Hardening beleid

Informatieveiligheid & Privacy

SWO

Auteurs : Wilbert Hepping, Jan Lemstra

Versie : 1.0
Status : Definitief
Datum : 11 juli 2022

INHOUDSOPGAVE

Documenthistorie

Versie	Datum	Auteur(s)	Status / omschrijving wijziging
0.1	10-06-2021	Wilbert Hepping	Concept hardening beleid
0.2	17-09-2021	Wilbert Hepping, Jan Lemstra	Aanpassingen na bespreking
0.3	15-02-2022	Wilbert Hepping	Aangepast na review automatisering
0.4	07-06-2022	Wilbert Hepping	Toevoegen blokkades, ict-koppelingen en netwerksegmentatie
1.0	11 juli 2022	Wilbert Hepping	Definitieve versie

Distributielijst

Naam	Organisatiedeel / Functie|Rol
Jan-Pieter Wind	FG
Daisy Djodikromo-de Jong	PO
Jan Lemstra	CISO
Johan Dijkink	Eenheidsmanager Advies en Services
Medewerkers SWO	Via Intranet

Review

Naam	Functie	Datum	Hoofdstukken/ onderwerpen
Ruben Bruinenberg	Systeembeheerder security	11-11-2021	Geheel document
Marlies Caneel	IT Processpecialist	11-11-2021	Geheel document

Accordering

Naam	Functie	Datum	Handtekening

1. Inleiding

Eén van de gemakkelijkste doelen voor een aanvaller is een systeem zonder de laatste patches en updates en een systeem met meer functionaliteiten en privileges (rechten of autorisaties) dan nodig is voor het uitvoeren van de taak (hardening). Door te hardenen wordt het mogelijke aanvalsoppervlak voor een aanvaller verkleind. De BIO geeft enkele maatregelen die op hardening ingaan, maar die ook nadere detaillering vragen bovenop wat in de BIO staat alsook in het beveiligingsbeleid van de gemeenten[1] en de SWO[2].

Doelstelling hardening beleid
Het hardening beleid van de Samenwerkingsorganisatie de Wolden Hoogeveen (hierna: SWO) geeft richting aan de wijze waarop de organisatie maatregelen wenst te treffen voor hardening. Hardening is het proces waarbij overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem verwijderd worden. En daarnaast door zodanige waarden toekennen aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat.

De effecten van hardening:

- Kans verkleinen op het benutten van zwakheden in systemen door een aanvaller.
- Het tegenwerken van een aanvaller die binnengedrongen is door de mogelijke programma's en tooling op systemen te minimaliseren.
- Het tegenwerken van een aanvaller die binnengedrongen is door het minimaliseren van ter beschikking staande systeemrechten.
- Verlagen van de mogelijkheden om verder door te dringen op het netwerk bij een gelukte aanval.
- Daarnaast kan een effect van hardening zijn het verminderen van systeem complexiteit en daarmee een verbeterde beheersing van het systeem en lagere beheerkosten.

De SWO onderschrijft het belang van een adequaat hardening-beleid omdat het niet uitvoeren van hardening ernstige schade kan toebrengen aan systemen en de informatievoorziening in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Bovendien kan het niet uitvoeren van hardening schade toebrengen aan het belang van de burger en het vertrouwen in de gemeenten en SWO.

Hardening dient gestructureerd te worden aangepakt en er moeten procedures worden vastgesteld om hardening doeltreffend en ordelijk te laten plaatsvinden. Dit beleid is van toepassing op alle systemen die in gebruik zijn is bij de organisatie.

De beleidsuitgangspunten die de SWO hanteert zijn ontleend aan de Baseline Informatiebeveiliging Overheid v1.04 (BIO) en de wereldwijd gehanteerde CIS Security baselines (Center of Internet Security).

[1] Zie Strategisch Beleid Informatieveiligheid & Privacy - De Wolden en Hoogeveen
[2] Zie Tactisch Beleid Informatieveiligheid & Privacy SWO

Vanuit de BIO gaat dit over onderstaande controls en de daaraan gekoppelde de maatregelen.

