanuit centraal opgestelde regels (*ruleset*); en
	  〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer);
	〉 IPS wordt actief ingezet op alle datastromen tussen publieke netwerken en gebruikerszone.
	
	Antimalware:
	〉 Alle datastromen van en naar gebruikersapparatuur worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria:

	〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; en 〉 Beveiliging tegen *zero-day*-aanvallen. 〉 Genereren van alarmen naar de *antimalware*-beheerders. ***Logging* en *monitoring***: 〉 Toegang van en naar de gebruikerszone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang en beheer van netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo Informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 IoT-toestellen die functioneel niet deel uitmaken van de administratieve bedrijfsprocessen moeten in een aparte zone, gescheiden van de gebruikerszone; 〉 Binnen de zone moeten maatregelen genomen worden om de impact tussen eindgebruikerstoestellen onderling te mitigeren en 〉 Gebruikerstoestellen die ingesteld kunnen worden als lokale gastheer (*local host*) moeten als een aparte netwerkzone beschouwd worden. Zij moeten voorzien zijn van *firewall*, *antimalware* en IPS. **Transportbeveiliging**: 〉 Versleutelde protocollen worden toegepast van en naar de betrokken *server*. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Content/URL-filtering***: 〉 Inspectie op alle datastromen die naar buiten gaat. ***Logging* en *monitoring***: 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS *use cases* moeten beschikbaar zijn voor SIEM.
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 +

	**SSL-inspectie**: 〉 De mogelijkheid tot uitzonderingen moet worden voorzien omdat bepaalde informatie zo gevoelig kan zijn dat SSL-inspectie niet wenselijk is: zie document '*Vo Informatieclassificatie – Minimale maatregelen – Cryptografie*'.

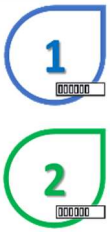
Integriteit

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 *Least privilege* wordt toegepast op datastromen van en naar de gebruikerszone; 〉 De datastromen voor beheer moeten gescheiden zijn van gebruikersdatastromen; 〉 Er moet een logische scheiding zijn tussen gebruikers- en datazone; 〉 Er moet een logische scheiding zijn tussen organisatie eigen gebruikerszones en publieke gebruikerszones (bv. *guest*); 〉 *Outbound web*-datastromen worden ontsloten via *proxyservers* waarbij de *proxy* controleert op juist protocolgebruik; en 〉 Bijkomende maatregelen worden genomen op niveau gebruikersapparatuur: dit document is nog in ontwikkeling. **IDS**: 〉 Wordt ingezet op alle datastromen van en naar de gebruikerszone. **Transportbeveiliging**: 〉 Versleutelde transportprotocollen worden voorzien voor *write access* vanuit gebruikerszone (integriteitsbewaking); en 〉 Versleutelde transportprotocollen of VPN voor beheerstaken die buiten de gebruiker zone worden uitgevoerd (integriteitsbewaking). **Inbraakpreventie**: 〉 Datastromen tussen gebruikerszone en publieke netwerken worden geleid via een *firewall* in de DMZ, die voldoet aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Filteren op basis van type datastromen; 〉 Beperken of blokkeren van bepaalde datastromen; 〉 *Stateful inspection* of gelijkwaardige technologie; 〉 Werken vanuit *default deny*-principe; 〉 Werken vanuit centraal opgestelde regels (*ruleset*); en

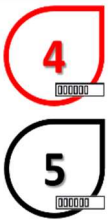
	〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS wordt actief ingezet op alle datastromen tussen publieke netwerken en gebruikerszone. ***Antimalware***: 〉 Alle datastromen van en naar gebruikersapparatuur worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; en 〉 Beveiliging tegen *zero-day*-aanvallen; 〉 Genereren van alarmen naar de *antimalware*-beheerders. ***Logging* en *monitoring***: 〉 Toegang van en naar de gebruikerszone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang en beheer van netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 IoT-toestellen die functioneel niet deel uitmaken van de administratieve bedrijfsprocessen moeten in een aparte zone, gescheiden van de gebruikerszone; 〉 Binnen de zone moeten maatregelen genomen worden om de impact tussen eindgebruikerstoestellen onderling te mitigeren. 〉 Gebruikerstoestellen die ingesteld kunnen worden als lokale gastheer (*local* host) moeten als een aparte netwerkzone beschouwd worden. Zij moeten voorzien zijn van *firewall*, *antimalware* en IPS. **Transportbeveiliging**: 〉 Versleutelde protocollen worden toegepast van en naar de betrokken server (integriteitsbewaking).

	SSL-inspectie: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* en *monitoring***: 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **SSL-inspectie**: 〉 De mogelijkheid tot uitzonderingen moet worden voorzien omdat bepaalde informatie zo gevoelig kan zijn dat SSL-inspectie niet wenselijk is: zie document '*Vo Informatieclassificatie – Minimale maatregelen – Cryptografie*'

Beschikbaarheid

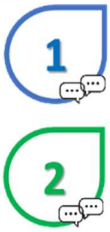
IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 *Least privilege* wordt toegepast op datastromen van en naar de gebruikerszone; 〉 De datastromen voor beheer moeten gescheiden zijn van gebruikersdatastromen; 〉 Er moet een logische scheiding zijn tussen gebruikers- en datazone; 〉 Er moet een logische scheiding zijn tussen organisatie eigen gebruikerszones en publieke gebruikerszones (bv. *guest*); 〉 *Outbound web*-datastromen worden ontsloten via *proxyservers* waarbij de *proxy* controleert op juist protocolgebruik; en 〉 Bijkomende maatregelen worden genomen op niveau gebruikersapparatuur: zie document 'Vo informatieclassificatie – minimale maatregelen – gebruikerstoestellen'. Dit document is nog in ontwikkeling. **IDS**: 〉 Wordt ingezet op alle datastromen van en naar de gebruikerszone. **Inbraakpreventie**: 〉 Datastromen tussen gebruikerszone en publieke netwerken worden geleid via een *firewall* in de DMZ, die voldoet aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria:

	〉 Filteren op basis van type datastromen; 〉 Beperken of blokkeren van bepaalde datastromen; 〉 *Stateful inspection* of gelijkwaardige technologie; 〉 Werken vanuit *default deny*-principe; 〉 Werken vanuit centraal opgestelde regels (*ruleset*); en 〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS wordt actief ingezet op alle datastromen tussen publieke netwerken en gebruikerszone. ***Antimalware***: 〉 Alle datastromen van en naar gebruikersapparatuur worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; en 〉 Beveiliging tegen *zero-day*-aanvallen. 〉 Genereren van alarmen naar de *antimalware*-beheerders. ***Logging* in het kader van beschikbaarheid**: 〉 Toegang van en naar de gebruikerszone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang en beheer van netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'. ***High-availability***: 〉 Het voorzien van reserve-onderdelen en reservecomponenten volstaat.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 IoT toestellen die functioneel niet deel uitmaken van de administratieve bedrijfsprocessen moeten in een aparte zone, gescheiden van de gebruikerszone. 〉 Binnen de zone moeten maatregelen genomen worden om de impact tussen eindgebruikerstoestellen onderling te mitigeren.

	〉 Gebruikerstoestellen die ingesteld kunnen worden als lokale gastheer (*local host*) moeten als een aparte netwerkzone beschouwd worden. Zij moeten voorzien zijn van *firewall*, *antimalware* en IPS. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* en *monitoring* in het kader van beschikbaarheid**: 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM. ***High-availability***: 〉 *High-availability*-infrastructuur implementeren (*loadbalancing*, *clustering*, *safe failover*, …).
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **SSL-inspectie**: 〉 De mogelijkheid tot uitzonderingen moet worden voorzien omdat bepaalde informatie zo gevoelig kan zijn dat SSL-inspectie niet wenselijk is: zie document '*Vo Informatieclassificatie – Minimale maatregelen – Cryptografie*'

1.3. Minimale maatregelen in de datazone

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 Toepassingen worden niet rechtstreeks ontsloten naar publieke netwerken (zoals het internet, derde partijen, …), enkel via een mitigerende component (*reverse proxy*-functionaliteit) in de DMZ waarbij minimaal gecontroleerd wordt op juist protocol gebruik; 〉 Er zijn geen *proxy* (*forward* & *reverse*) en *mail relays* toegelaten in deze zone (moeten in de DMZ geplaatst worden); 〉 *Least privilege* wordt toegepast voor datastromen van en naar de datazone; en 〉 Datazone wordt in fysiek gescheiden locaties geplaatst met toegangscontrole en fysieke beveiliging (zie ook document 'Vo informatieclassificatie – minimale maatregelen – fysische maatregelen').

	Transportbeveiliging: 〉 Versleutelde transportprotocollen (bv. https, sftp) worden toegepast voor informatie die ontsloten is naar het internet; en 〉 Versleutelde transportprotocollen of VPN worden toegepast voor beheerstaken die buiten de datazone worden uitgevoerd. **Inbraakpreventie**: 〉 Datastromen tussen de datazone en publieke netwerken worden geleid via een *firewall* in de DMZ, die voldoet aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Filteren op basis van type datastromen; 〉 Beperken of blokkeren van bepaalde datastromen; 〉 *Stateful inspection* of gelijkwaardige technologie; 〉 Werken vanuit *default deny*-principe; 〉 Werken vanuit centraal opgestelde regels (*ruleset*); en 〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS wordt actief ingezet op alle datastromen van en naar de datazone. ***Antimalware***: 〉 Alle datastromen van en naar de datazone worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; en 〉 Beveiliging tegen *zero-day*-aanvallen. 〉 Genereren van alarmen naar de *antimalware*-beheerders. ***Content/URL filtering***: 〉 *Whitelist* op *serverniveau* voor uitgaande datastromen. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* en *monitoring***: 〉 Toegang van en naar de datazone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip);

	〉 Toegang van server-beheer en beheer van netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 *Event logging* op kritische netwerktoestellen in de datazone (o.a. *up*/*down* gaan van *switch*-poorten); 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 Out-of-Band opzetten voor beheerstaken. **Transportbeveiliging**: 〉 Versleutelde protocollen van en naar de betrokken server, behalve in lokale zone (bv server naar databank). ***Cloud*-omgeving:** 〉 Sleutelbeheer buiten de *cloud provider* (eigen organisatie of *trusted partner*); 〉 Geen *cloud provider* kiezen zonder vestiging in de EU; en 〉 Auditeerbaarheid contractueel afdwingen. **IDS**: 〉 Aanwezig op alle datastromen van en naar datazone. **Inbraakpreventie**: 〉 IPS aanwezig op alle datastromen van en naar de datazone. ***Content/URL filtering***: 〉 Inspectie op alle uitgaande datastromen. ***Logging* en *monitoring***: 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 **Netwerkzonering**: 〉 Zonering per toepassing (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …) **Transportbeveiliging**: 〉 Enkel gebruik van versleutelde protocollen van en naar de betrokken *server* **IDS**: 〉 Aanwezig op alle datastromen van en naar de betrokken *servers*

	Inbraakpreventie: 〉 IPS aanwezig op alle datastromen van en naar de betrokken *servers* ***Antimalware***: 〉 Aanwezig op alle datastromen van en naar de betrokken *servers*
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 / Klasse 4 + **Netwerkzonering**: 〉 Segmentatie per *server* (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …). **Transportbeveiliging**: 〉 Voor transport buiten de zone toegang enkel toegestaan over VPN. **SSL-inspectie**: 〉 Mogelijkheid tot uitzonderingen: bepaalde informatie kan zo gevoelig zijn dat SSL-inspectie niet wenselijk is.

Integriteit

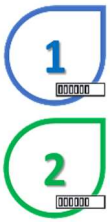
IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 Toepassingen worden niet rechtstreeks ontsloten naar publieke netwerken (zoals het internet, derde partijen, …), enkel via een mitigerende component (*reverse proxy*-functionaliteit) in de DMZ waarbij minimaal gecontroleerd wordt op juist protocol gebruik; 〉 Er zijn geen *proxy* (*forward* & *reverse*) en *mail relays* toegelaten in deze zone (moeten in de DMZ geplaatst worden); 〉 *Least privilege* wordt toegepast voor datastromen van en naar de datazone; en 〉 Datazone wordt in fysiek gescheiden locaties geplaatst met toegangscontrole en fysieke beveiliging (zie ook document ‘Vo informatieclassificatie – minimale maatregelen – fysische maatregelen’). **Transportbeveiliging**: 〉 Versleutelde transportprotocollen (bv. https, sftp) worden toegepast voor informatie die ontsloten is naar het internet (integriteitsbewaking); en 〉 Versleutelde transportprotocollen of VPN worden toegepast voor beheerstaken die buiten de datazone worden uitgevoerd (integriteitsbewaking).

