Informatieclassificatie Vlaamse overheid (Vo-ICR)

ICT-systemen

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

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 ICT-systemen. 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 tweede 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	18 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)

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

Inhoudsopgave

INLEIDING

Dit document beschrijft de maatregelen die we nemen om ICT-systemen die geen gebruikersapparatuur zijn, te beveiligen. Gebruikersapparatuur zijn hardware zoals laptops, smartphones, enzovoort die specifiek door eindgebruikers gebruikt worden. We beperken ons in dit document bovendien tot hardware en besturingssystemen (OS) van ICT systemen.

Vele maatregelen zijn inzetbaar op netwerkniveau (*network base)* én op systeemniveau (*host-based*). 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 systeem-gebaseerde oplossingen besproken, maar netwerk-gebaseerde maatregelen zijn nodig om restrisico's op het netwerk te mitigeren.

Meer informatie is te vinden in '<u>Vo informatieclassificatie – minimale maatregelen – netwerken</u>'.

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: ***Patching* en *hardening***: 〉 Besturingssystemen van ICT-systemen moeten up-to-date zijn (dus niet kwetsbaar voor gekende kwetsbaarheden ondersteund door leverancier); 〉 Beveiligingsupdates dienen zo snel mogelijk geïnstalleerd te worden; 〉 Er worden alleen protocollen gebruikt die nodig zijn voor de benodigde functionaliteit, andere protocollen worden verwijderd of *disabled*; 〉 Alle onnodige services dienen uitgezet te worden; 〉 Toepassen van een goedgekeurd en up-to-date paswoordbeleid voor systeemaccounts en voor geprivilegieerde accounts, dit houdt o.a. in dat alle paswoorden ingesteld door derden (bv. leveranciers) dienen te worden gewijzigd; 〉 Voor het beheer van ICT-systemen zijn geprivilegieerde accounts nodig, beheer van deze accounts moet via PAM-proces: zie ook document 'Vo Informatieclassificatie – minimale maatregelen – PAM'; en 〉 Indien IDS/IPS/*antimalware*-oplossingen aanwezig zijn, dienen deze periodiek updates te ontvangen via een automatisch proces. **Detectie**: 〉 Host-based IDS inzetten op hosts in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based IDS versleutelde trafiek te inspecteren. **Inbraakpreventie**: 〉 Host-based firewall inzetten op hosts in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based firewall versleutelde trafiek te inspecteren. 〉 Host-based IPS inzetten op hosts in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based IPS versleutelde trafiek te inspecteren. ***Antimalware***: 〉 Alle datastromen die het ICT-systeem 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. ***Logging***: 〉 *Event logging* wordt opgezet op kritische ICT-systemen; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo Informatieclassificatie – minimale maatregelen – PAM'; 〉 Zie ook document 'Vo Informatieclassificatie – minimale maatregelen – SIEM.'
	Alle maatregelen van Klasse 1 / Klasse 2 + **Interne controle op kwetsbaarheden**: 〉 Zie document 'Vo informatieclassificatie – minimale maatregelen – veiligheidstesten'.
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **Interne controle op kwetsbaarheden**: 〉 Zie document 'Vo informatieclassificatie – minimale maatregelen – veiligheidstesten'. ***Logging***: 〉 *Event logging* wordt opgezet voor alle ICT-systemen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.

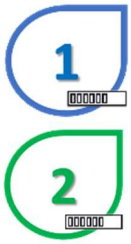
Integriteit

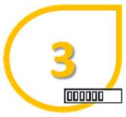
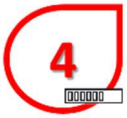
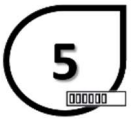
IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: ***Patching* en *hardening***: 〉 Besturingssystemen van ICT-systemen moeten up-to-date zijn (dus niet kwetsbaar voor gekende kwetsbaarheden ondersteund door leverancier); 〉 Beveiligingsupdates dienen zo snel mogelijk geïnstalleerd te worden;