H9. Toegangsbeveiliging
9.1.2: Beleid voor toegangsbeveiliging
9.4.1: Beperking toegang tot informatie
9.4.2: Beveiligde inlogprocedures

H12. Beveiliging bedrijfsvoering
12.2.1: Beheersmaatregelen tegen malware
12.5.1: Software installeren op operationele systemen
12.6.1: Beheer van technische kwetsbaarheden
12.6.2: Beperkingen voor het installeren van software
12.7.1: Beheersmaatregelen betreffende audits van informatiesystemen

H13. Communicatiebeveiliging
13.1.1: Beheersmaatregelen voor netwerken
13.1.2: Beveiliging van netwerkdiensten
13.1.3: Scheiding in netwerken

H14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
14.1.2: Toepassingen op openbare netwerken beveiligen
14.1.3: Transacties van toepassingen beschermen
14.2.3: Technische beoordeling van toepassingen na wijzigingen besturingsplatform
14.2.6: Beveiligde ontwikkelomgeving

Mochten de uitgangspunten tegenstrijdig zijn tussen de verschillende richtlijnen dan prevaleren de BIO controls en maatregelen.

2. Beleidsuitgangspunten hardening

2.1 Algemeen

1. Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
2. Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten door beheerders.
3. Gebruik alleen beheerinterfaces waarvan de netwerkcommunicatie beveiligd is.
4. Op alle systemen[3] waar dit mogelijk is, worden beschikbare firewalls, antivirusscanners en andere beschermende maatregelen geactiveerd.
5. Op alle systemen wordt (waar mogelijk) systeem logging geactiveerd om detectie mogelijk te maken van malware en ongebruikelijke systeem activiteiten.
6. Systemen worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken zo veel mogelijk beperkt is.
7. De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument[4] waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.
8. Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
9. Voor toegang tot systemen door middel van wachtwoorden dient men zich te houden aan het (separate) wachtwoord beleidsdocument[5].
10. De infrastructuur is middels het defense-in-depth principe[6] op diverse lagen beveiligd.
11. Binnen het netwerk van de SWO wordt geen externe apparatuur van een leverancier geplaatst welke niet in beheer is bij de SWO (zoals pc's, servers of camera's). Indien dit toch noodzakelijk is dan worden er in de overeenkomst concrete afspraken gemaakt over het beheer van deze apparatuur en zal er actieve monitoring plaatsvinden over de status van de apparatuur.

2.2 Minimaliseren van geïnstalleerde software

Overbodige software, services en gebruikersaccounts worden uitgeschakeld en/of van het systeem verwijderd. Hieronder een opsomming van operationele maatregelen die dit ondersteunen:

1. Om te voorkomen dat schadelijke software kan worden uitgevoerd door middel van een browser dient de mogelijkheid van een gebruiker om mobiele code uit te voeren te worden beperkt.
2. Daarnaast dienen de instellingen die dit mogelijk maken te worden geblokkeerd door middel van een systeem policy.
3. Gebruikersrechten worden beperkt tot het minimaal noodzakelijke.

[3] Zie H4. Definities voor uitwerking van term systemen
[4] De indeling is uitgewerkt in deze beleidsuitgangpunten en H3. van dit document
[5] Zie Wachtwoordbeleid SWO
[6] Zie H3. Verdediging in lagen "Defense in Depth"

4. Alleen geautoriseerde software[7] wordt toegestaan binnen het netwerk van de SWO.
5. Installeer alleen de noodzakelijke functies van een besturingssysteem, database of middleware op productiesystemen.
6. Verwijder na installatie eventuele installatiebestanden en/of broncode van productiesystemen.
7. Zorg ervoor dat gebruikte software afkomstig is uit een betrouwbare bron.
8. Alleen geautoriseerd personeel kan functies en software installeren of activeren.

2.3 Toepassen van security best practices conform CIS

1. Indien voor systemen een CIS benchmark beschikbaar is moeten systemen gehard worden conform deze richtlijn.
2. De CIS benchmark wordt vertaald naar de SWO baseline en ingericht in de tooling;
3. Afwijken van CIS benchmark, waarbij de beveiliging minder is dan deze benchmark, is toegestaan indien voldoende gemotiveerd ter beoordeling van de proceseigenaar in overleg met de CISO/ISO conform proces hardening.
4. Een afwijking wordt altijd schriftelijk vastgelegd en de afwijking wordt verwerkt in de SWO baseline;
5. Een systeem is altijd 100% compliant met de SWO baseline;

2.4 Controle op implementatie van beveiligingsinstellingen

1. Alle apparatuur moet regelmatig[8] worden getest op bekende zwakheden zoals beschreven in het beleid voor patchmanagement[9].
2. De security instellingen worden gecontroleerd ten opzichte van de SWO baseline via de reguliere, periodieke controles[10].
3. De oplossing en plan van aanpak van afwijkingen van de vastgestelde baseline moeten binnen tien werkdagen na constatering helder zijn. De oplostermijn is opgenomen in het plan van aanpak of in overleg met de proceseigenaar wordt een aanpassing in de SWO baseline gedaan en gemotiveerd.