	Inbraakpreventie: 〉 Datastromen tussen de datazone en publieke netwerken worden geleid via een *firewall* in de DMZ, die voldoet aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Filteren op basis van type datastromen; 〉 Beperken of blokkeren van bepaalde datastromen; 〉 *Stateful inspection* of gelijkwaardige technologie; 〉 Werken vanuit *default deny*-principe; 〉 Werken vanuit centraal opgestelde regels (*ruleset*); en 〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS wordt actief ingezet op alle datastromen van en naar de datazone. ***Antimalware***: 〉 Alle datastromen van en naar de datazone worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; 〉 Beveiliging tegen *zero-day*-aanvallen; en 〉 Genereren van alarmen naar de *antimalware*-beheerders. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* en *monitoring***: 〉 Toegang van en naar de datazone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang van *server*-beheer en beheer van netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 *Event logging* op kritische netwerktoestellen in de datazone (o.a. *up*/*down* gaan van *switch*-poorten); 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**:

	〉 Out-of-Band opzetten voor beheerstaken. **Transportbeveiliging**: 〉 Versleutelde protocollen van en naar de betrokken *server*, behalve in lokale zone (bv. *server* naar databank) (integriteitsbewaking). ***Cloud*-omgeving:** 〉 Sleutelbeheer buiten de *cloud provider* (eigen organisatie of *trusted partner*); 〉 Geen *cloud provider* kiezen zonder vestiging in de EU; en 〉 Auditeerbaarheid contractueel afdwingen. **IDS**: 〉 Aanwezig op alle datastromen van en naar datazone. **Inbraakpreventie**: 〉 IPS aanwezig op alle datastromen van en naar de datazone. ***Logging* en *monitoring***: 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **Netwerkzonering**: 〉 Zonering per toepassing (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …). **Transportbeveiliging**: 〉 Enkel gebruik van versleutelde protocollen van en naar de betrokken *server* (integriteitsbewaking). **IDS**: 〉 Aanwezig op alle datastromen van en naar de betrokken *servers* **Inbraakpreventie**: 〉 IPS aanwezig op alle datastromen van en naar de betrokken *servers.* ***Antimalware***: 〉 Aanwezig op alle datastromen van en naar de betrokken *servers*.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + **Netwerkzonering**: 〉 Segmentatie per *server* (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/'security *zone*, *security*-groepen, …).

	Transportbeveiliging: 〉 Voor transport buiten de zone toegang enkel toegestaan over VPN (integriteitsbewaking). **SSL-inspectie**: 〉 Mogelijkheid tot uitzonderingen: bepaalde informatie kan zo gevoelig zijn dat SSL-inspectie niet wenselijk is.

Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 Toepassingen worden niet rechtstreeks ontsloten naar publieke netwerken (zoals het internet, derde partijen, …), enkel via een mitigerende component (*reverse proxy*-functionaliteit) in de DMZ waarbij minimaal gecontroleerd wordt op juist protocol gebruik; 〉 Er zijn geen *proxy* (*forward* & *reverse*) en *mail relays* toegelaten in deze zone (moeten in de DMZ geplaatst worden); 〉 *Least privilege* wordt toegepast voor datastromen van en naar de datazone; en 〉 Datazone wordt in fysiek gescheiden locaties geplaatst met toegangscontrole en fysieke beveiliging (zie ook document 'Vo informatieclassificatie – minimale maatregelen – fysische maatregelen'). **Transportbeveiliging**: 〉 Versleutelde transportprotocollen of VPN worden toegepast voor beheerstaken die buiten de datazone worden uitgevoerd. **Inbraakpreventie**: 〉 Datastromen tussen de datazone en publieke netwerken worden geleid via een *firewall* in de DMZ, die voldoet aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Filteren op basis van type datastromen; 〉 Beperken of blokkeren van bepaalde datastromen; 〉 *Stateful inspection* of gelijkwaardige technologie; 〉 Werken vanuit *default deny*-principe; 〉 Werken vanuit centraal opgestelde regels (*ruleset*); en 〉 Beveiligd beheer van de *firewall* (d.m.v. authenticatie en beveiligd verkeer); 〉 IPS wordt actief ingezet op alle datastromen van en naar de datazone.

	Antimalware: 〉 Alle datastromen van en naar de datazone worden gecontroleerd op kwaadaardige software; *antimalware* moet voldoen aan goede praktijken zoals ISF *good practice for information security* (recente versie) of gelijkwaardig, rekening houdende met volgende criteria: 〉 Optreden tegen alle aanvalsvectoren met mogelijkheid tot blokkeren of minimaal in quarantaine plaatsen; 〉 Gecentraliseerd beheer; 〉 Altijd actief; 〉 Mogelijkheid tot *real-time scanning*; 〉 Niet-intrusief: de gebruiker minimaal belasten; 〉 Automatische updates van de *signature database*; 〉 Beveiliging tegen *zero-day*-aanvallen; en 〉 Genereren van alarmen naar de *antimalware*-beheerders. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* in het kader van beschikbaarheid**: 〉 Toegang van en naar de datazone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang van *server*-beheer en beheer van netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 *Event logging* op kritische netwerktoestellen in de datazone (o.a. *up*/*down* gaan van *switch*-poorten); 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'. ***High-availability***: 〉 Het voorzien van reserve-onderdelen en reservecomponenten volstaat. ***Cloud*-omgeving**: 〉 Auditeerbaarheid contractueel afdwingen; en 〉 Exit procedure (opnemen in contract).
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 Out-of-Band opzetten voor beheerstaken. **IDS**: 〉 Aanwezig op alle datastromen van en naar datazone. **Inbraakpreventie**:

	〉 IPS aanwezig op alle datastromen van en naar de datazone. 〉 ***Logging* en *monitoring* in het kader van beschikbaarheid:** 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM. ***High-availability*:** 〉 *'High-availability*-infrastructuur implementeren (*loadbalancing*, *clustering*, *safe failover*, …).
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **Netwerkzonering**: 〉 Zonering per toepassing (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …). **IDS**: 〉 Aanwezig op alle datastromen van en naar de betrokken *servers*. **Inbraakpreventie**: 〉 IPS aanwezig op alle datastromen van en naar de betrokken *servers*. ***Antimalware***: 〉 Aanwezig op alle datastromen van en naar de betrokken *servers*. ***Cloud provider*:** 〉 Back-up van data bij een andere partij dan de *cloud provider* (om *vendor lock*-in te vermijden).
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + **Netwerkzonering**: 〉 Segmentatie per *server* (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …).

1.4. Minimale maatregelen in de IoT-zone

Vertrouwelijkheid

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 *Least privilege* toepassen voor datastromen van en naar de IoT-zone; 〉 Logische scheiding met gebruikerszone; 〉 Indien DMZ aanwezig: *proxy* verplichten; en 〉 Toegang vanaf publiek netwerk enkel via mitigerende component (bv. *proxyserver*). **Transportbeveiliging**: 〉 Versleutelde transportprotocollen (bv. https, sftp) voor informatie die ontsloten is naar het internet; 〉 Versleutelde transportprotocollen of VPN voor beheerstaken die buiten IoT-zone worden uitgevoerd; en 〉 Versleutelde transportprotocollen voor *write access* vanuit gebruikerszone. **Inbraakpreventie**: 〉 Filtering op basis van IP-adressen en protocollen. ***Antimalware***: 〉 Alle datastromen van en naar de betrokken *servers* behalve in lokale zone worden gecontroleerd op kwaadaardige software. ***Content/URL filtering***: 〉 *Whitelist* op toepassing voor uitgaand datastromen naar internet. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* en *monitoring***: 〉 Toegang van en naar netwerkzone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang van *server*-beheer en beheer netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 Voor *logging* van toegangsbeheer: zie document ‘Vo informatieclassificatie – minimale maatregelen – PAM’; en 〉 Zie ook document ‘Vo informatieclassificatie – minimale maatregelen – SIEM’.

	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**: 〉 Zones moeten fysiek beveiligd zijn tegen niet-geautoriseerde toegang (zie document '[Vo informatieclassificatie – minimale maatregelen – fysische maatregelen]'). [Vo informatieclassificatie – minimale maatregelen – fysische maatregelen] **Transportbeveiliging**: 〉 Versleutelde protocollen van en naar de betrokken component, behalve in lokale zone. **IDS**: 〉 Aanwezig op alle datastromen van en naar IoT-zone. **Inbraakpreventie**: 〉 IPS aanwezig op alle datastromen van en naar IoT-zone. ***Content/URL filtering***: 〉 Inspectie op uitgaand datastromen. ***Logging* en *monitoring:*** 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 **Transportbeveiliging**: 〉 Enkel gebruik van versleutelde protocollen van en naar de betrokken component.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + **Netwerkzonering**: 〉 Segmentatie per component (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …). **Transportbeveiliging**: 〉 Voor transport buiten de zone toegang enkel toegestaan over VPN. **SSL-inspectie**: 〉 Mogelijkheid tot uitzonderingen: bepaalde informatie kan zo gevoelig zijn dat SSL-inspectie niet wenselijk is.

Integriteit

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 *Least privilege* toepassen voor datastromen van en naar de IoT-zone; 〉 Logische scheiding met gebruikerszone; 〉 Indien DMZ aanwezig: *proxy* verplichten; en 〉 Toegang vanaf publiek netwerk enkel via mitigerende component (bv. *proxyserver*). **Transportbeveiliging**: 〉 Versleutelde transportprotocollen (bv. https, sftp) voor informatie die ontsloten is naar het internet (integriteitsbewaking); 〉 Versleutelde transportprotocollen of VPN voor beheerstaken die buiten IoT-zone worden uitgevoerd (integriteitsbewaking); en 〉 Versleutelde transportprotocollen voor *write access* vanuit gebruikerszone (integriteitsbewaking). **Inbraakpreventie**: 〉 Filtering op basis van IP-adressen en protocollen. ***Antimalware***: 〉 Alle datastromen van en naar de betrokken *servers* behalve in lokale zone worden gecontroleerd op kwaadaardige software. **SSL-inspectie**: 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* en *monitoring:*** 〉 Toegang van en naar netwerkzone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang van *server*-beheer en beheer netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**:

	〉 Zones moeten fysiek beveiligd zijn tegen niet-geautoriseerde toegang (zie document '[Vo informatieclassificatie – minimale maatregelen – fysische maatregelen]'). **Transportbeveiliging**: 〉 Versleutelde protocollen van en naar de betrokken component, behalve in lokale zone (integriteitsbewaking). **IDS**: 〉 Aanwezig op alle datastromen van en naar IoT-zone. **Inbraakpreventie**: 〉 IPS aanwezig op alle datastromen van en naar IoT-zone. ***Logging* en *monitoring*:** 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **Transportbeveiliging**: 〉 Enkel gebruik van versleutelde protocollen van en naar de betrokken component (integriteitsbewaking).
	Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + Klasse 4 + **Netwerkzonering**: 〉 Segmentatie per component (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …). **Transportbeveiliging**: 〉 Voor transport buiten de zone toegang enkel toegestaan over VPN (integriteitsbewaking). **SSL-inspectie**: 〉 Mogelijkheid tot uitzonderingen: bepaalde informatie kan zo gevoelig zijn dat SSL-inspectie niet wenselijk is.

Beschikbaarheid

IC klasse	Minimale maatregelen
 	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Netwerkzonering**: 〉 *Least privilege* toepassen voor datastromen van en naar de IoT-zone; 〉 Logische scheiding met gebruikerszone; 〉 Indien DMZ aanwezig: *proxy* verplichten; en 〉 Toegang vanaf publiek netwerk enkel via mitigerende component (bv. *proxyserver*). **Transportbeveiliging:** 〉 Versleutelde transportprotocollen (bv. https, sftp) voor informatie die ontsloten is naar het internet; 〉 Versleutelde transportprotocollen of VPN voor beheerstaken die buiten IoT-zone worden uitgevoerd; en 〉 Versleutelde transportprotocollen voor *write access* vanuit gebruikerszone. **Inbraakpreventie:** 〉 Filtering op basis van IP-adressen en protocollen. ***Antimalware*:** 〉 Alle datastromen van en naar de betrokken *servers* behalve in lokale zone worden gecontroleerd op kwaadaardige software. **SSL-inspectie:** 〉 IDS/IPS/*antimalware* moet alle datastromen kunnen inspecteren. Dit kan via SSL-inspectie, *SSL offloading* of op de *endpoints*. ***Logging* in het kader van beschikbaarheid:** 〉 Toegang van en naar netwerkzone moet gelogd worden (betrokken IP-adressen, protocollen en tijdstip); 〉 Toegang van server-beheer en beheer netwerkapparatuur moet kunnen worden gelinkt aan een toestel, en het toestel aan de eigenaar; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo informatieclassificatie – minimale maatregelen – PAM'; en 〉 Zie ook document 'Vo informatieclassificatie – minimale maatregelen – SIEM'. ***High-availability***: 〉 Het voorzien van reserve-onderdelen en reservecomponenten volstaat.
	Alle maatregelen van Klasse 1 / Klasse 2 + **Netwerkzonering**:

	〉 Zones moeten fysiek beveiligd zijn tegen niet-geautoriseerde toegang (zie document 'Vo informatieclassificatie – minimale maatregelen – fysische maatregelen'). **IDS**: 〉 Aanwezig op alle datastromen van en naar IoT-zone. **Inbraakpreventie**: 〉 IPS aanwezig op alle datastromen van en naar IoT-zone. ***Logging* in het kader van beschikbaarheid**: 〉 *Event logging* op alle netwerktoestellen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM. ***High-availability*:** 〉 *High-availability*-infrastructuur implementeren (*loadbalancing*, *clustering*, *safe failover*, …).
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **Netwerkzonering**: 〉 Segmentatie per component (d.m.v. bijvoorbeeld *host-based firewall*, VLAN/*security zone*, *security*-groepen, …).

1.5. Minimale specifieke (GDPR) maatregelen

De minimale algemene fysieke maatregelen moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing (zie hoofdstuk 'minimale algemene maatregelen').