	〉 Er worden alleen protocollen gebruikt die nodig zijn voor de benodigde functionaliteit, andere protocollen worden verwijderd of *disabled*; 〉 Alle onnodige services dienen uitgezet te worden; 〉 Toepassen van een goedgekeurd en up-to-date paswoordbeleid voor systeemaccounts en voor geprivilegieerde accounts, dit houdt o.a. in dat alle paswoorden ingesteld door derden (bv. leveranciers) dienen te worden gewijzigd; 〉 Voor het beheer van ICT-systemen zijn geprivilegieerde accounts nodig, beheer van deze accounts moet via PAM-proces: zie ook document 'Vo Informatieclassificatie – minimale maatregelen – PAM'; en 〉 Indien IDS/IPS/*antimalware*-oplossingen aanwezig zijn, dienen deze periodiek updates te ontvangen via een automatisch proces. **Detectie**: 〉 Host-based IDS inzetten op hosts in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based IDS versleutelde trafiek te inspecteren. **Inbraakpreventie**: 〉 *Host-based firewall* inzetten op hosts in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based firewall versleutelde trafiek te inspecteren. 〉 *Host-based* IPS inzetten op *hosts* in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based IPS versleutelde trafiek te inspecteren. ***Antimalware***: 〉 Alle datastromen die het ICT-systeem 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. ***Logging***: 〉 *Event logging* wordt opgezet op kritische ICT-systemen; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo Informatieclassificatie – minimale maatregelen – PAM'; 〉 Zie ook document 'Vo Informatieclassificatie – minimale maatregelen – SIEM.'

	Alle maatregelen van Klasse 1 + Klasse 2 + **Interne controle op kwetsbaarheden**: 〉 Zie document 'Vo informatieclassificatie – minimale maatregelen – veiligheidstesten'.
	Klasse 4 en Klasse 5 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 / Klasse 2 + Klasse 3 + **Interne controle op kwetsbaarheden**: 〉 Zie document 'Vo informatieclassificatie – minimale maatregelen – veiligheidstesten'. ***Logging* en *monitoring*:** 〉 *Event logging* wordt opgezet voor alle ICT-systemen; en 〉 IDS/IPS-*use cases* moeten beschikbaar zijn voor SIEM.

Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 en Klasse 2 kennen dezelfde maatregelen: **Detectie**: 〉 Host-based IDS inzetten op hosts in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based IDS versleutelde trafiek te inspecteren. **Inbraakpreventie**: 〉 *Host-based firewall* inzetten op hosts in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based firewall versleutelde trafiek te inspecteren. 〉 *Host-based* IPS inzetten op *hosts* in hoog-risico omgevingen zoals bvb DMZ als het niet opportuun is om via netwerk-based IPS versleutelde trafiek te inspecteren. ***Antimalware***: 〉 Alle datastromen die het ICT-systeem 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. ***Logging***: 〉 *Event logging* wordt opgezet op kritische ICT-systemen; 〉 Voor *logging* van toegangsbeheer: zie document 'Vo Informatieclassificatie – minimale maatregelen – PAM'; 〉 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 + **Interne controle op kwetsbaarheden**: 〉 Zie document 'Vo informatieclassificatie – minimale maatregelen – veiligheidstesten'. ***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 + **Interne controle op kwetsbaarheden**: 〉 Zie document 'Vo informatieclassificatie – minimale maatregelen – veiligheidstesten'.

1.2 Minimale specifieke (GDPR) maatregelen

Er zijn geen minimale specifieke maatregelen voor GDPR rond ICT-systemen.

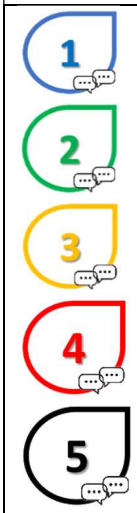
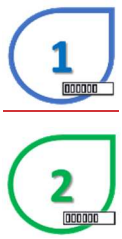
1.3 Minimale specifieke (NISII) maatregelen

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

1.4 Minimale specifieke (KSZ) maatregelen

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

Beschikbaarheid, Integriteit en vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: Elke organisatie moet: 〉 De eigen mobiele toestellen duidelijk identificeren, veilig configureren (met de nodige anti-malware software en met software die alle data op het toestel vanop afstand kunnen wissen) en de identificatie bijhouden in een centraal register (Ref. KSZ: 5.3.2.1.e). 〉 Over geactualiseerde systemen beschikken ter bescherming (voorkoming, detectie en herstel) tegen malware (Ref. KSZ: 5.9.3).
	
	

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 beveiliging van ICT-systemen, onderscheiden we volgende preventieve maatregelen:

- *Patching* en *hardening* (zie hoofdstuk: '*Patching en hardening als maatregel*');
- Interne controle op kwetsbaarheden (zie hoofdstuk '*Interne controle op kwetsbaarheden als maatregel'*);
- *Malware*-inspectie (zie hoofdstuk: '*Antimalware als maatregel'*);
- *Intrusion prevention* (IPS) (zie hoofdstuk: 'Host-based *Intrusion Prevention System (IPS)*');
- *High-availability* als maatregel (zie hoofdstuk: '*High-availability als maatregel*'); en
- Scheiding van functies.