2.5 Toepassen van blokkades

Het gebruik van blokkades of filtering op geografische regio's en IP-adressen is een effectieve manier om het hackers moeilijker te maken om een organisatie aan te vallen. Vanuit de monitoring/tooling blijkt dat er vaak inkomende verbindingen worden gedetecteerd welke potentieel gevaarlijk kunnen zijn. Dit gaat om verbindingen vanuit bijvoorbeeld landen als Indonesië, Iran, Nigeria, Syrië en Oekraïne. Uit ervaring blijkt dat het toepassen van deze blokkering geen tot zeer weinig impact op de organisatie.
Door een blokkade van de filesharing services wordt ervoor gezorgd dat het hackers moeilijker gemaakt wordt om bestanden vanuit ons netwerk buit te maken. Daarnaast voorkomen wij ook de kans op datalekken doordat medewerkers bestanden uploaden naar deze services. Ook kunnen medewerkers geen (onveilige) bestanden meer

[7] Zie Incident- en Wijzigingsbeheer SWO
[8] Zie Procesbeschrijving hardening SWO v1.0def
[9] Zie Patchmanagement beleid SWO v1.0def
[10] Zie Procesbeschrijving hardening SWO v1.0def

downloaden. Er is een veilige mail applicatie beschikbaar om grote bestanden op een veilige manier te versturen of te ontvangen.

De volgende blokkades worden toegepast:

1. Een regionale blokkering[11] op inkomende verbindingen op de mailserver op basis van de resultaten van de monitoring software;
2. Een regionale blokkering[12] voor de (externe) toegang tot Citrix;
3. Het blokkeren van het delen van bestanden via filesharing-services (zoals Dropbox, WeTransfer, 4Shared, Zippyshare, Google Drive, iCloud Drive en Filehippo);
4. De vrije internettoegang op onze servers te blokkeren[13];

[11] Bijlage: lijst met geblokkeerde landen mail
[12] Bijlage: lijst met toegestane landen Citrix
[13] Werkgerelateerde websites worden op verzoek vrijgeven op Citrix