Er zijn geen minimale specifieke maatregelen voor GDPR rondom netwerken

1.6. Minimale specifieke (NIS II) maatregelen

In afwachting van de goedkeuringen omtrent NISII is er in dit document alvast de nodige ruimte voorzien voor toekomstige minimale specifieke NISII maatregelen.

TBA

1.7. Minimale specifieke (KSZ) maatregelen

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van netwerken toegepast worden:

Integriteit & Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: Elke organisatie moet: 〉 Een schriftelijke machtiging en afwijking aanvragen aan de leidend ambtenaar van de Kruispuntbank van de Sociale Zekerheid (KSZ) wanneer ze wil gebruik maken van het internet als toegangsmiddel tot het netwerk van de KSZ. Het gebruik van het internet als toegangsmiddel tot het netwerk van de KSZ vormt een uitzondering op het algemene principe van de toegang via het Extranet van de Sociale Zekerheid (Ref. KSZ 5.6.2); 〉 Zorgen dat de inhoud van de machtigings- en afwijkingsaanvraag voldoet aan de specificaties vermeld in de paragraaf 'inhoud van de aanvraag' van de beleidslijn 'Gebruik van internet om toegang te krijgen tot het netwerk van de Kruispuntbank van de Sociale Zekerheid in het kader van de verwerking van persoonsgegevens door de actoren van de sociale sector'(Ref. KSZ 5.6.2); 〉 Wanneer ze wil gebruik van het internet als toegangsmiddel tot het netwerk van de KSZ, strikt de voorwaarden toepassen die zijn opgesomd in de bijlage D (Voorwaarden voor toegang tot het Extranet van de Sociale Zekerheid via internet) van de beleidslijn. Deze voorwaarden hebben betrekking op: 〉 Het niveau toegangsmachtiging; 〉 Het niveau identificatie/ authenticatie; 〉 De traceerbaarheid; 〉 Beperkingen; en 〉 De verbinding via file transfer (Ref. KSZ 5.6.2).
	
	
	
	
	
	
	〉 Elke instelling van de sociale zekerheid van het primaire netwerk moet het Extranet van de sociale zekerheid gebruiken voor alle externe verbindingen of de verbindingen met haar secundair netwerk. Voor iedere afwijking op deze maatregel moet een gemotiveerde aanvraag via de veiligheidsdienst van de KSZ worden ingediend (Ref. KSZ 5.6.7).
	〉 Elke organisatie behorend tot een secundair netwerk kan gebruik maken van het Extranet van de sociale zekerheid voor haar verbindingen extern aan de sociale zekerheid. Indien de organisatie een verbinding heeft met externe netwerken zonder te passeren via het Extranet van de sociale zekerheid moet: 〉 De betrokken organisatie veiligheidsmaatregelen implementeren die een gelijkaardig veiligheidsniveau garanderen als dat van het Extranet van de sociale zekerheid voor de informaticasystemen die gebruikt worden voor de verwerking van de persoonsgegevens (Ref. KSZ 5.6.8); 〉 De beheersinstelling van het secundaire netwerk veiligheidsvoorzieningen treffen die een gelijkaardig veiligheidsniveau garanderen als dat van het Extranet van de sociale zekerheid (Ref. KSZ 5.6.8).

	〉 Elke organisatie moet voor alle draadloze netwerken onder beheer van de organisatie op alle locaties: 〉 De draadloze netwerken beheren en beheersen, om toegang tot en gebruik van het netwerk te beperken, en om de informatie in systemen en toepassingen die over draadloze netwerken wordt verstuurd te beschermen (Ref. KSZ 5.10.1); 〉 De richtlijnen naleven die beschreven zijn in bijlage C van de beleidslijn 'Veilige draadloze netwerken' (Ref. KSZ 5.10.1). 〉 Elke organisatie moet nazien dat de netwerken gepast beheerd en gecontroleerd worden, zodanig dat ze beveiligd zijn tegen bedreigingen, en de beveiliging van de systemen en toepassingen die het netwerk gebruiken afdoende garanderen. (Ref. KSZ 5.10.2). 〉 Elke organisatie moet een geactualiseerde cartografie bijhouden van de geïmplementeerde technische stromen via het Extranet van de sociale zekerheid. De veiligheidsconsulent moet hierover geïnformeerd worden (Ref. KSZ 5.10.4). 〉 Elke overdracht van sociale gegevens binnen het netwerk van de sociale zekerheid moet zo spoedig mogelijk worden verwerkt door alle betrokken partijen, of ze nu tussenpersoon of bestemmeling/ontvanger zijn (Ref. KSZ 5.10.5). 〉 Instellingen die sociale gegevens versturen binnen het netwerk van de sociale zekerheid, in het bijzonder wanneer ze de authentieke bron zijn, moeten te gepasten tijde de opvolgingsberichten verwerken die ze van de bestemmelingen of tussenpersonen moeten ontvangen (Ref. KSZ 5.10.5). 〉 Elke bij de verzending betrokken partij, zowel de bestemmeling/ontvanger als de tussenpersoon of de verzender, moet zo snel mogelijk de gepaste maatregelen nemen bij de verwerking van de opvolgingsberichten (Ref. KSZ 5.10.5). 〉 Elke anomalie of lacune in de elektronische verzending van de gegevens moet zo spoedig mogelijk worden gemeld aan de betrokken partijen, of ze nu ontvanger, tussenpersoon of verzender zijn (Ref. KSZ 5.10.5).

Beschikbaarheid

IC klasse	Minimale maatregelen

Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen:

Elke organisatie moet:

- Een schriftelijke machtiging en afwijking aanvragen aan de leidend ambtenaar van de Kruispuntbank van de Sociale Zekerheid (KSZ) wanneer ze wil gebruik maken van het internet als toegangsmiddel tot het netwerk van de KSZ. Het gebruik van het internet als toegangsmiddel tot het netwerk van de KSZ vormt een uitzondering op het algemene principe van de toegang via het Extranet van de Sociale Zekerheid (Ref. KSZ 5.6.2);
- Zorgen dat de inhoud van de machtigings- en afwijkingsaanvraag voldoet aan de specificaties vermeld in de paragraaf 'inhoud van de aanvraag' van de beleidslijn 'Gebruik van internet om toegang te krijgen tot het netwerk van de Kruispuntbank van de Sociale Zekerheid in het kader van de verwerking van persoonsgegevens door de actoren van de sociale sector' (Ref. KSZ 5.6.2);
- Wanneer ze wil gebruik van het internet als toegangsmiddel tot het netwerk van de KSZ, strikt de voorwaarden toepassen die zijn opgesomd in de bijlage D (Voorwaarden voor toegang tot het Extranet van de Sociale Zekerheid via internet) van de beleidslijn. Deze voorwaarden hebben betrekking op:
  - Het niveau toegangsmachtiging;
  - Het niveau identificatie/ authenticatie;
  - De traceerbaarheid;
  - Beperkingen; en
  - De verbinding via file transfer (Ref. KSZ 5.6.2).

- Elke instelling van de sociale zekerheid van het primaire netwerk moet het Extranet van de sociale zekerheid gebruiken voor alle externe verbindingen of de verbindingen met haar secundair netwerk. Voor iedere afwijking op deze maatregel moet een gemotiveerde aanvraag via de veiligheidsdienst van de KSZ worden ingediend (Ref. KSZ 5.6.7).
- Elke organisatie behorend tot een secundair netwerk kan gebruik maken van het Extranet van de sociale zekerheid voor haar verbindingen extern aan de sociale zekerheid. Indien de organisatie een verbinding heeft met externe netwerken zonder te passeren via het Extranet van de sociale zekerheid moet:
  - De betrokken organisatie veiligheidsmaatregelen implementeren die een gelijkaardig veiligheidsniveau garanderen als dat van het Extranet van de sociale zekerheid voor de informaticasystemen die gebruikt worden voor de verwerking van de persoonsgegevens (Ref. KSZ 5.6.8);
  - De beheersinstelling van het secundaire netwerk veiligheidsvoorzieningen treffen die een gelijkaardig veiligheidsniveau garanderen als dat van het Extranet van de sociale zekerheid (Ref. KSZ 5.6.8).
- Elke organisatie moet voor alle draadloze netwerken onder beheer van de organisatie op alle locaties:
  - De draadloze netwerken beheren en beheersen, om toegang tot en gebruik van het netwerk te beperken, en om de informatie in systemen en toepassingen die over draadloze netwerken wordt verstuurd te beschermen (Ref. KSZ 5.10.1);

	〉 De richtlijnen naleven die beschreven zijn in bijlage C van de beleidslijn 'Veilige draadloze netwerken' (Ref. KSZ 5.10.1). 〉 Elke organisatie moet nazien dat de netwerken gepast beheerd en gecontroleerd worden, zodanig dat ze beveiligd zijn tegen bedreigingen, en de beveiliging van de systemen en toepassingen die het netwerk gebruiken afdoende garanderen; ((Ref. KSZ 5.10.2) 〉 Elke organisatie moet de noodzakelijke, afdoende, gepaste en doeltreffende technische maatregelen implementeren om het hoogste niveau van beschikbaarheid voor de verbinding met het netwerk van de Kruispuntbank te waarborgen teneinde een maximale toegankelijkheid van de beschikbaar gestelde en geraadpleegde gegevens te verzekeren. Bijgevolg veronderstelt dit dat deze verbinding minstens ontdubbeld moet zijn naar verschillende knooppunten van het Extranet (Ref. KSZ 5.10.3). 〉 Elke overdracht van sociale gegevens binnen het netwerk van de sociale zekerheid moet zo spoedig mogelijk worden verwerkt door alle betrokken partijen, of ze nu tussenpersoon of bestemmeling/ontvanger zijn (Ref. KSZ 5.10.5). 〉 Instellingen die sociale gegevens versturen binnen het netwerk van de sociale zekerheid, in het bijzonder wanneer ze de authentieke bron zijn, moeten te gepasten tijde de opvolgingsberichten verwerken die ze van de bestemmelingen of tussenpersonen moeten ontvangen (Ref. KSZ 5.10.5). 〉 Elke bij de verzending betrokken partij, zowel de bestemmeling/ontvanger als de tussenpersoon of de verzender, moet zo snel mogelijk de gepaste maatregelen nemen bij de verwerking van de opvolgingsberichten (Ref. KSZ 5.10.5). 〉 Elke anomalie of lacune in de elektronische verzending van de gegevens moet zo spoedig mogelijk worden gemeld aan de betrokken partijen, of ze nu ontvanger, tussenpersoon of verzender zijn (Ref. KSZ 5.10.5).

2. AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1. Categorisatie van maatregelen

Controlemaatregelen vallen onder volgende categorieën:

〉 **Preventie**: vermijden dat iets gebeurt of het verlagen van de waarschijnlijkheid dat het gebeurt;
〉 **Detectie**: detecteren van de (potentiële) schade als een bedreiging zou optreden; of
〉 **Reactie**: beperken van de schade wanneer een bedreiging optreedt of het effect hiervan gedeeltelijk of geheel corrigeren.

2.1.1. Preventieve maatregelen

Maak de dreiging zo goed als onmogelijk of in elk geval aanvaardbaar. In extremis zou men de verbindingen met de buitenwereld verbreken en de deur dichtmetselen. Maar dan zijn er ook geen zakelijke processen meer mogelijk, dit is dus onuitvoerbaar. Er zijn ook uitvoerbare maatregelen. Het in een kluis leggen van gevoelige informatie bijvoorbeeld valt onder preventieve maatregelen. Het maken van een back-up is een ander voorbeeld van een preventieve maatregel; hiermee wordt immers voorkomen dat data geheel verloren gaat mocht een bedreiging zich manifesteren.

In het kader van minimale maatregelen voor netwerkbeveiliging, onderscheiden we volgende preventieve maatregelen:

- Netwerksegmentatie (zie hoofdstuk *'Netwerkzonering als maatregel'*);
- Transportbeveiliging (zie hoofdstuk: '*Transportbeveiliging als maatregel*');
- *Intrusion prevention* (IPS) (zie hoofdstuk: '*Intrusion prevention-systemen (IPS)*');
- SSL-inspectie (zie hoofdstuk: *'SSL-inspectie als maatregel');*
- *Content/URL-filters* (URL/URI, binary-filters zoals exe-bestanden en versleutelde zip-bestanden) (Zie hoofdstuk: '*Content/URL filtering als maatregel*');
- *High-availability* als maatregel (zie hoofdstuk: 'high-availability'); en
- Scheiding van functies.

2.1.2. Detectiemaatregelen

Als de onmiddellijke gevolgen van een bedreiging niet te groot zijn of er is tijd om gevolgschade te beperken, dan is detectie een goede maatregel. Dit houdt bijvoorbeeld in dat een incident zo snel mogelijk wordt gedetecteerd en dat de betrokkenen daarvan op de hoogte worden gebracht. Een bijkomend voordeel is het ontradingseffect: de mededeling dat al het internetgebruik wordt vastgelegd, weerhoudt veel medewerkers van ongeoorloofd surfgedrag. Traceerbaarheid is een belangrijk aspect in detectie en speelt een steeds grotere rol in ICT-beheer ('informatie- en communicatietechnologie').