2.1.2. Detectie

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 beveiliging van ICT-systemen, onderscheiden we volgende detectiemaatregelen:

- *Logging* (zie hoofdstuk *'Logging' als maatregel'*)
- *Intrusion detection* (IDS) (zie hoofdstuk: *'Host-based Intrusion Detection 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 beveiliging van ICT-systemen, onderscheiden we volgende reactieve maatregelen:

- *Malware*-filter (zie hoofdstuk: '*Antimalware als maatregel*');
- Notificaties naar incidentbeheer (zie document: Vo informatieclassificatie – minimale maatregelen – incident beheer);
- Geautomatiseerde tegenmaatregelen; en
- Corrigerende maatregelen op een sessie.

2.2. *Patching* en *hardening* als maatregel

Patching en hardening zijn preventieve maatregelen.

Eén van de makkelijkste doelen voor een aanvaller is een niet goed actueel gehouden systeem met de laatste *patches* en updates en een systeem waarbij functionaliteiten en privileges niet zijn teruggebracht tot het minimum dat noodzakelijk is voor het uitvoeren van de taak. Dit noemt men *hardening*.

2.2.1. *Patching*

Patching is gericht op het verminderen van risico's als gevolg van benutting van gepubliceerde technische kwetsbaarheden of *bugs* in OS (*operating system* of besturingssysteem) en software.

Patchmanagement is het proces waarmee *patches* op gecontroleerde beheerste (risicobeperkende) wijze uitgerold kunnen worden. *Patches* zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware.

Patches zijn geen upgrades. Upgrades bevatten technische of functionele verbeteringen en zijn meestal grote programma's die een uitgebreid en grondig testschema moeten ondergaan alvorens uitgerold te worden. *Patches* moeten ook getest worden vooraleer in productie gezet te worden, maar dit testschema is beperkter dan bij upgrades.

Het doel van *patchmanagement* is tweeledig, het is gericht op:

- Het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur; en
- Een zo efficiënt mogelijk wijze met zo min mogelijk verstoringen stabiele (veilige) systemen te creëren.

2.2.2. *Hardening*

Hardening is het proces waarbij overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem (*servers*, netwerkcomponenten zoals *firewalls*, *routers* en *switches*, desktops, laptops, mobiele apparatuur, …) verwijderd worden. Daarbij hoort ook het toekennen van zodanige waarden aan beveiligingsinstellingen en -parameters dat hiermee de mogelijkheden om een systeem te compromitteren, worden verlaagd. Het verwijderen van niet gebruikte of onnodige gebruikers of *serviceaccounts*, en het wijzigen van standaard paswoorden die op sommige systemen aanwezig kunnen zijn, behoren ook tot *hardening*.

2.3. Interne controles op kwetsbaarheden als maatregel

Het bestaan van kwetsbaarheden in ICT-systemen is geen onbekende. Af en toe haalt dit fenomeen de kranten wanneer zo'n kwetsbaarheid misbruikt wordt om in te breken in deze ICT-systemen. Dit gebeurt niet alleen in de privésfeer maar ook in organisaties.

Om zich te wapenen tegen dit soort misbruik is het van belang om de kwetsbaarheden te kennen en potentieel misbruik te voorkomen. Organisaties zoals cert.be publiceren informatie over nieuw ontdekte kwetsbaarheden en geven advies. Maar ook leveranciers van software en hardware informeren hierover. Het is dus zaak goed op de hoogte te blijven en bij elke relevante nieuwe kwetsbaarheid de risico's voor de organisatie in te schatten en waar nodig te mitigeren door de aanbevelingen op te volgen.

Om vast te stellen of er nog bekende kwetsbaarheden in de eigen ICT-infrastructuur of applicaties aanwezig zijn, kan periodiek een *vulnerability scan* worden uitgevoerd. Om deze oefening te automatiseren, worden speciale *tools* gebruikt. Zo'n *tool* gaat op zoek naar ontbrekende *patches*, open en kwetsbare netwerkpoorten, standaard paswoorden, enz. Het resultaat is een rapport met kwetsbaarheden en aanbevelingen om deze aan te pakken. Met dit rapport kunnen gericht patches worden geïnstalleerd, *hardening* toegepast of systemen worden vervangen door nieuwere versies.