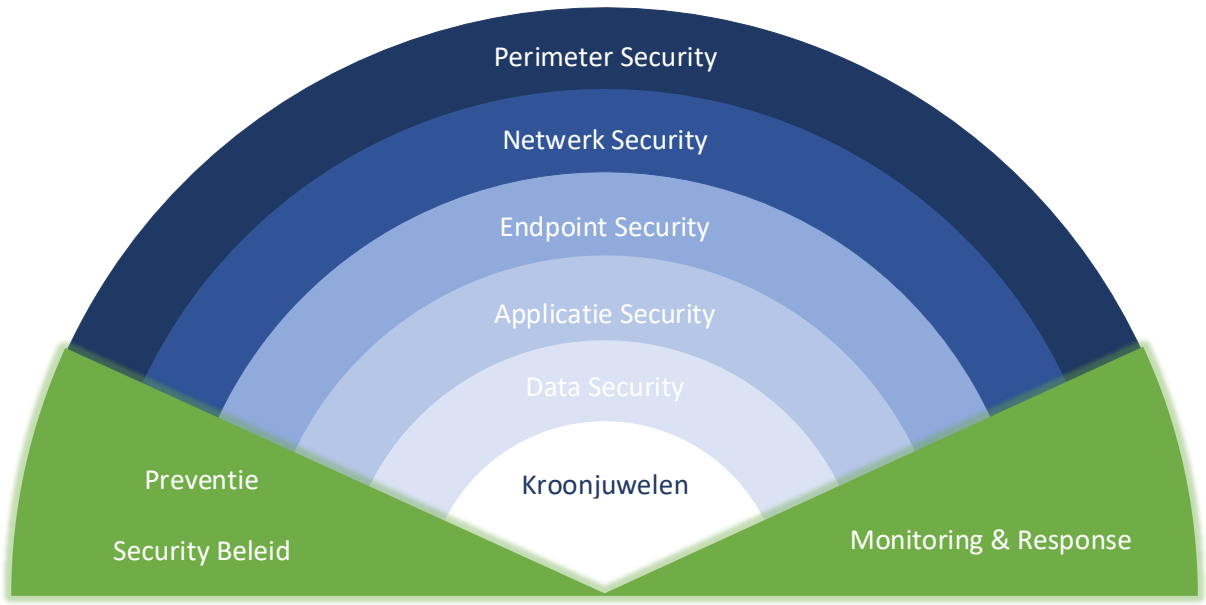
3. Uitwerking hardening principes

3.1 Verdediging in lagen "Defense in Depth"

Hardening van de actieve infrastructuur, servers en netwerkcomponenten, is een belangrijke stap in de strijd om de betrouwbaarheid van de informatievoorziening te waarborgen. Het beveiligen van een infrastructuur omvat verschillende stappen die samen verschillende beschermingslagen vormen. Deze benadering wordt vaak genoemd: 'verdediging in lagen' (zie figuur 1).

De lagen die in een infrastructuur onderscheiden kunnen worden:

- **Perimeter Security**: De buitenste schil van een organisatie. Hieronder vallen bijvoorbeeld de firewall, DMZ en IPS/IDS. In de DMZ van de organisatie dienen services te worden aangeboden die ook gebruikt worden om gegevens aan te bieden op het internet, zoals bijvoorbeeld een webserver. Een firewall zorgt ervoor dat internetgebruikers bij zo'n firewall alleen toegang hebben tot de webservers en dat beheerders intern de server kunnen beheren.
- **Netwerk Security**: Security maatregelen op het netwerk, zoals filteren van webverkeer, Network Access Control (NAC). Het internet is een bron van kwaadaardige software, websites en e-mails en daarmee een van de grootste dreigingen op het gebied van security voor een organisatie. Daarom dient dit inkomende internet- en e-mailverkeer te worden gecontroleerd op malware voordat dit afgeleverd wordt bij de eindgebruikers.
- **Endpoint Security**: Bescherming van het apparaat van de eindgebruiker. Het regelmatig toepassen van beveiligingspatches van leveranciers beveiligingspatches is de eerste stap om endpoints te hardenen. Daarnaast is het installeren en regelmatig gebruiken van software voor antivirus- en antispyware samen met het plannen van dagelijkse automatische definitie-updates en automatische scans op systemen essentiël. Ook adviseren veel beveiligingsexperts het installeren van een softwarematige firewall op de computer. Op deze firewall dienen management services (bijv. RDP en SSH) alleen toegankelijk gemaakt te worden voor de beheerders door gebruik te maken van een apart beheernetwerk.
- **Applicatie Security**: De beveiliging van applicaties zelf door bijvoorbeeld goed loggingbeleid met controle op afwijkingen en het monitoren van de database. Voor applicaties die direct op het internet worden aangeboden kan er gebruik gemaakt worden van Web Application Firewall (WAF). Een WAF kan detecteren of de applicatie regulier gebruikt wordt of dat een kwaadwillig persoon misbruik probeert te maken van de webapplicatie.
- **Data Security**: Bescherming van de data door bijvoorbeeld gebruik van dataclassificatie, Identity Access Management (IAM) en encryptie. Openbare data en geheime informatie dienen op verschillende manieren behandeld te worden. Het gebruik van IAM is geen verplichting uit de BIO, maar is wel een methode om de volwassenheid van security binnen een organisatie te verhogen.



Figuur 1: Defence in Depth (gebaseerd op The Fan™[14])

Maatregelen om de verschillende lagen te beschermen:

- **Monitoring & Response**: De acties en processen op operationeel niveau zoals SIEM, SOC en CIRT om de gehele infrastructuur te monitoren en bij afwijkingen hierop te acteren.
- **Preventie en Security Beleid**: Door gebruik te maken van risico management, IB bewustwording en toepassen van de security architectuur wordt er op tactisch en strategisch niveau gewerkt aan security bij de organisatie.