In het kader van minimale maatregelen voor netwerkbeveiliging, onderscheiden we volgende detectiemaatregelen:

- *Logging* (zie hoofdstuk *'Logging als maatregel'*)
- *Intrusion detection* (IDS) (zie hoofdstuk: *'Intrusion detection als maatregel'*)
- SSL-inspectie (zie hoofdstuk: *'SSL-inspectie als maatregel')*

2.1.3. Reactie

Wanneer er onverhoopt en ondanks alle preventieve maatregelen toch een bedreiging zich manifesteert, en er dus sprake is van een incident, is het zaak de gevolgen te beperken. Reactieve maatregelen, zoals het blussen van een beginnende brand, zijn erop gericht de schade die ontstaat zoveel mogelijk te beperken.

Als een incident heeft plaatsgevonden, dan is er vaak iets dat hersteld moet worden. Afhankelijk van de implementatie van reactieve maatregelen is de schade beperkt of juist zeer groot.

In het kader van minimale maatregelen voor netwerkbeveiliging, onderscheiden we volgende reactieve maatregelen:

- Notificaties naar incidentbeheer (zie document: Vo informatieclassificatie – minimale maatregelen – incident beheer);

- *Content/URL-filters* (URL/URI, binary-filters zoals exe bestanden en versleutelde zip bestanden) (zie hoofdstuk: '*Content/URL filtering als maatregel*');
- Geautomatiseerde tegenmaatregelen; en
- Corrigerende maatregelen op een sessie.

2.2. Netwerkzonering als maatregel

Netwerkzonering is een preventieve maatregel

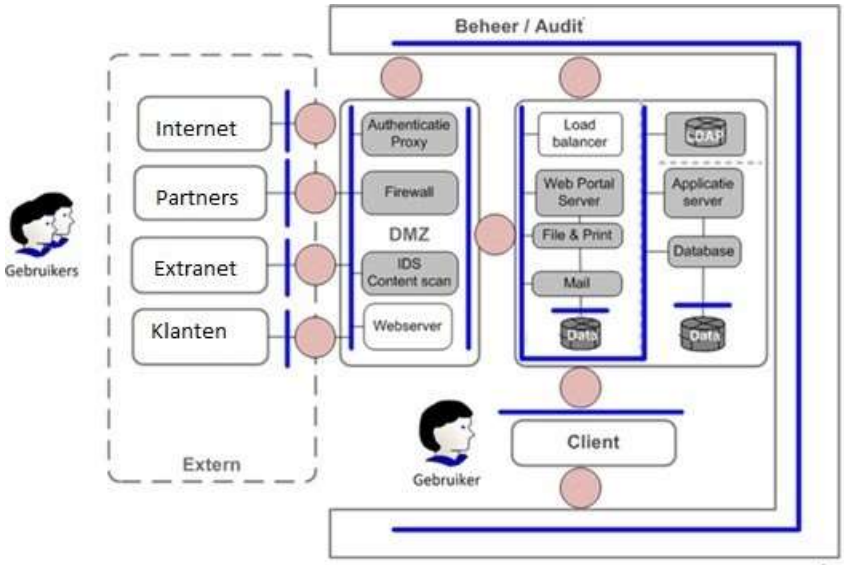
Netwerken maken lokale en wereldwijde connectiviteit mogelijk tussen (ICT-)apparatuur. Netwerken zijn meestal opgebouwd uit functionele zones, waarbij systemen logisch met elkaar gekoppeld zijn op een zone. Netwerkzonering is dus het opsplitsen van een netwerk in logische of fysieke gescheiden zones. Dit kan helpen bij het voldoen aan geldende wet- en regelgeving, informatiebeveiligingsbeleid, beperking van risico's en vereenvoudigen van toezicht.

Zones bestaan op hun beurt uit één of meerdere technische netwerksegmenten.

In een zone kunnen datastromen vrij over het netwerk bewegen. Dat wil niet zeggen dat alles zomaar mogelijk is: er zijn immers nog andere maatregelen buiten de netwerkmaatregelen (zoals bv. authenticatie), maar op netwerkniveau is er binnen de zone geen beperking. Datastromen tussen zones zijn wel aan beperkende maatregelen zoals bv. *filtering* onderworpen.

Zones kunnen worden onderscheiden door gebruikmaking van *routering* van datastromen, verificatie van de bron- en de bestemmingsadressen, door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van *servers*, maar ook door fysieke scheiding. Bij logische scheiding wordt gebruik gemaakt van technieken zoals VLAN (*Virtual Local Area Network*), ACL (*Access Control Lists*), NAC (*Network Access Control*) en NGFW (*Next Generation firewalls*).

Onderstaande figuur schetst de belangrijkste netwerkzones binnen een organisatie.



Een netwerkzone is een afgebakend deel van het netwerk van ICT-apparatuur, waarin trafiek vrij kan manoeuvreren. Gegevensuitwisseling met andere zones verloopt via gedefinieerde interfaces. Het primaire doel van segmentering is het isoleren van risico's zodat bedreigingen en incidenten uit de ene zone niet kunnen doorwerken in de andere zone. Mocht één laag worden doorbroken, dan voorkomt de volgende beveiligingslaag in deze architectuur dat bedrijfsprocessen en gegevens direct kunnen worden benaderd vanuit de andere zone. Vergelijk het met de veiligheidsdeuren in een schip, die het ene compartiment afscheiden van het andere zodat bij waterdoorbraak het water niet in het andere compartiment kan lopen.

Wanneer twee netwerkzones gekoppeld worden zodat netwerktrafiek van de ene zone naar de andere zone doorvloeit, geldt globaal het betrouwbaarheidsniveau van de zone met het laagste niveau. Bijkomende maatregelen zijn dan nodig om het niveau van betrouwbaarheid tot het gewenste niveau te verhogen door passende maatregelen te nemen in de zones (op netwerk- of systeemniveau) zelf of op de *interface*.

Waar vroeger een netwerkarchitectuur geïmplementeerd werd binnen de muren van de organisatie, vervagen deze fysieke grenzen meer en meer door de toepassing van virtualisatie en het gebruik van clouddiensten. Fysieke bescherming en afscherming van een perimeter wordt op deze manier moeilijker omdat ook de fysieke grenzen verdwijnen.

In de meeste netwerkarchitecturen vindt men een combinatie van volgende zones:

- DMZ: deze zone vormt een buffer tussen de organisatie en de buitenwereld;
- Gebruikerszone: in deze zone bevindt zich de gebruikersapparatuur, d.w.z. dit is de enige zone waarin gebruikers interageren met ICT-apparatuur;
- Datazone: deze zone bevat alle ICT-apparatuur nodig voor gebruikerstoepassingen; en
- IoT-zone (*Internet of Things*): zone voor koppelen van intelligente apparatuur zoals printers, camera's, sensoren, …

2.2.1. Logische indeling

DMZ

Dit domein is een neutraal gebied tussen de buitenwereld en de organisatie en fungeert voornamelijk als doorgeefluik. De buitenkant van een DMZ (*demilitarized zone*) wordt gevormd door een grensbescherming met filterfuncties, zoals NAT (*Network Address Translation*) en/of *network based firewall.* De DMZ omvat één of meer mechanismen voor *filtering* van protocollen en ongewenste communicatie, afhandelen van *malware*, functies voor ontkoppeling (*proxy*), voor protocoltransformatie, misleiding van *hackers* en *monitoring*. Als de grensbescherming aan de buitenkant wordt gebroken, dan kan een *hacker* toegang krijgen tot de data binnen de DMZ. De filterende mechanismen en de grensbescherming tussen DMZ en de organisatie moeten voorkomen dat *hackers* vanuit de DMZ door kunnen gaan naar interne zones.

De DMZ bevat in veel gevallen ook *webservers*, die publiek toegankelijke organisatiegegevens bevatten. Dit zijn zowel informatieverstrekkende *webservers* opgesteld als *webservers* die transacties van gebruikers kunnen doorzetten naar de achterliggende, interne omgeving. Vanuit de externe

omgeving gerekend fungeert de DMZ als doorgeefluik waar klantinformatie wordt verwerkt tot organisatie-informatie en omgekeerd.

Een DMZ kan in een eigen *datacenter* opgezet worden, of *hosted* bij een provider of in een publieke cloud.

Gebruikerszone

Deze zone bevat zowel ondersteunende systemen als systemen voor het operationeel verwerken van systemen en de gebruikersapparatuur (bv. laptop, desktop, …). Hier werken toepassingen voor de normale bedrijfsvoering van de organisatie.

Deze zone is een hoog-risicozone omwille van de grote aantallen aansluitingen, de directe toegang op de toestellen door gebruikers en de relatief grote kwetsbaarheid voor inbreuk. De controle op naleving van beveiligingsrichtlijnen in de gebruikerszone is doorgaans beperkt.

Gebruikers kunnen potentieel overal zijn: op kantoor, werken van thuis uit of vanuit elke omgeving die één of andere vorm van door de organisatie toegelaten connectiviteit aanbiedt.

Datazone

Deze zone bevat de apparatuur waarop de toepassingen draaien voor normale bedrijfsvoering van de organisatie. Deze toepassingen worden door de gebruikers in de gebruikerszone benaderd voor verwerking van informatie.

Vaak kiezen organisaties voor het uitbesteden van het beheer en onderhoud van de toepassingen of van de apparatuur waarop deze toepassingen draaien. Deze apparatuur komt dan fysiek in een *datacenter* te staan.

Zo'n *datacenter* kan onder eigen beheer vallen (*on premise*) of *hosted* bij een *provider* of in een niet-publieke cloud.

IoT-zone

Een IoT-zone (*Internet of Things*) bestaat uit toestellen die met elkaar communiceren. Deze communicatie omvat het meten en doorsturen van meetgegevens vanuit diverse sensoren, het verzamelen van gegevens en het geven van commando's. Sommige apparatuur doet specifiek één taak, anderen combineren meerdere taken. Een voorbeeld van IoT is het aansturen van huishoudapparatuur vanaf de smartphone, maar ook bijvoorbeeld printers op een netwerk, camera's en toegangspoortjes voor beheer van gebouwen, enz.

IoT kan over diverse netwerken werken. Sommige netwerken zijn heel specifiek en beperkt tot een bepaalde omgeving of zelfs organisatie (bv. ProRail van de Nederlandse Spoorwegen). Maar er zijn ook publieke netwerken voor IoT. Het mobiele netwerk (3G, 4G, 5G), GPRS, bluetooth en wifi worden als IoT-netwerk ingeschakeld waar er grote hoeveelheden data aan hoge snelheid moeten worden verwerkt, maar er zijn ook standaarden ontwikkeld specifiek voor IoT met als voornaamste kenmerk een laag verbruik. Ze worden LPWA (*Low Power Wide Area*) genoemd en voorbeelden hiervan zijn LoRa en SigFox. Een geslaagd IoT-netwerk bestaat uit de juiste combinatie van LPWA en de klassieke mobiele, bluetooth- en wifi-oplossingen.

Beveiliging van IoT-netwerken is een belangrijk onderwerp. Niet alleen toegang tot deze netwerken, maar ook de beveiliging van (gevoelige) data die over deze netwerken gaan, moeten in orde zijn.

2.2.2. Beheer

Alle ICT-apparatuur moet op één of andere wijze beheerd worden. Problemen moeten opgelost worden, configuraties aangepast, updates en wijzigingen geïmplementeerd. Waar dit in een ver verleden vaak rechtstreeks op het apparaat zelf werd uitgevoerd, gebeurt dit nu via een netwerk-verbinding.

Een beheerszone kan opgezet worden op netwerkniveau door bv. *Out-of-Band* (OoB), maar ook via andere maatregelen zoals centralisatie van beheers *tools*, sterke authenticatie op beheers *tools*, enz.

Om de scheiding tussen connectiviteit voor beheer en voor operationele datastromen uit te voeren, wordt vaak *Out-of-Band* gewerkt. Hierbij wordt een specifieke netwerkverbinding voor beheer van de toestellen opgezet die verschilt van de zone voor de reguliere gebruiker (de gebruikerszone). Omdat over deze OoB enkel netwerktrafiek gerelateerd aan beheersprocessen gaat, wordt het vaak als een beveiligd kanaal opgezet.

2.2.3. *Datacenter*

Een *datacenter* bevat bedrijfskritische ICT-apparatuur. Een *datacenter* is dan ook uitgerust met diverse voorzieningen zoals klimaatbeheersing, geavanceerde branddetectie en -blussystemen, beveiliging enz.

Omdat er in zo'n *datacenter* typisch grote hoeveelheden data verwerkt wordt, bestaat het netwerk vaak uit complexe, ontdubbelde en snelle netwerkverbindingen. Redundantie is belangrijk omdat men moet kunnen garanderen dat de *servers* geplaatst in een *datacenter* beschikbaar zijn volgens de specificaties van de SLA (*Service Level Agreement*).

In een *datacenter* zijn geen gebruikers actief, zij werken vanuit de gebruikerszone. Maar ook beheerders opereren meestal buiten het *datacenter* via de beheerszone. Enkel specifieke taken die niet vanop afstand kunnen uitgevoerd worden, vereisen rechtstreekse (fysieke) toegang tot de systemen en het netwerk van het *datacenter*.

Meer en meer wordt het opzetten en beheer van een *datacenter* uitbesteed. Gespecialiseerde organisaties (*serviceproviders*) zetten groots opgebouwde *datacenters* op voor de verschillende klanten die hun systemen hierin plaatsen en laten beheren. Het netwerk (of op zijn minst toch een gedeelte ervan) in zo'n *datacenter* wordt dan gedeeld door de verschillende klant-organisaties, wat natuurlijk aangepaste beveiliging vergt om de scheiding tussen de verschillende klanten te handhaven.