Een *pen*-test gaat nog een stap verder. Bij een *pen*-test, kort voor *penetration*-test, worden de gevonden kwetsbaarheden gebruikt om na te gaan of er kan worden ingebroken. Het doel van een *pen*-test is inzicht te verkrijgen in de moeilijkheidsgraad om in te breken op het netwerk van de organisatie. Het resultaat van zo'n pen-test is een rapport met bevindingen en aanbevelingen gerangschikt volgens prioriteit.

Zero-day kwetsbaarheden vormen een specifieke groep van kwetsbaarheden. *Zero-day* verwijst naar recent ontdekte kwetsbaarheden, waarvan de leverancier pas na de ontdekking op de hoogte wordt gesteld. Daardoor is er vooreerst geen *patch* beschikbaar, wat de kwetsbaarheid extra gevaarlijk maakt voor misbruik. Dit is het grote verschil met 'gewone' kwetsbaarheden: deze worden gecontroleerd bekend gemaakt op het moment dat de *patch* beschikbaar is, waardoor de kwetsbare omgeving onmiddellijk kan worden beveiligd. Een *responsible disclosure* beleid zorgt ervoor dat er op een ethische manier gezocht wordt naar kwetsbaarheden in een omgeving. Via zo'n programma worden leveranciers op de hoogte gesteld van zulke nieuwe kwetsbaarheden, waardoor alsnog een patch kan worden ontwikkeld vooraleer de kwetsbaarheid kan worden misbruikt. Hoe kan een organisatie zich dan beschermen tegen *zero day* aanvallen? Aangezien *patching* hier niet effectief is, moet er gekeken worden naar bijkomende controlemaatregelen zoals:

- Up-to-date besturingssystemen en toepassingen;
- Anti-malware die kan omgaan met *zero-day exploits*;
- Monitoring: abnormale activiteit detecteren.

2.4. Inbraakpreventie als maatregel

Inbraakpreventie is een preventieve maatregel

2.4.1. *Host-based firewall*

Firewalls bestaan in twee vormen: netwerk-gebaseerd en *host*-gebaseerd, waarbij de netwerk-*firewall* een netwerksegment beveiligt en de *host*-gebaseerde-*firewall* enkel 'zijn' *server* beveiligt. In een scenario waarbij slechts één *server* beveiligd moet worden, zou men kunnen overwegen om enkel een *host*-gebaseerde-*firewall* te installeren. De *server* + *host*-gebaseerde-*firewall* kan aanzien worden als één netwerkzone. Echter, de eigenschappen en kwaliteiten van een *host*-gebaseerde-*firewall* en een netwerk-gebaseerde-*firewall* zijn verschillend. Een *host*-gebaseerde-*firewall* kan enkel als aanvullend beschouwd worden maar een netwerk-gebaseerde-*firewall* is steeds nodig.

2.4.2. *Host-based Intrusion Prevention System* (IPS)

Intrusion Prevention systemen zorgen ervoor dat kwaadaardige datastromen geblokkeerd worden. Voor meer uitleg over IPS: zie document 'Vo informatieclassificatie - minimale maatregelen – netwerken'.

Host-based IPS wordt geïmplementeerd op een ICT-systeem en is in staat om – naast monitoring en analyse van netwerktrafiek van en naar het ICT-systeem (de *host*) – ook interne processen te analyseren en eventueel in te grijpen.

2.5. *Host-based intrusion detection* als maatregel

Intrusion detection is een detectiemaatregel.

Voor meer uitleg over IDS: zie document 'Vo informatieclassificatie – minimale maatregelen – netwerken'.

Detectie op systeemniveau of *host-based* IDS gaat terug tot de tijd van mainframes en bestaat daarmee het langst. Een IDS op systeemniveau baseert zich op lokaal beschikbare informatie. Denk daarbij aan informatie over bestanden op het systeem, de inhoud van logbestanden of netwerkverkeer dat de netwerkkaart op het systeem verwerkt. Op basis van deze informatie bepaalt het IDS of er zich een beveiligingsprobleem op het systeem voordoet of dreigt voor te doen.

2.6. *Host-based* versus network-based

We hebben in vorige hoofdstukken uitgelegd wat *host-based firewall, IDS* en *IPS* betekenen. Van deze oplossingen bestaat ook een netwerk-based variant. Beide technieken zijn complementair en kunnen in verschillende omgevingen en voor verschillende functies ingezet worden. Meer uitleg over netwerk-base *firewall, IDS* en *IPS* is terug te vinden in 'Vo informatieclassificatie – minimale maatregelen – netwerken'. Dit hoofdstuk schetst de verschillen tussen beide technieken.