Goede beveiliging is het vinden van de juiste balans tussen het hardenen van de systemen tegen mogelijke bedreigingen versus er voor te zorgen dat er toch goed mee kan worden gewerkt in relatie tot de toegewezen taak. Als een bepaalde applicatie of service niet nodig is moet deze worden uitgeschakeld en verwijderd. Extra software die aanwezig is vereist meer werk van de systeembeheerders en vergroot de kans dat een aanval succesvol kan worden uitgevoerd. Onnodige software toevoegen kan ervoor zorgen dat een computer een lanceer platform wordt voor de verspreiding van een virus en tevens voor een hacker een toegangspoort wordt om andere systemen binnen het netwerk te kunnen aanvallen.

3.2 Zero Trust

Steeds meer organisaties kiezen ervoor om gebruik te maken van Zero Trust-principes bij het beveiligen van hun IT-infrastructuur. Zij zoeken een beveiligingsmodel dat zich effectief weet aan te passen aan de complexe moderne omgeving. In deze omgeving moeten apparaten en gegevens worden beschermd ongeacht de locatie waar zij zich bevinden of het type apparaat dat binnen organisaties wordt gebruikt. Zero Trust biedt organisaties de mogelijkheid hun risico's te beperken in deze nieuwe situatie. Met behulp van de maatregelen die getroffen worden bij Zero Trust kunt u tekortkomingen in het traditionele beveiligingsmodel verhelpen. Hierdoor wordt bijvoorbeeld horizontale verplaatsing – het tussen systemen verplaatsen op zoek naar data om te exfiltreren – binnen het netwerk bemoeilijkt.

[14] Northrop Grumman's Cybersecurity Reference Framework titled The Fan™

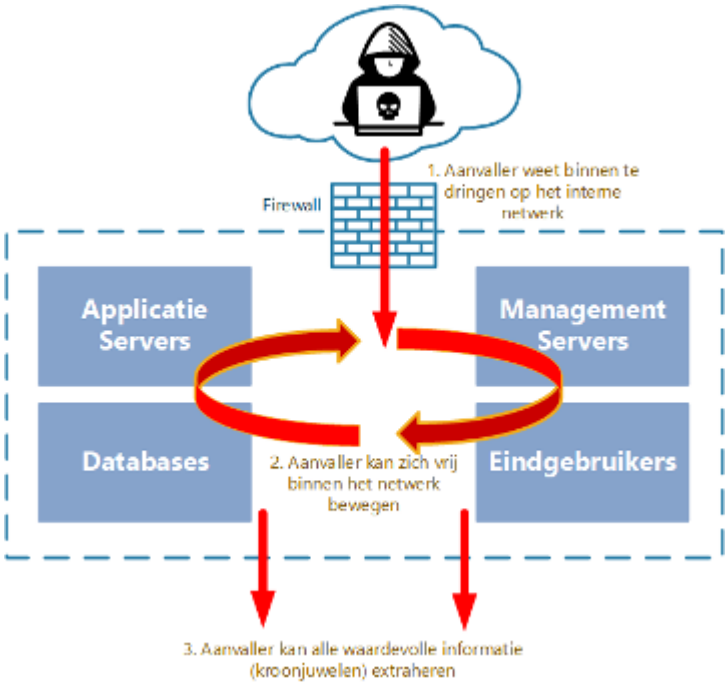
Zero Trust is een beveiligingsmodel met een set ontwerpprincipes dat aanvallen en datalekken helpt te voorkomen. Hierbij wordt het concept van een vertrouwde netwerkpositie uit de architectuur verwijderd. Het is gebaseerd op de erkenning dat traditionele beveiligingsmodellen werken op de verouderde veronderstelling dat alles aan de binnenkant van het netwerk van een organisatie kan worden vertrouwd. Geworteld in het principe van *never trust, always verify*, is Zero Trust ontworpen om moderne digitale omgevingen te beschermen. Het maakt gebruik van fijnmazige netwerksegmentatie en biedt dreigingspreventie op de randen van segmenten. Daarnaast vereenvoudigt Zero Trust gedetailleerde conditionele gebruikerstoegangscontrole.

Een architectuur is Zero Trust als hij voldoet aan de volgende set van ontwerpprincipes:

- Identificeer de te beschermen onderdelen van de IT-infrastructuur en beveilig alle paden er naartoe.
- Verschaf alleen toegang tot informatie via beveiligde verbindingen, ongeacht de locatie.
- Handhaaf strikte toegangscontrole op een need-to-know-basis.
- Bepaal de toegangsrechten op basis van mate van vertrouwen die afgeleid wordt uit verschillende eigenschappen van de toegangsaanvraag: account, apparaat, IP-adres en locatie.
- Zorg voor uitgebreide monitoring en logging.