2.2.4. Fysieke indeling

Er bestaan diverse manieren om netwerken op te zetten. Zo is een belangrijk onderscheid te maken tussen bekabelde en draadloze netwerken. Onder de draadloze netwerken is wifi het meest verspreide. Draadloze netwerken hebben zo hun eigen uitdagingen wat betreft beveiliging, omdat de netwerktrafiek en -signalen over de lucht gaan en dus niet fysiek af te scheiden zijn.

Bekabelde netwerken

Hoewel draadloze netwerken aan een niet te stuiten opmars bezig zijn, vindt men nog steeds veel bekabelde netwerken, bijvoorbeeld in de kantooromgeving en in *datacenters*. Om fysieke inbreuk zoals interceptie en beschadiging, illegale verbindingen of wijzigingen in de netwerktopologie te voorkomen, is het dan ook belangrijk om de nodige fysieke controlemaatregelen te nemen. Hiertoe

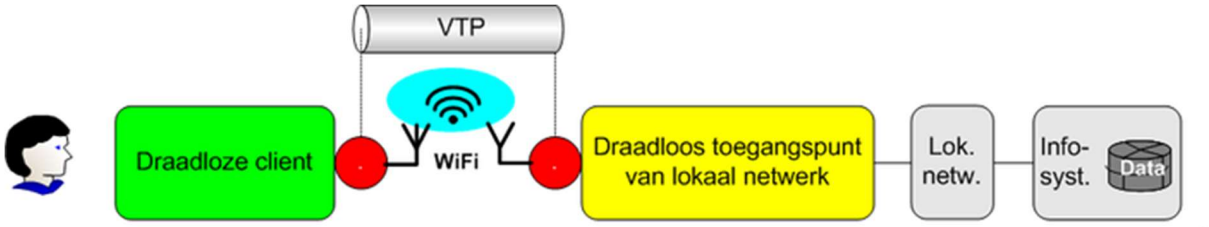
horen de fysieke afscheiding van hoofdkabels door middel van kabelgoten of mantelbuizen, een doordacht bekabelingsschema waarbij de kabels zo min mogelijk door openbare ruimten lopen, het gebruik van afsluitbare *patch*-kasten en het toezicht op het gebruik van de sleutels ervan.

Beveiliging van het bekabeld netwerk houdt ook in dat enkel geautoriseerde netwerkverbindingen mogen opgezet worden, bijvoorbeeld door toegang tot de patch-kasten te beperken tot geautoriseerd personeel of door machine-authenticatie toe te passen zie hoofdstuk 'machine-authenticatie als maatregel' (in document *Vo Informatieclassificatie – Minimale maatregelen - ICT-systemen)*.

WiFi

Inbreukgevoeligheid is één van de belangrijkste bedreigingen van draadloze lokale netwerken. Naast de implementatie van beveiligde netwerkprotocollen zoals WPA 2, moet de nodige aandacht besteed worden aan beveiliging tegen de inherente risico's van het mobiele apparaat zelf. De inbreukgevoeligheid en de mogelijkheden voor aftappen van het draadloze netwerk wordt gereduceerd door versleuteling van de communicatie (zie hiervoor ook het document '*Vo Informatieclassificatie – Minimale maatregelen – Cryptografie')* en het up-to-date houden van OS (*operating systems*) door regelmatige installatie van *patches*.

Er kunnen ook fysieke maatregelen genomen worden om afluisteren zo veel mogelijk te voorkomen, namelijk door het netwerk zodanig in te delen dat er zo weinig mogelijk straling buiten de fysiek beveiligde zone van een organisatie terecht komt. Richtantennes en ontwerp-*tools* voor de fysieke netwerktopologie helpen daarbij. Zo'n zone kan ook gesitueerd worden in een bepaalde ruimte in een gebouw. Met behulp van speciale beheers-*tools* is het stralingsdiagram van wifi-netwerken nauwkeurig vast te stellen. De beschikbaarheid wordt gegarandeerd door te zorgen dat er geen dode plekken in het stralingsdiagram van wifi-netwerken voorkomen en dat het netwerk qua nuttige bandbreedte geografisch zo goed mogelijk is afgestemd op het gebruik binnen de organisatie.



Sommige toestellen bieden de mogelijkheid tot authenticatie en/of het toestel kan zich authentiseren aan het bedrijfsnetwerk. Bij wifi wordt dit opgelost binnen de 801.11 standaard.

Een speciale uitdaging van wifi is het gebruik van draadloze publieke netwerken. Inbreukgevoeligheid is hier meestal niet echt een probleem, omdat de protocollen stabiel zijn en de communicatie standaard versleuteld is. Het zwakke punt ligt bij het draadloze toestel zelf. Trojaanse paarden en andere *malware* kunnen voor de *hacker* mogelijkheden bieden om direct dan wel indirect de datastroom af te luisteren. Merk op dat bij gebruik van publieke netwerken waarbij het toestel connecteert tot aan de interne zone van een organisatie, een inspectieonderbreking in de DMZ moet worden voorzien.

Sterke authenticatie door middel van 2-factor-authenticatie kan een bijkomende maatregel zijn. Dit kan bijvoorbeeld via internet naar het bedrijfsnetwerk en met behulp van een *token*, waarbij men

minder afhankelijk is van het mobiele apparaat en het type netwerk. Voorwaarde is wel dat bedrijfstoepassingen op deze wijze ontsloten kunnen worden.

Bluetooth

Bluetooth is een open standaard voor draadloze verbinding tussen apparaten op korte afstand door middel van een radioverbinding. Bluetooth werkt binnen een straal van 1 tot 10 meter, maar dit kan uitgebreid worden door het zendvermogen op te voeren.

Bluetooth wordt vooral gebruikt als vervanger voor korte kabels om allerlei apparatuur met elkaar te laten communiceren, zoals bijvoorbeeld een draadloze muis of een *headset* voor een computer. Daar gebruik gemaakt wordt van goedkope radiotechniek is bluetooth in vele apparaten ingebouwd. En omdat het weinig energie verbruikt, is het ook terug te vinden in vele mobiele, batterij gestuurde toestellen.

Omdat de radiosignalen kunnen worden opgevangen door alle ontvangers die zich in de buurt van de bluetoothapparaten bevinden, wordt bluetooth beveiligd door middel van authenticatie en encryptie. Authenticatie vindt plaats met behulp van een geheime sleutel, die zich op beide apparaten moet bevinden. Na authenticatie is het mogelijk om de verbinding te versleutelen.

Als het bluetoothapparaat niet voldoende beveiligd wordt, kan illegaal informatie verzonden worden naar het apparaat. Het ongevraagd en dus illegaal lezen van de documenten via bluetooth is ook mogelijk. Verder kan een apparaat onbruikbaar worden gemaakt door middel van DoS-aanvallen.

2.3. Transportbeveiliging als maatregel

Transportbeveiliging is een preventieve maatregel.

Wanneer data een omgeving verlaat, en dus in beweging komt (DIM: *Data In Motion*), moet ze evenzeer beveiligd worden. Een veel gebruikte methode is VPN (*Virtual Private Network*).

VPN is een verzameling van technieken waarvan sommigen werken met het versleutelen van de gegevens, waardoor alleen de ontvangers die beschikken over de juiste sleutel de inhoud van het bericht kunnen lezen. Er wordt gebruik gemaakt van een proces dat *tunneling* wordt genoemd.

2.3.1. Soorten VPN

VPN-verbindingen verschillen op twee manieren van elkaar: de gebruikte manier van *tunneling* en de manier waarop zender en ontvanger met elkaar communiceren.

Tunneling

Er zijn verschillende vormen van *tunneling*:

〉 **PPTP:** PPTP staat voor *point-to-point protocol*. Het is een manier om informatie te versturen waarbij de inhoud van de VPN-tunnel *niet* wordt versleuteld. PPTP zit standaard bijvoorbeeld in Windows ingebouwd. Er is dus slechts beperkte beveiliging mogelijk. Dit betekent dat voor het beveiligen van de gegevensstroom extra maatregelen buiten VPN om nodig zijn.

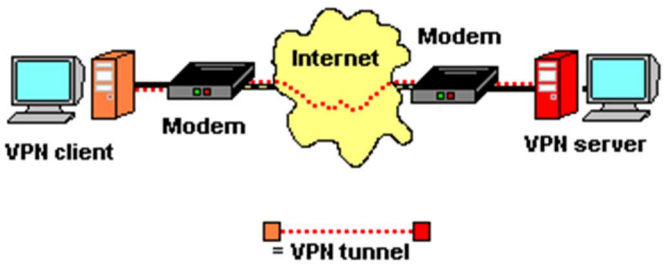
- **L2TP:** L2TP staat voor *layer 2 tunneling protocol*. De voor- en nadelen zijn te vergelijken met PPTP.
- **IPsec:** IPsec (*Internet Protocol Security*) is een standaard voor het beveiligen van IP door middel van encryptie (*Encapsulating Security Payload* of ESP) en/of authenticatie (*Authentication Header* of AH) van de IP-pakketten. ESP IPsec is volgens velen de "echte" vorm van VPN, omdat het de *tunneling* combineert met een bepaalde vorm van encryptie. Om gebruik te kunnen maken van deze techniek moet speciale software aanwezig zijn. AES 256 wordt aanzien als de beste standaard. AH IPsec voorziet enkel in authenticatie van de IP-pakketten maar maakt geen versleutelde verbinding.
- **SSL VPN**: SSL VPN (*Secure Sockets Layer Virtual Private Network*) is een web gebaseerde technologie die het mogelijk maakt om een beveiligde verbinding te maken met een netwerk. Deze techniek maakt gebruik van de mogelijkheden die standaard in de meeste browsers is ingebouwd. De beveiliging gebeurt enerzijds door de authenticatie op gebruikersniveau en anderzijds doordat de data die verstuurd en ontvangen wordt, geëncrypteerd is.
- **MPLS VPN**: MPLS (*MultiProtocol Label Switching*) is een netwerktechnologie dat transport van data of WANs (*Wide Area Networks)* verzorgt. Het wordt dan ook veel gebruikt in *datacenters* van dienstenleveranciers. Bij MPLS wordt vanaf het begin een route bepaald. Een klein label aan het pakketje beschrijft de route die het door het netwerk af moet leggen. Het idee is altijd de snelste route te nemen. *Routers* hoeven alleen maar naar het label te kijken en niet zelf een afweging te maken. MPLS kan met ieder protocol overweg en is geschikt voor veilige VPN-verbindingen omdat het voor aanvallers lastiger is het eindpunt (*endpoint*) te bereiken. Het voorziet echter geen mogelijkheid tot versleuteling (vertrouwelijkheid/integriteit).

Er bestaat een relatie tussen de gebruikte vorm van VPN en de performantie van de connectie. Veilige vormen van encryptie vragen meer rekenwerk en dus risico op lagere performantie. Bij sommige VPN-datastromen kan dit van belang zijn, maar in de meeste situaties heeft het de voorkeur om de meest veilige vorm van versleuteling te gebruiken.

Connectiviteit

Er zijn drie combinaties van VPN tussen computers en netwerken mogelijk, afhankelijk van de punten waartussen de VPN-verbinding moet lopen:

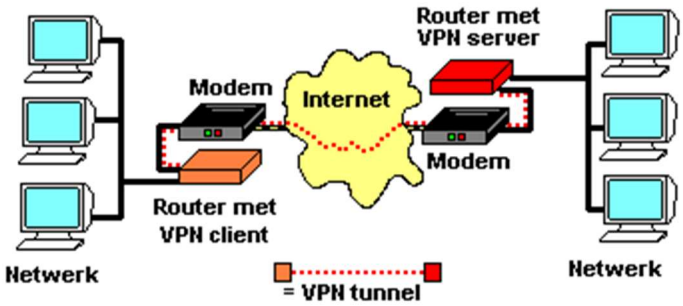
- **Rechtstreeks van computer tot computer:** De meest directe is een vorm van VPN tussen twee computers. Hiervoor hebben deze twee computers respectievelijk een VPN-client en VPN-serverprogramma nodig:



Het gebruik van een computer als VPN-client of -*server* maakt standaard deel uit van sommige versies van Windows. Dit soort VPN-verbindingen zijn vrij recht-toe-recht-aan. Een PPTP of L2TP VPN kan al worden opgezet tussen twee computers die beiden gebruik maken van Windows.

- **Tussen twee *routers* of *firewalls* die VPN ondersteunen:** Om een netwerk van computers toegang tot bijvoorbeeld het internet te geven, heeft men routing-functionaliteit nodig. Als men twee of

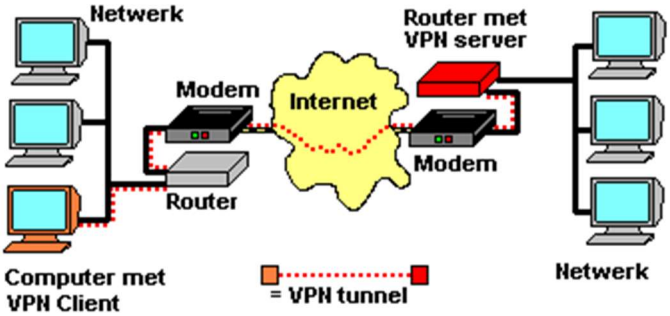
meer netwerken via VPN met elkaar wil verbinden kan men ervoor kiezen de VPN-verbinding niet te laten maken door de individuele computers maar bijvoorbeeld door *routers* of *firewalls* af te laten handelen. De verschillende aangesloten computers hoeven in dit geval geen aparte VPN-software te gebruiken. Zo ontstaat een transparant VPN-netwerk dat over meer dan één locatie gespreid kan zijn. Deze configuratie is ideaal voor het koppelen van bijvoorbeeld een aantal agentschappen en een hoofdzetel.