Host-based technologie kan heel goed overweg met versleutelde trafiek omdat een *host-based* oplossing de trafiek analyseert voor die wordt versleuteld of nadat die is ontcijfert. Een netwerk-based oplossing kan niet zomaar versleutelde trafiek verwerken: deze oplossing 'ziet' alleen de versleutelde trafiek en heeft geen mogelijkheid om vast te stellen of er binnen de versleutelde trafiek

malafide communicatie plaats vindt. Voor TLS is wel een oplossing door middel van SSL-inspectie, maar hiervoor heeft de netwerk-based oplossing de private sleutel nodig waarmee de TLS is opgezet. Vaak argumenteert men hiertegen uit het oogpunt van beveiliging en bescherming van persoonsgegevens.

Een ander belangrijk aspect is het kostenplaatje: door netwerk-based technologie in te zetten, is het mogelijk om met één oplossing alle systemen in het netwerk of de netwerkzone in één keer te beveiligen. Om hetzelfde resultaat te bekomen met een *host-based* oplossing, moet elk ICT-systeem voorzien worden van een eigen implementatie van zo'n oplossing.

Daarnaast is een *host-based* oplossing afhankelijk van het ICT-systeem waarop het draait. Wanneer de integriteit van dit ICT-systeem wordt aangetast (bijvoorbeeld door malware of tijdens een cyberaanval), kan dit een negatief effect hebben op de goede werking van de *host-based* oplossing. Een netwerk-based oplossing heeft dit probleem niet.

Samengevat kan gesteld worden dat beide technologieën – *host-based* en netwerk-based – elk hun eigen voor- en nadelen hebben.

2.7. *Antimalware* als maatregel

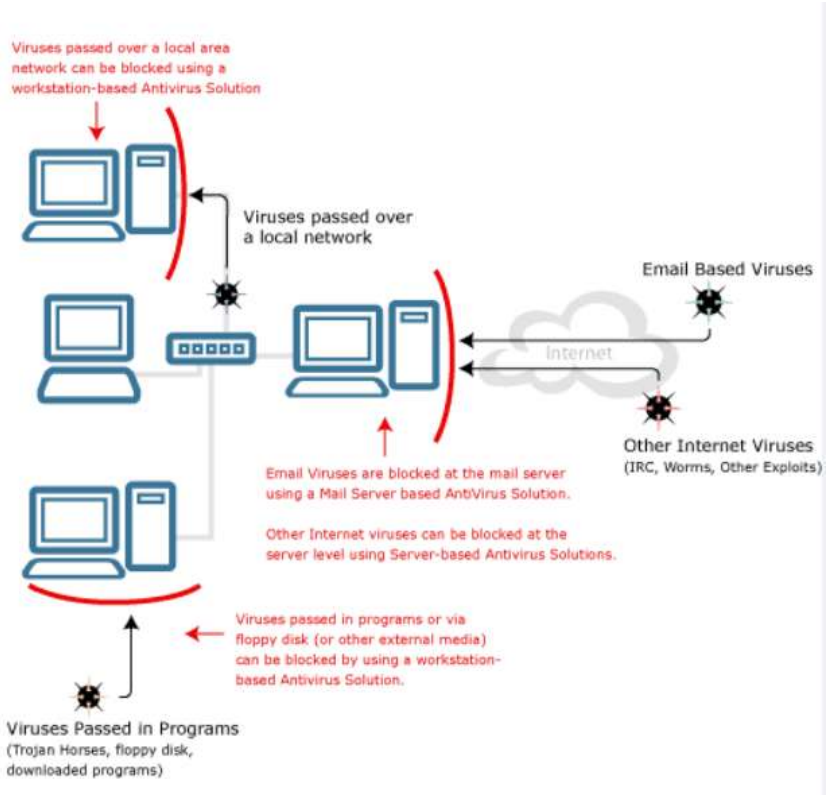
Antimalware is een preventieve en een reactieve maatregel.

De letterlijke betekenis van *malware* is 'kwaadaardige programma's'. *Antimalware* is een verzamelwoord voor programma's die een computer kan beschermen tegen *malware*.