3.3 Netwerksegmentatie

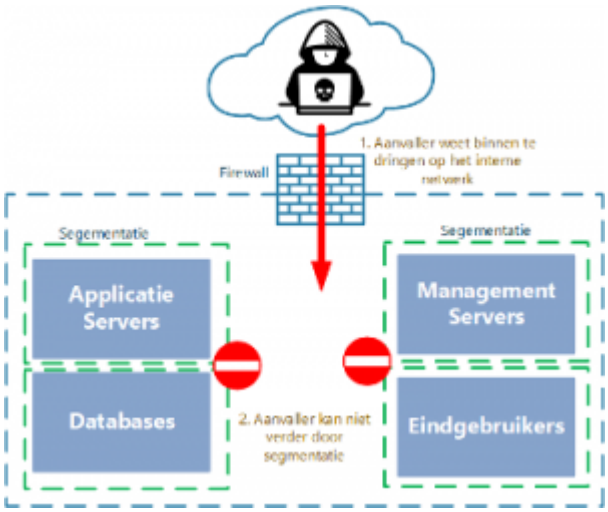
In een klassieke netwerkarchitectuur wordt een enkele firewall gebruikt en een scheiding gemaakt tussen extern (onvertrouwd) en intern (vertrouwd) middels een soort kasteelmuur om interne componenten. Het grootste gevaar van deze oplossing is dat zodra een aanvaller (hacker) weet binnen te dringen op het interne netwerk men vrij spel heeft. Na een succesvolle inbraak kan de aanvaller zich vrij binnen het interne gemeentenetwerk verplaatsen. Een veel voorkomende methode van bijvoorbeeld Ransomware criminelen is naast het versleutelen van de gegevens, ook de waardevolle gegevens, informatie en kroonjuwelen extraheren. Binnen deze architectuur is dat buitengewoon eenvoudig.



Figuur 2: Schematische netwerktekening zonder segmentering

Netwerksegmentatie is het opknippen van het totale netwerk in kleinere segmenten, met tussen de segmenten een beveiligd koppelvlak. Dit zorgt ervoor dat kwaadwillenden die zich in een netwerksegment bevindt niet direct ongehinderd toegang heeft tot andere netwerksegmenten.

Het verkeer tussen deze netwerksegmenten kan gecontroleerd en/of geblokkeerd worden door goede regels in de beveiligde koppelvlakken (meestal firewalls) in te stellen en dit te controleren. Hierdoor wordt een eventueel incident beperkt tot een afgeschermd deel van het netwerk en kan men zich dus niet direct vrij bewegen door het hele netwerk.



Figuur 3: Schematische netwerktekening met segmentering

De beleidsuitgangspunten 2.1.6, 2.1.7 en 2.1.8 in dit beleid geven richting aan de wijze waarop de SWO het segmenteren van het netwerk wil uitvoeren. De organisatie onderschrijft het belang van netwerksegmentatie omdat hierdoor de waardevolle gegevens, informatie en kroonjuwelen.

4. ICT-koppelingen

Er komen steeds vaker verzoeken om een koppeling te realiseren tussen een applicatie op internet (SAAS) naar een applicatie die op de on-premise omgeving (lokale netwerk) van de SWO draait. Er zijn al een aantal van dergelijke koppelingen gerealiseerd, maar nog niet op basis van een vastgestelde standaard. Daardoor zijn de huidige koppelingen op verschillende wijze gebouwd. En is de wijze van koppelen nog niet getoetst aan de steeds strengere eisen vanuit informatieveiligheid.

Daarnaast zullen ook steeds vaker koppelingen gerealiseerd moeten worden tussen SaaS-applicaties onderling.