Een paar opmerkingen over deze opzet:

- De verschillende *routers*/*firewalls* moeten compatibel met elkaar zijn;
- De *routers* moeten het VPN-verkeer normaal doorlaten en de *firewalls* in de *routers* moeten goed zijn geconfigureerd; en
- De netwerken aan de verschillende kanten van de tunnel mogen niet hetzelfde IP-bereik gebruiken.

- **Mengvormen:** Soms wordt de VPN-verbinding opgezet door de computers zelf maar maakt één of beide kanten van de verbinding gebruik van een *router* of *firewall*. Neem bijvoorbeeld een thuiswerker die verbinding moeten krijgen met een kantoor. De *server* staat in het netwerk van de organisatie achter een *router*/*firewall*, die gebruikt wordt om het internet te delen en in zijn geheel af te schermen met een *firewall*. Maar het kan ook andersom: een VPN-client PC achter een *router*/*firewall* die met een *VPN-server* contact probeert te maken. Of een verbinding tussen twee netwerken met *routers*/*firewalls* waarbij de VPN-verbinding door de computers verzorgd wordt.



Deze configuraties kunnen werken, maar niet bij ieder type verbinding, *router* of *firewall* en VPN-programma. Er kunnen zich de volgende problemen voordoen:

- Het gebruikte protocol wordt niet door de router/firewall ondersteund;
- Het gebruikte VPN-algoritme kan niet altijd tegen NAT (*Network Address Translation*). Een voorbeeld hiervan is de *IPSec tunnel transport Mode* in combinatie met AH (*Authentication Header*) als transportprotocol; en

〉 In sommige gevallen kan een VPN-verbinding tussen computers tot stand worden gebracht door de router(s) transparant (als modem/*bridge*) in te stellen. In dat geval staat het netwerk mogelijk open voor de buitenwereld en moet de *VPN-server* een eigen *firewall* hebben.

2.3.2. Link met cryptografie als maatregel

Document '*Vo Informatieclassificatie – Minimale maatregelen – Cryptografie*' beschrijft de kwaliteitseisen waaraan encryptie en sleutelbeheer als bouwstenen van de minimale cryptografische maatregelen moeten voldoen.

VPN maakt gebruik van cryptografische technieken en sluit dus aan bij deze maatregel.

2.4. *Intrusion detection* als maatregel

Intrusion detection is een detectiemaatregel*Intrusion detection* (IDS) heeft als doel om op te merken wanneer een potentieel malafide activiteit plaatsvindt binnen het netwerk van een organisatie. Het is vervolgens aan de systeembeheerder om te onderzoeken wat er daadwerkelijk aan de hand is en om gepaste actie te ondernemen. Reageert een beheerder niet op een dergelijke alert, dan zal de aanval ook niet gestopt kunnen worden. Een IDS gaat dus nooit actief een aanval blokkeren.

Er bestaan verschillende oplossingen voor IDS. Welke oplossing geschikt is binnen een netwerk hangt af van de locatie binnen het netwerk en het doel van de IDS.

Een IDS op netwerkniveau (*network-based* IDS of netwerk-IDS) heeft geen kennis van de acties die op afzonderlijke systemen plaatsvinden maar ziet wel de datastromen die systemen met elkaar uitwisselen. Op basis van de inhoud van deze datastromen kan een IDS bepalen of er mogelijk sprake is van malafide communicatie.

Met de opkomst van draadloze netwerken is ook hiervoor een type IDS ontstaan dat zich richt op draadloze communicatie. Dit type IDS, een *wireless*-IDS, richt zich niet zozeer op de inhoud van de communicatie maar veel meer op de draadloze communicatie zelf. Zo is een *wireless*-IDS bijvoorbeeld in staat om *WEP cracking* (paswoordaanval), draadloze (D)DoS-aanvallen en het gebruik van zwakke versleuteling vast te stellen. In een omgeving waarin, naast bekabelde communicatie, ook draadloze netwerkcommunicatie plaatsvindt, vormen deze twee oplossingen een aanvulling op elkaar.

Een ander bijzonder type IDS dat met de toenemende populariteit van virtualisatie ontstaat, is de gevirtualiseerde IDS. Dit type IDS heeft als doel om detectie uit te voeren op de communicatie tussen virtuele systemen onderling. Een netwerk-based IDS werkt hier niet omdat de communicatie tussen virtuele systemen niet via het klassieke netwerk verloopt.

Een belangrijk voordeel van detectie op netwerkniveau ten opzichte van detectie op systeemniveau is de kosteneffectiviteit. Door detectie op netwerkniveau in te richten, is het mogelijk om in één keer detectie uit te voeren voor alle systemen die op dit netwerk zijn aangesloten. Om eenzelfde resultaat te bereiken met een systeem-gebaseerde oplossing, moet elk van de afzonderlijke systemen worden

voorzien van een IDS. Op het gebied van versleuteling heeft een systeem-IDS duidelijk voordelen omdat het systeem het begin- en eindpunt is van een versleutelde verbinding. Een systeem-IDS kan dus datastromen inzien voordat het wordt versleuteld of nadat het is ontcijferd. Een netwerk-IDS heeft hier problemen mee.

Een netwerk-gebaseerd IDS plaatst men over het algemeen niet *inline* maar *out-of-band*. Bij *out-of-band* plaatsing neemt het IDS geen actieve rol in het netwerk in, maar verkrijgt het een kopie van de datastromen. Bij *inline*-plaatsing staat de IDS in het netwerk pad en verwerkt de actieve data. Een voordeel van een *inline* geplaatst netwerk-gebaseerd IPS is dat het nooit datastromen zal missen. Immers, alle datastromen moeten hierbij door het systeem heen gaan. Bij *out-of-band*-plaatsing bestaat altijd de kans dat trafiek wordt gemist. Dit gebeurt bijvoorbeeld op het moment dat de belasting op een *switch* of *router* te hoog wordt en de *switch*/*router* daardoor niet alle trafiek meer kopieert naar de IDS.

2.5. Inbraakpreventie als maatregel

Inbraakpreventie is een preventieve maatregel

2.5.1. *Firewall*

Een *firewall* controleert internetverkeer en laat het door of blokkeert het, op basis van een aantal parameters. Op deze manier werkt een *firewall* op een preventieve manier door aanvallen te blokkeren vooraleer ze op het netwerk komen. De *firewall*-configuratie omvat een aantal filters. Filteren op poort betekent dat datastromen worden geblokkeerd of toegestaan op verschillende poorten. Door te filteren op bekende poorten gelinkt aan bepaalde protocollen zoal FTP, http, enz wordt het gebruik van die protocollen toegestaan of verboden. Filteren op IP-adres kan ook, net als filteren op domeinnaam (webadres) waardoor de toegang tot specifieke websites geblokkeerd kan worden.

De kerntaak van een *firewall* is het regelen en opvolgen van datastromen tussen netwerksegmenten, bv. tussen internet en een DMZ of tussen een DMZ en het interne netwerk. Dit houdt in:

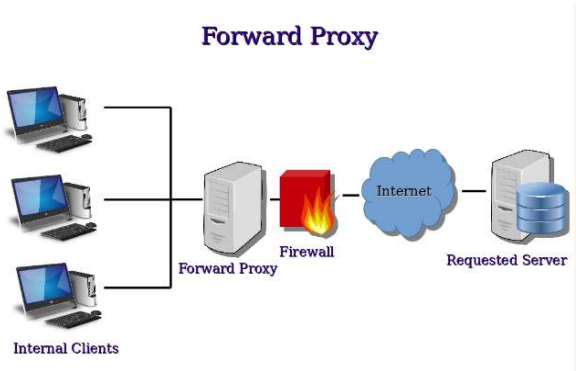
- Toestaan of verbieden van connectie verzoeken;
- Bewaken van het protocol na het opbouwen van een (toegestane) verbinding; en
- *Logging* van de gebeurtenissen met betrekking tot de firewall en de datastromen.

Net zoals bij IDS is een netwerk firewall niet in staat om virtuele systemen te beveiligen en moet men hier beroep doen op virtuele firewall systemen.

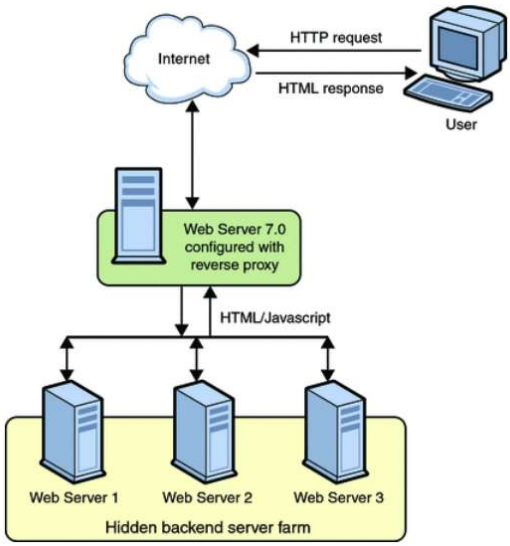
2.5.2. *Proxyserver*

Een ***proxyserver*** is een server die als 'tussenpersoon' optreedt en aanvragen aanneemt en doorstuurt naar de doelcomputer. Een *proxyserver* komt in twee vormen: *forward proxy* en *reverse proxy*. Het verschil tussen beide wordt bepaald door het standpunt van implementatie. De *forward proxy* behandelt vragen uit het eigen organisatie netwerk, de *reverse proxy* uit het publieke netwerk.

Een ***forward proxy*** kanaliseert alle aanvragen van gebruikers en stuurt die met een eigen afzendadres door naar de 'doelservers' op het publieke netwerk (meestal het internet). Antwoorden van de *servers* bereiken eerst de *proxy* voor ze worden gedirigeerd naar de diverse gebruikersapparatuur. Door als tussenpersoon op te treden kan de *proxyserver* niet alleen garanderen dat gebruikers anoniem blijven maar ook dat er bijkomende controles (bv. op *malware*) op de ontvangen informatie wordt uitgevoerd alvorens deze doorgestuurd wordt naar de gebruiker. Een *forward proxy* wordt vaak ook gewoon *proxyserver* genoemd.



Een ***reverse proxy*** is een extra veiligheidsmaatregel die voor een of meerdere *webservers* ingeschakeld kan worden. Een webadres wordt in de omgekeerde richting van een *forward proxy* omgezet. Een *reverse proxy* neemt plaatsvervangend de aanvragen van *servers* aan en leidt ze naar de bijbehorende aanvrager. De *reverse proxy* vormt daarbij, net als een *forward proxy*, de enige verbinding tussen internet en het privénetwerk. Door deze consolidatie is het mogelijk om het inkomende dataverkeer extra te controleren, meerdere *servers* onder dezelfde URL (*Uniform Resource Locator*) beschikbaar te stellen, aanvragen gelijkmatig te verdelen over de verschillende *servers* en het ophalen van gegevens te versnellen met behulp van *caching*.



2.5.3. *Intrusion prevention* systemen (IPS)

Een *intrusion prevention* systeem (IPS) heeft als doel om kwaadaardige datastromen te blokkeren terwijl een *intrusion detection* systeem (IDS) deze datastromen alleen wil detecteren (inzichtelijk maken) om hier vervolgens over te rapporteren. Een IDS en een IPS maken wel gebruik van dezelfde technieken, waardoor een IPS in feite een IDS is met extra's, namelijk de mogelijkheid tot het blokkeren van de gedetecteerde aanvallen. Hoewel in het verleden het verschil tussen een IDS en IPS nog expliciet bestond, is dit verschil tegenwoordig veel minder aanwezig. Standaard is vaak sprake van een IPS, maar door dit IPS anders te configureren, en op een andere manier aan het netwerk te koppelen, functioneert het systeem als een IDS.

Een IPS levert naast detectie ook bescherming tegen potentiële aanvallen aangezien een IPS aanvallen daadwerkelijk kan blokkeren, terwijl een IDS deze alleen kan detecteren en dus geen automatische acties onderneemt om de impact van de aanval te beperken. Zolang het IPS aanvallen terecht blokkeert, vormt het systeem een waardevolle toevoeging op de beveiliging van het netwerk. Wanneer het IPS echter te veel vals-positieven genereert, zorgt dit ervoor dat verbindingen, processen of bestanden onterecht geblokkeerd worden.

Om datastromen te kunnen blokkeren wordt een netwerk-IPS *inline* in het netwerk geplaatst. Bij *inline*-plaatsing moeten alle datastromen door het IPS heen stromen en enkel zo kan het IPS ingrijpen zodra het verdacht verkeer waarneemt.

Een traditioneel netwerk-based IPS volstaat niet in virtuele omgevingen: hier heeft men een virtuele IPS nodig.

2.6. SSL-inspectie als maatregel

SSL-inspectie is een detectiemaatregel.

