Patronen Informatiebeveiliging

Colofon

Datum bijgewerkt : vrijdag 11 januari 2013
Status : Definitief
Vindplaats : http://www.PvIB.nl
Contactadres : j.e.veen@minfin.nl

Voorwoord

Voor u ligt een operationeel referentiekader voor informatiebeveiligers.

Het bevat concrete oplossingsgebieden voor de meest voorkomende problemen bij het beveiligen van IT-infrastructuur. Het zijn *handreikingen*, beschreven als *patronen* op basis van de Open Group standaard.

Het doel van patronen is *kennisdeling* en het geven van inzicht en overzicht in een vakgebied, dat met de toenemende bedreigingen steeds complexer lijkt te worden. Het document is tot stand gekomen in een expert-community van het Platform voor Informatiebeveiliging (PvIB), die bestond uit senior architecten en adviseurs vanuit het bedrijfsleven en de overheid.

Als methodiek is uit het NORA dossier Informatiebeveiliging de *Architectuuraanpak* toegepast.
Als normenkader zijn de *Normen IT-voorzieningen* toegepast. Beide stukken zijn op de e-overheidssite gepubliceerd als Best Practices voor NORA 3.0:
http://e-overheid.nl/onderwerpen/architectuur-en-nora/982-dossier-informatiebeveiliging

In de Architectuuraanpak vindt u een uitwerking van de modellering die in deze IB-patronen is toegepast, maar de aanpak fungeert tevens als handreiking voor het opstellen van IB-architectuur.

In bijlage 1 is een relatie gelegd van de patronen met de normen van de Code voor Informatiebeveiliging (ISO 27002) en de daarvan afgeleide Normen IT-voorzieningen.

Dit document bestaat uit 2 delen:

1. **Beschouwingsmodellen**. Beschrijft de basistopologie van een bedrijfsnetwerk (zonering) en hoe IB-patronen in samenhang werkzaam zijn in bouwblokken van generieke infrastructuur.
2. **Thema's en Patronen.** Beschrijven generieke oplossingen voor specifieke problemen.

Als uitgangspunt voor het opstellen van de patronen is een template gehanteerd, dat als eerste hoofdstuk in dit document te vinden is.

Gebruikerservaringen en suggesties voor verbetering van deze versie zijn welkom!

Namens de community,

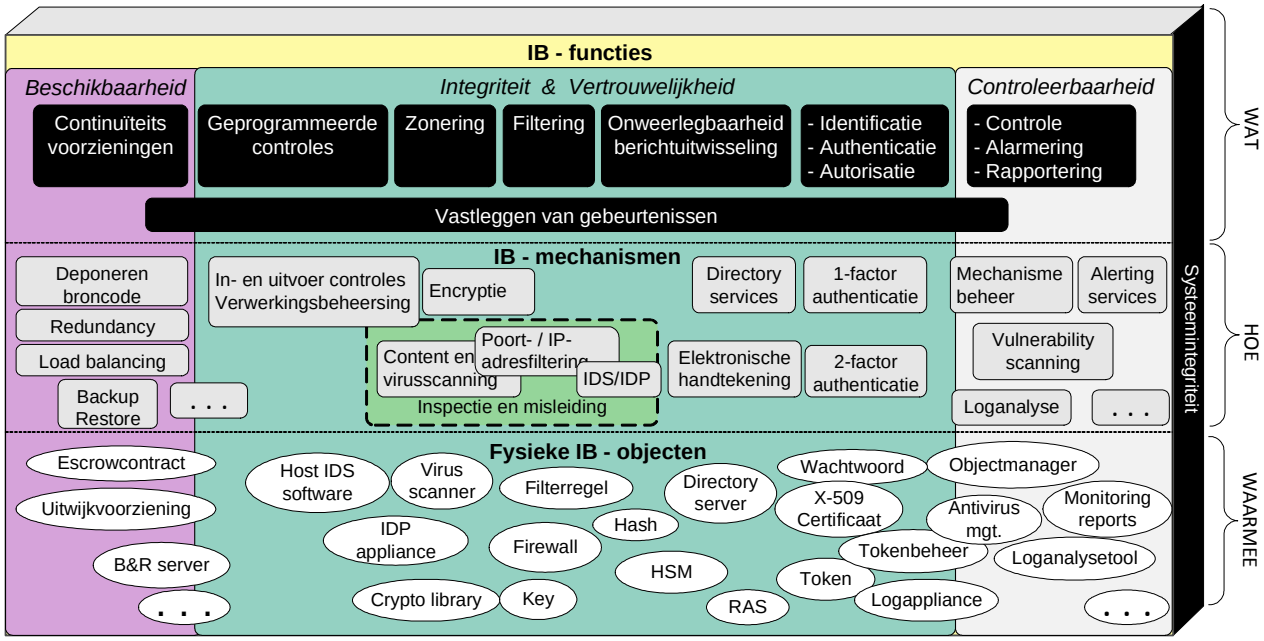
Jaap van der Veen.