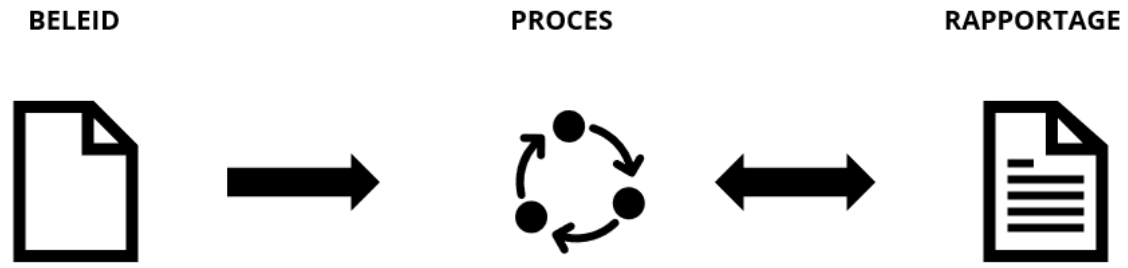
Hieronder zijn de uitgangspunten opgenomen waaraan van systemen, applicaties en koppelingen moeten voldoen.

1. Er wordt voor ieder systeem (server) een eigen segment gecreëerd;
2. Systemen die van buiten de on-premise omgeving (lokale netwerk) benaderd moeten worden, worden in het DMZ geplaatst;
3. Koppelingen tussen de segmenten worden beperkt door middel van een toegangsregel (access rule) gebaseerd op het 'Principle of Least Privilege[15]';
4. Toegang van buiten het lokale netwerk naar de koppeling wordt beperkt middels een toegangsregel (access rule) gebaseerd op het 'Principle of Least Privilege';
5. De toegangsregel bestaat minimaal uit de volgende parameters:
    a. Bron IP-adres (Source IP address);
    b. Bron poort (Source port);
    c. Bestemming IP-adres (Destination IP address);
    d. Bestemming poort (Destination port);
6. Op de gegevens en dataverkeer via de koppeling wordt altijd encryptie (versleuteling) toegepast (zowel intern als extern), bijvoorbeeld door certificaten (geen self-signed);
7. Voor iedere koppeling wordt een specifieke gebruiker (user) aangemaakt met beperkte autorisaties;
8. Voor implementatie van de koppeling wordt deze samen met de leverancier en FAB-er geheel gedocumenteerd;

[15] Zie: https://en.wikipedia.org/wiki/Principle_of_least_privilege

5. Inzet tooling

De SWO zet software in om de fundamentele beveiligingsrisico's van de ICT-infrastructuur periodiek te controleren. Deze software controleert geautomatiseerd en periodiek alle aangesloten servers, databases, laptops, desktops en netwerkcomponenten in het bedrijfsnetwerk. Het rapporteert de afwijkende configuraties, achterlopende security patches van alle software en de aanwezigheid van antivirussoftware. Daarnaast rapporteert de software over rechten, inrichting en gedrag binnen de Active Directory. Compliancy en afwijkingen worden gemeld via een overzichtelijk dashboard en via rapportages.



Figuur 4: Hardening, van beleid tot rapportage

Hierdoor kan de SWO werkzaamheden tijdig plannen, beter bijsturen en verbeteringen duidelijk zichtbaar maken en compliancy blijvend aantonen. De software controleert of de basis technische securitymaatregelen in overeenstemming zijn met het intern beleid en met geldende wet- en regelgeving.

6. Gehanteerde definities

Systemen
Met systemen wordt in dit verband bedoeld: Servers, actieve netwerkcomponenten zoals firewalls en switches, desktops, laptops, smartphones en tablets. Kortom, alles met een besturingssysteem.

CIS benchmark
Het Center of Internet Security heeft per besturingssysteem benchmarks ontwikkeld die informatie verschaffen op basis waarvan organisaties weloverwogen beslissingen kunnen nemen aangaande bepaalde beveiligingsmogelijkheden. De CIS benchmarks zijn de basis waarop de SWO haar eigen specifieke security baseline (hardening) heeft gebaseerd.

SWO Baseline
De organisatie specifieke baseline, gebaseerd op de CIS benchmark, waarin relevante wijzigingen zijn doorgevoerd of niet relevante instellingen zijn uitgezet/verwijderd. De organisatie baseline is de richtlijn waartegen de toetsing van de actuele beveiligingsinstellingen van een systeem worden getoetst.

Hardening
Het doel van hardening is om zo veel mogelijk veiligheidsrisico's te elimineren. Dit wordt over het algemeen gedaan door overbodige functies en/of software van het besturingssysteem uit te zetten, in te regelen of van het systeem te verwijderen.

Compliancy
Mate van compliancy (%), ten opzichte van de organisatiebaseline, waaraan een set van ICT Level componenten dienen te voldoen.