SSL-/ TLS-inspectie (*Secure Sockets Layer/Transport Layer Security* inspectie) is een techniek die al lang bestaat maar die men steeds vaker implementeert. Het internetverkeer gaat via een *firewall*, een website of internetapplicatie. Voorheen gingen deze datastromen over een niet-versleutelde HTTP-verbinding en was dus eenvoudig te controleren en tegen te houden in geval van ongewenste inhoud (bv. *malware*). Tegenwoordig is een versleutelde HTTPS-verbinding eerder de norm dan uitzondering. Aangezien HTTPS-datastromen versleuteld zijn, is het moeilijk om *malware* in dit verkeer te detecteren en is er geen controle mogelijk op de informatie die verzonden wordt naar een derde partij. SSL-inspectie biedt hierop een antwoord.

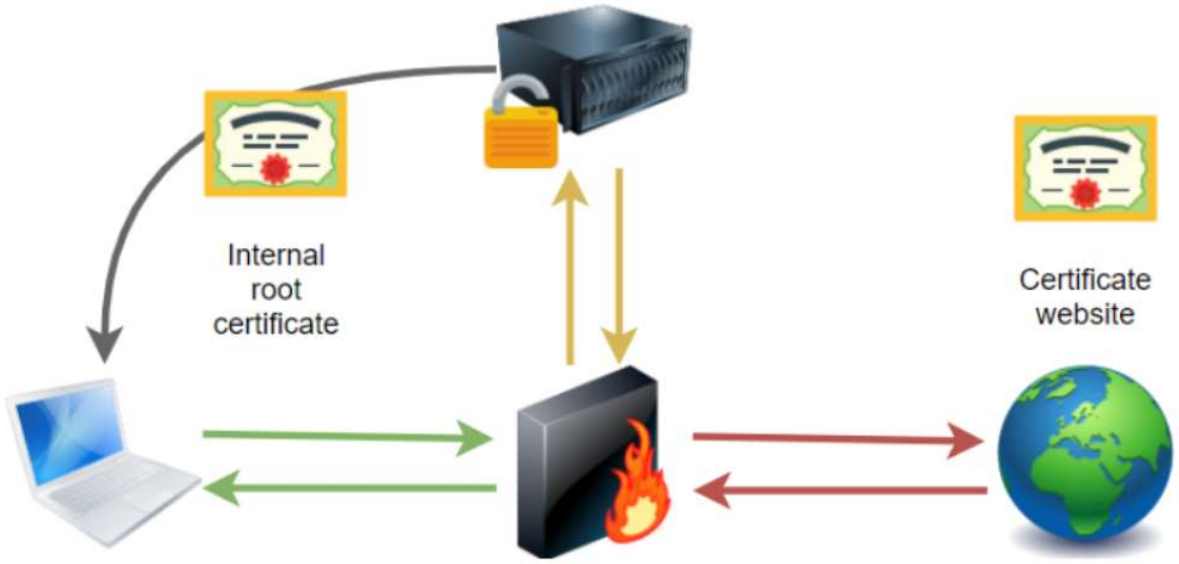
SSL-inspectie is geen alleenstaande maatregel maar dient ter ondersteuning van maatregelen zoals *antimalware*, IDS en IPS.

De toepassing van SSL-inspectie als mitigerende maatregel hangt onder meer af van de klasse van informatie; sommige informatie wenst men niet aan SSL-inspectie te onderwerpen omdat het risico op niet-geautoriseerde toegang door middel van de SSL-inspectie te groot is.

2.6.1. Uitgaande datastromen

Om SSL-inspectie te kunnen toepassen is er een zogenaamde *Man in the Middle* nodig. Deze *Man in the Middle* is vaak een *prox server* die de versleutelde datastromen opvangt en ontcijfert zodat de inhoud kan worden geanalyseerd. Vervolgens gaat het gecontroleerde verkeer verder naar de bestemmeling. Om dit zonder SSL-foutmeldingen op de gebruikersapparatuur te realiseren in geval van uitgaande datastromen, is er een interne *certificate authority* (CA) nodig met een eigen *root*-

certificaat. Vaak zit deze functionaliteit in de *firewall* zelf. Het *root*-certificaat moet op de betrokken apparatuur geïnstalleerd worden.



Om SSL-inspectie technisch toe te kunnen passen zijn dus volgende componenten nodig in het netwerk:

- Een ***prox server***, dit is nodig om de datastromen te kunnen scannen op *malware*, virussen en documenten die het bedrijf niet via het internet mogen verlaten;
- Een interne ***certificate authority*** met een geldig zelf gegenereerd (*self signed*) ***root*-certificaat** geïnstalleerd op de betrokken apparatuur; en
- Een ***firewall*** die bijvoorbeeld de https-datastromen transparant doorstuurt naar de *proxyserver*, of **instellingen in de browsers** binnen het netwerk waarin staat dat de *proxyserver* gebruikt moet worden.

2.6.2. Inkomend verkeer

In geval van inspectie op inkomende datastromen is geen *root*-certificaat en interne CA nodig.

2.7. *Content/URL filtering* als maatregel

Content/URL filtering is een preventieve en een reactieve maatregel.

Meer en meer worden diensten of informatie aangeboden via internet. Het is dan ook ondenkbaar dat men deze toegang zou ontzeggen. Aan de andere kant wordt de kans op misbruik steeds groter. Het is evident dat illegale of ongepaste websites geblokkeerd worden. Maar ook toegang verbieden tot sociale netwerken en tot websites niet gerelateerd aan de kernactiviteiten van de organisatie kan deel uitmaken van het beleid.

Om dit beleid technisch af te dwingen biedt *content filtering* en/of *URL-filtering* een oplossing. Dit biedt de mogelijkheid te bepalen wie waar op internet mag en kan. In theorie kan dit ook geregeld

worden in de *firewall*: men kan in de filter immers aanduiden welke websites bezocht mogen worden en welke niet. In de praktijk is het opzetten en onderhouden van zo'n lijst ondoenbaar: er zijn te veel malafide websites en bovendien veranderen ze frequent van domeinnaam. Daar kan de *content/URL filter* bij helpen.

Surfen op internet wordt door de *content/URL filter* onder andere voortdurend vergeleken met een lijst van meer miljoenen websites. Deze websites zijn in categorieën ingedeeld. Per persoon of groep van personen wordt bepaald tot welke categorie gebruikers al dan niet toegang hebben. Er wordt gecontroleerd of een persoon toestemming heeft om op deze categorie te surfen. De *database* waarop de *content/URL filter* steunt, wordt voortdurend bijgewerkt (te vergelijken met de *signature database* van *signature* gebaseerde *antimalware software*).

Content/URL filters worden ook vaak als bijkomende *antimalware*-maatregel aanzien – naast de gekende *antimalware software* – omdat deze filters de toegang blokkeren tot websites die vaak als *hosts* voor *malware* worden gebruikt. Sommige filters kunnen zelfs informatie blokkeren die via internet wordt verzonden, om ervoor te zorgen dat bepaalde gegevens niet worden vrijgegeven.

Er bestaan verschillende methoden om te beoordelen of een bepaalde website aan de gebruiker getoond mag worden. De meest toegepaste methoden zijn de volgende:

- Controleren of de site op de vooraf samengestelde ***whitelist*** met toegestane websites staat;
- Controleren of de site op de vooraf samengestelde ***blacklist*** met verboden websites staat;
- Controleren of de betreffende website door de uitgever voorzien is van een **classificeringslabel**, bijvoorbeeld een ICRA-label; en
- Controleren of in de **inhoud** van de website bepaalde niet-toegestane woorden voorkomen.

De meeste *content/URL filters* gebruiken een combinatie van de hierboven genoemde filtermethoden.

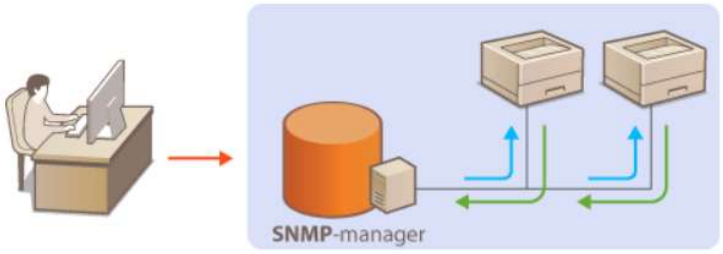
De *URL-filter* kijkt naar de URL van de gewenste site en bepaalt of de verbinding wordt geblokkeerd of toegestaan. Filters worden vaak geïnstalleerd als *browser*-uitbreiding, als zelfstandig computerprogramma of als onderdeel van een uitgebreide beveiligingsoplossing. Organisaties kunnen filters echter ook in het netwerk installeren om de internettoegang van meerdere gebruikers tegelijk te beperken. Sommige zoekmachines bevatten ook eenvoudige filters om ongewenste pagina's uit de zoekresultaten te verwijderen.

Er zijn echter manieren om *content/URL filters* te omzeilen, zoals het gebruik van een web-gebaseerde *proxy*, het gebruik van websites in een andere taal, of het creëren van een VPN naar een persoonlijke *proxyserver*.

2.8. *Logging* als maatregel

Logging is een reactieve maatregel.

Logging is het verzamelen en beoordelen van systeemdata en waarschuwingen van – in de context van dit document – netwerkinfrastructuur. SNMP (*Simple Network Management Protocol*) wordt hiervoor vaak ingezet. SNMP is een protocol voor het bewaken en aansturen van apparatuur in een netwerk.



Met het SNMP-protocol kan op een eenvoudige manier bijvoorbeeld de status van een *disk* opgevraagd worden of de hoeveelheid datastromen over een netwerk. Bijna iedere leverancier ondersteunt dit protocol dat via SNMP-*agents* het netwerk monitort en hieruit statistische informatie genereert. Het is een populair protocol om vanop afstand te monitoren en aan te sturen. Bij fouten kan een centraal managementsysteem verwittigd worden aan de hand van speciale berichten.

Naast SNMP wordt ook vaak met *syslogs* gewerkt. *Syslog* is een standaard client-/*server*-protocol voor het loggen van berichten. Het wordt ondersteund door een groot aantal architectuurcomponenten en platformen. De *syslog* van de client stuurt kleine tekstberichten van gebeurtenissen naar de *syslog*-ontvanger (*syslog daemon* of *syslog server*). Transport van deze tekstberichten kan bovendien beveiligd worden door gebruik te maken van SSL. De verzamelde logmeldingen kunnen eenvoudig centraal opgeslagen worden en gekoppeld aan alarmering functionaliteit (bv. via SMS of e-mail) of doorgestuurd naar een SIEM-oplossing.

Meer details over het opzetten van *logging* en SIEM (*Security Information and Event Management*) is beschreven in het document 'Vo Informatieclassificatie – minimale maatregelen – veiligheidslogging en monitoring'.

2.9. *High availability* als maatregel

Het belang van netwerkconnectiviteit kan niet overschat worden. Het netwerk is immers één van de basiscomponenten die zorgen voor beschikbaarheid van informatie en informatie verwerkende systemen, d.w.z. de gebruiker in staat stellen om informatie te verwerken op het ogenblik dat hij/zij die nodig heeft. Een infrastructuur met hoge garanties op beschikbaarheid van het netwerk is daarom vaak onmisbaar.

Om dit te bereiken, worden drie principes toegepast:

- Eliminatie van *single points failure*: ervoor zorgen dat onbeschikbaarheid van één enkele component (een *firewall*, een netwerkverbinding) geen impact heeft op de beschikbaarheid van de informatie door middel van ontdubbeling en/of inbouwen van redundantie (software- en hardwareredundantie);
- Betrouwbare *failover* in redundant opgezette netwerken: vaak is de *failover* van een falende component naar zijn redundante evenknie een *single point of failure* op zich; en
- Snelle en betrouwbare detectie van onbeschikbaarheden: incidenten die te maken hebben met onbeschikbaarheid van componenten moeten tijdig ontdekt en opgelost worden zonder impact op de eindgebruikers.

Het garanderen van *high availability* kan op verschillende niveaus:

- Door componenten uit te breiden, zowel horizontaal (toevoegen van extra componenten) als verticaal (toevoegen van extra CPU, RAM, …);
- Door toepassingen te implementeren op verschillende *servers* in plaats van op één *server*;

- Door het opzetten van *load balancing*: *load balancers* verdelen de trafiek over verschillende componenten, bv. over verschillende *firewalls* zodat deze niet als *single point of failure* optreedt;
- Door het toepassen van *clustering*: *high availability*-clusters zijn opgezet als een redundante set van componenten met dezelfde functionaliteiten, zodat deze functionaliteiten hoog beschikbaar kunnen worden aangeboden aan de eindgebruiker.

Naast deze specifieke technische oplossingen mogen volgende elementen zeker niet ontbreken om de beschikbaarheid van het netwerk te optimaliseren:

- *Antimalware*: om *malware*-aanvallen zoals (D)DoS tijdig te stoppen;
- Incidentbeheer: om onbeschikbaarheden tijdig aan te pakken; en
- (Capaciteits-)*monitoring*: om tijdig in te grijpen vooraleer onbeschikbaarheid een probleem wordt.

2.10. Virtuele netwerken/*cloud computing*

Virtuele netwerken zijn netwerken die niet gevormd worden door middel van fysieke verbindingen, maar door middel van protocollen (VLAN, VPN, …) of virtuele machines.