Een oudere term voor *antimalware* is antivirus. Een virus is een bepaald type *malware*, namelijk een kwaadaardig programma dat zich op een bepaalde manier gedraagt en zich verspreidt. Het gedrag van een virus verschilt van een *rootkit*, *adware*, Trojaanse paarden, wormen, *drive-by downloads*, *browser hijacker*, *spyware* en andere *malware*-soorten. Het landschap van *malware* is zo complex geworden en de aanvalshoeken zo divers dat de term antivirus niet meer accuraat is. De term *antimalware* dekt de lading beter aangezien een huidig antiviruspakket (of *antimalware*-pakket) een computer moet beschermen tegen alle soorten *malware.*

Malware komt via allerlei kanalen het netwerk binnen. Aangezien meer en meer toestellen (bv. smartphones, laptops, tablets, mobiele media, …) aanloggen op het netwerk, vergroot het risico op infectie. *Malware* kan vanuit verschillende invalshoeken opereren, bv.:

- Een bijlage bij een mail bericht kan geïnfecteerd zijn;
- Een download van een website kan *malware* bevatten
- Een USB of ander mobiel medium kan schadelijke code bevatten; of
- Een programma kan *malware* bevatten.



Het is dan ook belangrijk om *antimalware*-producten te installeren op de belangrijkste toegangspoorten tot het netwerk:

- Mail *gateway*;
- *Proxyserver*;
- *Webserver*;
- *Application server*; en
- Gebruikersapparatuur (PC, laptop, smartphone, tablet, …).

Een *antimalware*-software bevat niet alleen een complete *malwarescanner* die alle type *malware* kan detecteren en verwijderen, maar ook andere preventieve waarschuwingstechnologie om bv. phishing-aanvallen en besmette websites te vermijden. Als een extra aandachtspunt geldt dat een *antimalware*-software best ook *ransomware* moet kunnen verwijderen.

De grootste oorzaak van *malware*-besmetting is kwetsbaarheden in de software en hardware. Deze kwetsbaarheden kunnen via een *exploit* misbruikt worden, waardoor kwaadwillende personen de computer kunnen infecteren.

De gebruiker kan ook zelf de oorzaak zijn van een *malware*-infectie, bijvoorbeeld door malafide websites te bezoeken of door gratis software te installeren. Vaak is deze software extra voorzien van – door de gebruiker onvermoede – aanwezigheid van *malware*-code.

Antimalware-pakketten zijn gebaseerd op volgende principes:

- *Signature*-gebaseerde-detectie: werkt met een *signature database*, waarin de gekende *exploits* zijn opgenomen.
- Heuristische analyse: scant *malware* door te kijken naar het gedrag van de gescande code om zo nieuwe en onbekende *malware* waarvoor nog geen *signature* bestaat, op te sporen. Wanneer het gedrag overeenkomt met gedrag van *malware*, neemt de scanner aan dat het om *malware* gaat.

- *Sandboxing*: werkt door middel van het uitvoeren van de verdachte code in een afgeschermde omgeving (de *sandbox*). Door de code uit te voeren in een *sandbox* worden de andere processen niet verstoord.

Zeker wanneer gewerkt wordt met *signature*-gebaseerde-detectie is het van groot belang dat steeds de laatste versie van de *malware database* voorhanden is. Periodiek opladen van de laatste versie is hoe dan ook de boodschap.

Antimalware-pakketten voorzien in twee kernacties:

- Detectie van *malware*; en
- Reactie: het melden aan een beheerder en/of gebruiker, het verwijderen of in quarantaine plaatsen van het geïnfecteerd bestand.

Het dient opgemerkt te worden dat versleutelde data niet kan worden gescand op *malware*. Om dit te kunnen doen, moet de data eerst ontcijferd worden. Dit is een bijkomende reden om niet alleen *malware scanners* op de *gateways* en *servers* te plaatsen, maar ook op gebruikersapparatuur. Bij de plaatsing van *antimalware*-componenten moet dus rekening gehouden worden met al dan niet versleutelde trafiek.

2.8. *Logging* als maatregel

Logging is een reactieve maatregel.

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

Soms worden ICT-systemen zo onmisbaar dat ze als kritisch beschouwd kunnen worden op niveau beschikbaarheid. Er zijn dan verschillende technieken die men kan inzetten om de beschikbaarheid/betrouwbaarheid van een ICT-systeem te verhogen:

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 ICT-systemen te optimaliseren:

- *backup- en herstelprocedures:* deze vormen de basis voor de meeste omgevingen waarin hoge beschikbaarheid belangrijk is.
- *Patching* en *hardening*: om kwetsbaarheden in de componenten te mitigeren, met name kwetsbaarheden die uitgebuit kunnen worden door (D)DoS-aanvallen;
- *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.