De eerste vorm – gebaseerd op protocollen – is reeds besproken in het voorgaande, in dit hoofdstuk gaan we wat dieper in op virtualisatie, een techniek die veel gebruikt wordt in *cloud computing*.

Virtuele machines staan lijnrecht tegenover fysieke machines. Waar op fysieke machines slechts één OS operationeel is, kunnen er meerdere OS-instanties (of virtuele machines) gelijktijdig werken op een fysieke machine die is ingericht op basis van virtualisatie. Op die manier is het mogelijk om meerdere virtuele computers te laten werken op één hardwarecomponent.

Virtualisatie creëert een tussenlaag tussen het OS en de onderliggende hardware. Deze laag simuleert de capaciteiten van de hardware (CPU, werkgeheugen, …) waardoor deze als het ware opgesplitst kan worden in meerdere virtuele machines op dezelfde hardware. Op deze manier kan de hardware optimaal ingezet worden. Kenmerkend van deze virtuele opzet is de isolatie tussen de verschillende virtuele machines. Zij gedragen zich onafhankelijk van elkaar, dus als aparte machines, dat wil zeggen:

- Iemand die toegang heeft tot één bepaalde VM (virtuele machine), heeft niet automatisch toegang tot een andere VM;
- Problemen met één VM staan los van de andere VMs; en
- De prestaties van één VM worden niet beperkt of geschaad door de andere VMs.

Door middel van virtualisatie is het mogelijk om schaalbaar online-dienstverlening aan te bieden.

2.10.1. Beveiliging van de virtuele wereld

In feite kunnen virtuele machines net zo ingericht en beveiligd worden als fysieke machines. Zo kan men onder meer:

- Netwerksegmentatie opzetten;
- *Firewalls*, IDS/IPS inzetten om netwerktrafiek te controleren; en
- *Antimalware* inzetten om *malware* tegen te houden.

Natuurlijk zijn hiervoor andere producten nodig dan voor de beveiliging van fysieke machines, maar de principes en de logische architectuur zijn dezelfde.

Bij virtuele machines moet echter wel rekening gehouden worden met een extra component: de *hypervisor*. Deze dient om de virtuele laag te creëren en beheren. Aangezien deze *hypervisor* dient om deze virtuele wereld in te richten en te beheren, is het duidelijk dat deze goed beveiligd moet zijn. Immers, indien een aanvaller toegang krijgt tot de *hypervisor*, krijgt deze toegang tot alle onderliggende VMs. Beveiliging van de *hypervisor* houdt volgende goede praktijken in:

- Inrichten van (*security*) *monitoring* – koppelen aan SIEM;
- *Hardening* van de *hypervisor* (schakel onnodige services en eigenschappen uit);
- Toepassen van PAM – beheer van geprivilegieerde accounts;
- Fysieke en logische toegangsbeveiliging toepassen; en
- Goed ingerichte processen voor beheer: *patch management*, wijzigingsbeheer, incidentbeheer, enz.

Gezien het belang van de *hypervisor* is het aangewezen om deze component minstens de vertrouwelijkheidsklasse 4 en integriteitsklasse 4 te geven. De beschikbaarheidsklasse is minstens één klasse hoger dan de hoogste informatieklasse op de VMs beheerd door de *hypervisor*.

2.10.2. Online dienstverlening – *cloud computing*

We onderscheiden diverse *as-a-service*-modellen, waarvan de meest gebruikelijke zijn:

- IaaS (*infrastructure-as-a-service*): aanbieden van virtuele infrastructuur componenten zoals virtuele *servers*, netwerken, opslagcapaciteit, enz.;
- PaaS (*Platform-as-a-Service*): aanbieden van een aantal diensten bovenop de infrastructuur die het mogelijk maakt om toepassingen op een gestructureerde en geïntegreerde wijze te ontwikkelen zoals toegangsbeheer, identiteitsbeheer, portaalfunctionaliteit, enz.; en
- SaaS (*Software-as-a-Service*): aanbieden van eindtoepassingen zoals e-mail, klantenbeheer, personeelsbeheer, videoapplicaties, enz.

Deze *as-a-service*-modellen kunnen aangeboden worden in verschillende types cloudoplossingen:

- Publiek: de software en data staan op infrastructuur van een externe dienstverlener (= buiten de eigen organisatie) en er wordt een generieke dienstverlening afgeleverd;
- Privaat: de software en data staan op eigen fysieke of virtuele infrastructuur, d.w.z. de eigen organisatie heeft volledige controle over de data, beveiliging en kwaliteit van de dienstverlening en deze wordt niet gedeeld met andere externe partijen. Het beheer kan uitbesteed worden aan een externe dienstenleverancier en de infrastructuurcomponenten kunnen geïnstalleerd worden in de gebouwen van de organisatie of van een externe dienstenleveranciers;
- Gemeenschappelijk: afnemers uit verschillende organisaties werken op dezelfde infrastructuur. Dit is mogelijk omdat deze afnemers elkaar voldoende vertrouwen en/of vergelijkbare eisen stellen aan de *cloud*-omgeving, bv. een groep overheidsinstellingen of onderwijsinstellingen; en
- Hybride: het samen gebruiken van een meerdere interne/externe *cloud*-omgevingen.

2.10.3. Voordelen van *cloud*

Er zijn diverse overwegingen om over te stappen in een *cloud*-dienstverlening, waarvan de belangrijkste zijn:

- Schaalbaarheid: door het toepassen van virtualisatie is het mogelijk om snel en vrij eenvoudig meer of minder van een bepaalde dienstverlening te gebruiken, bv. meer of minder *servers*, meer of minder netwerkcapaciteit. Dit kan ook een voordeel zijn om piekmomenten op te vangen;
- Kostprijs: voor de organisatie is er geen aankoop- en onderhoudskost van de infrastructuur die de dienstverlening nodig heeft;
- Locatie-onafhankelijkheid: vaak volstaat een internetverbinding en een browser om gebruik te kunnen maken van de dienstverlening. Is er toch een speciale toepassing nodig, dan is die meestal eenvoudig te downloaden;
- Betrouwbaarheid: omdat de dienstverlener over gespecialiseerde deskundigen beschikt, zijn complexe problemen vaak sneller opgelost dan wanneer de organisatie deze zelf moet aanpakken. Het beheer en aanbieden van de dienstverlening behoort tot de kerntaak van de dienstverlener. Daar tegenover staat dat men afhankelijk is van de dienstverlener: de organisatie staat machteloos tot de dienstverlener het probleem oplost; en
- Beschikbaarheid: vaak is de infrastructuur van de dienstverlener gespreid over meerdere *datacenters*, waardoor een hoge mate van beschikbaarheid gegarandeerd kan worden.

2.10.4. Risico's van *cloud*

Er zijn wel wat risico's verbonden aan het uitbesteden van diensten die vertrouwelijke informatie kunnen bevatten:

- **Wetgeving**: sommige nationale wetten stellen bepaalde eisen aan de opslag en verwerking van data die soms tegenstrijdig zijn. Zo stelt de GDPR heel wat eisen en legt verantwoordelijkheden op bij de verwerking van persoonsgegevens. Daar tegenover staat de Amerikaanse 'Patriot Act' die gericht is op het bestrijden van terrorisme en een verregaande toegang tot data toelaat door Amerikaanse overheden, zelfs als die data zich buiten USA bevindt;
- **Juridische aspecten** zijn er o.a. op gebied van eigendom van data en toepassingen. Veel landen hebben eigen regels over het opslaan van data (locatie en duurtijd). Dit is lastig om af te dwingen;
- De beveiliging van de informatie is geheel of gedeeltelijk **afhankelijk van de dienstverlener**; en
- Indien de dienstverlening stopt of bij een faillissement van de dienstverlener loopt de organisatie het risico dat de toepassingen en data (tijdelijk) onbeschikbaar worden.

Het mag duidelijk zijn dat de organisatie voldoende maatregelen moet nemen in haar informatiebeveiliging om de vertrouwelijkheid, integriteit en beschikbaarheid van haar data veilig te stellen. Wanneer het gaat over data in de *cloud*, speelt nog een vierde factor mee: betrouwbaarheid. Betrouwbaarheid en controleerbaarheid gaan hand in hand. Een informatiebeveiliging is betrouwbaar als ze controleerbaar is, met andere woorden als met voldoende zekerheid kan worden gestaafd dat er voldaan is aan de eisen van vertrouwelijkheid, integriteit en beschikbaarheid.

Het gaat ons echter te ver om hier dieper in te gaan op juridische maatregelen, deze zijn dan ook buiten scope van dit document. We leggen de focus op technische en organisatorische maatregelen.

2.10.5. Vertrouwelijkheid van data in de cloud

Op zich zijn de maatregelen voor de *cloud* en voor virtuele netwerken niet anders dan voor 'in huis'-/fysieke oplossingen, dat wil zeggen de maatregelen die eerder in dit document beschreven werden, zijn ook hier van toepassing.

Maar we leggen een aantal accenten. Specifiek voor vertrouwelijkheid houdt dit het volgende in:

- **Netwerkzonering** dringt zich sterk op, met name om de scheiding met andere klanten van de *cloud provider* mogelijk te maken;
- **Toegangscontrole** is belangrijk: er moet immers worden gewaarborgd dat alleen de afnemer en diens gemachtigde gebruikers technisch toegang hebben tot de data;
- **Controle op gebruik van geprivilegieerde rechten**: even belangrijk is de beperking van en controle op het beheer van de (virtuele) omgeving, hiervoor zijn immers vaak geprivilegieerde *accounts* nodig;
- **Controle op de werking van de toegangscontrole via *logging***: om de technische controle van de werking van deze maatregel, is *logging* nodig. Met behulp van *logging* kunnen alle handelingen die gebeuren op de data bijgehouden worden; en
- Cryptografische beveiliging – **beheer van encryptiesleutels**: vaak wordt encryptie aangeboden door de *cloud provider* en kan men versleutelen van data in de *cloud* als dienst afnemen. Nadelig is het feit dat de encryptiesleutels dan in het bezit zijn van de *cloud provider*. Daardoor bestaat de kans dat de *cloud provider* gedwongen kan worden om de sleutels af te staan (bv. door de overheid), waarmee de vertrouwelijkheid van de data geschonden kan worden. Met name heerst de bezorgdheid dat buitenlandse overheden inzage zouden krijgen in de data. Door de encryptiesleutels in eigen beheer of in beheer van een vertrouwde partij te leggen, kan men dit risico mitigeren.

2.10.6. Integriteit van data in de *cloud*

De opmerkingen voor vertrouwelijkheid van data in de *cloud* gelden ook als het gaat over integriteit van data in de *cloud*.

2.10.7. Beschikbaarheid van data in de *cloud*

Beschikbaarheid is vaak een goede reden om data onder te brengen in een *cloud*-oplossing. In het algemeen bieden *cloud providers* een hoog beschermingsniveau tegen onbeschikbaarheid van data en dataverwerkende systemen wanneer zij in de *cloud* zijn ingericht. Dit behoort immers tot één van de kerntaken van de *cloud provider*.

Ook hier kan men stellen dat de maatregelen beschreven in voorgaande paragrafen om hoog beschikbare toepassingen mogelijk te maken, geldig blijven in de *cloud*-omgeving.

2.10.8. Betrouwbaarheid van data in de *cloud*

Een afnemer kan diverse maatregelen overwegen om de betrouwbaarheid in de *cloud* te verhogen:

- **Certificeringen**: er bestaan heel wat internationaal erkende certificeringen, ISO27001 is een wijd gebruikte norm waartegen een *cloud provider* zich kan laten certificeren. Een belangrijk aandachtspunt is de scope van het certificaat. Een *cloud provider* kiest namelijk zelf welke dienst of onderdeel van een dienst hij wil laten certificeren. Daardoor bestaat het risico dat bepaalde diensten niet zijn gecontroleerd en niet voldoen, terwijl de aanwezigheid van een certificaat misschien wel die indruk wekt;

- **Auditeerbaarheid** van de *cloud provider*: het (laten) uitvoeren van audits door de afnemer verhoogt de controleerbaarheid en dus ook de betrouwbaarheid van de *cloud provider*. Het recht op audits moet dan wel contractueel vastgelegd zijn;
- Het opzetten van ***logging* en periodiek analyseren van de loginformatie** verhoogt eveneens de controleerbaarheid van de *cloud provider*;
- ***Exit*-procedure**: door de data en hun ondersteunende infrastructuur bij een *cloud provider* te plaatsen, wordt de afnemer afhankelijk van het voortbestaan van de dienstverlening. Een degelijke *exit*-procedure is dan ook belangrijk én deze moet contractueel afdwingbaar zijn;
- **Onafhankelijkheid van de *cloud provider***: door de data en hun ondersteunende infrastructuur bij een *cloud provider* te plaatsen, wordt de afnemer afhankelijk van het voortbestaan van de *provider* zelf. Een faillissement van de *cloud provider* kan de afnemer voor grote problemen stellen. Hiertegen kan de afnemer zich wapenen door back-ups te bewaren bij een andere partij dan de *cloud provider*; en
- Tenslotte kan de afnemer zich enigszins wapenen tegen inzage door buitenlandse autoriteiten door enerzijds niet te kiezen voor een *cloud provider* zonder vestiging in de EU en anderzijds door cryptografische beveiliging van de data in de *cloud* waarbij het sleutelbeheer niet in handen is van de *cloud provider*.