Deelnemers Community:

Jaap Arbouw
Ralf Boersma
Bart Bokhorst
Rinus Braak
Renato Kuiper
Onno Massar
Jan Mendrik
Kees Louwerse
Jan van Prooijen
Hanno Steenbergen
Kees Terlouw
Jaap van der Veen

Toelichting

Deze patronen geven de samenhang weer hoe IB-functies werkzaam zijn in IT-*infrastructuur*.
Het onderstaande IB-functiemodel wordt toegelicht in het NORA-document: “Architectuur Aanpak Informatiebeveiliging”



IB-Functiemodel voor IT-voorzieningen

IB-patronen en beschouwingsmodellen zijn te groeperen naar onderlinge samenhang en aard in onderstaande tabel, die tevens als index kan worden gebruikt.

Deel 1. Beschouwingsmodellen

1. Beschouwingsmodel zonering: *Beschrijft de basistopologie van een bedrijfsnetwerk.*
2. Client
3. Server
4. Server Virtualisatie
5. Netwerk
6. Draadloze netwerken
7. Printer

Beschrijft hoe de IB-patronen in samenhang werkzaam zijn in de delen waaruit generieke infrastructuur is opgebouwd

Deel 2. Thema’s en patronen

Koppelvlakken

8. Themapatroon Koppelvlakken
9. Externe koppelvlakken
10. Interne koppelvlakken voor de productieomgeving
11. Interne koppelvlakken voor de ontwikkelomgeving
12. Interne koppelvlakken met beheer en audit
13. Koppelnetwerken met vertrouwde organisaties

Beschrijft gecontroleerde doorgang tussen de zones

Logische toegang

14. Thema Identity & Access Management (IAM)
15. Identity Management (IdM)
16. Access Management (AM)
17. Federated Identity & Access Management
18. Single Sign-On (SSO)
19. Portaal - toegangserver
20. Vertrouwd toegangspad (VTP)

Beschrijft vertrouwde toegang tot infrastructuur en applicaties

Encryptie

21. Themapatroon Encryptie
22. Symmetrische encryptie
23. Public Key Infrastructure (PKI)
24. Elektronische handtekening
25. Sleutelhuis
26. Secure Email

Beschrijft de borging van vertrouwelijkheid en integriteit van gegevens

Logging, Monitoring en Continuïteit

27. Logging
28. Security Information Event Management (SIEM)
29. Themapatroon Bedrijfscontinuïteit (BCM)
30. Backup & Restore strategie
31. Disaster Recovery
32. Uitbesteding IT-diensten

Beschrijft vastlegging en controle van gebeurtenissen en maatregelen voor bedrijfscontinuïteit

Inhoud

0. Template van een patroon

Naam

De naam moet het doel van het patroon kort samenvatten

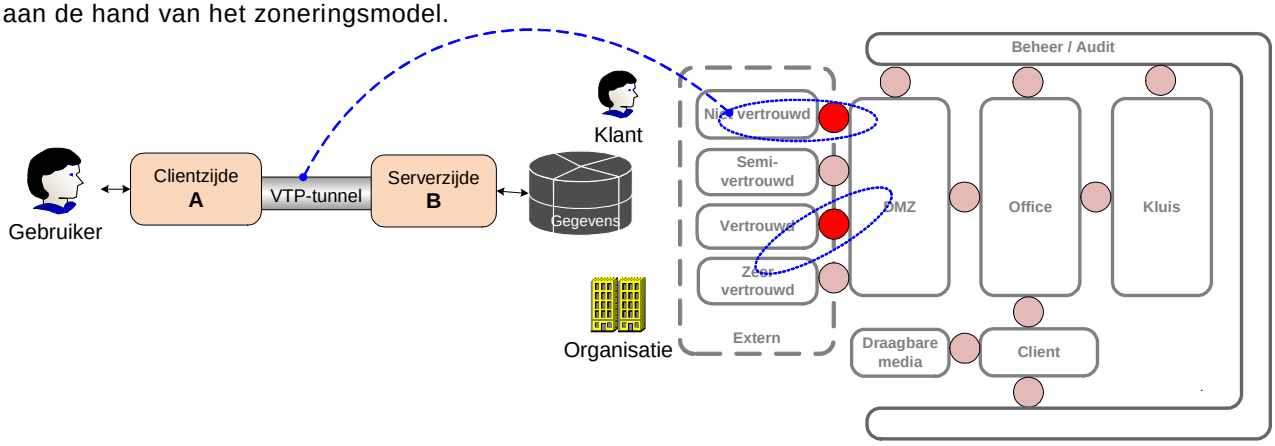
Criteria

Onder IB-criteria verstaan we: *Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid*

Hoewel voor elke beveiligingsoplossing alle IB-criteria van toepassing zijn, noemen we in deze rubriek alleen die criteria, waarvoor het patroon binnen zijn probleemstelling een functionele uitwerking biedt. In de beschouwingsmodellen zijn alle criteria van toepassing en is deze rubriek weggelaten.

Context

Beschrijft de omgeving waarin het risico of het op te lossen probleem zich voordoet, bij voorkeur geschetst aan de hand van het zoneringsmodel.



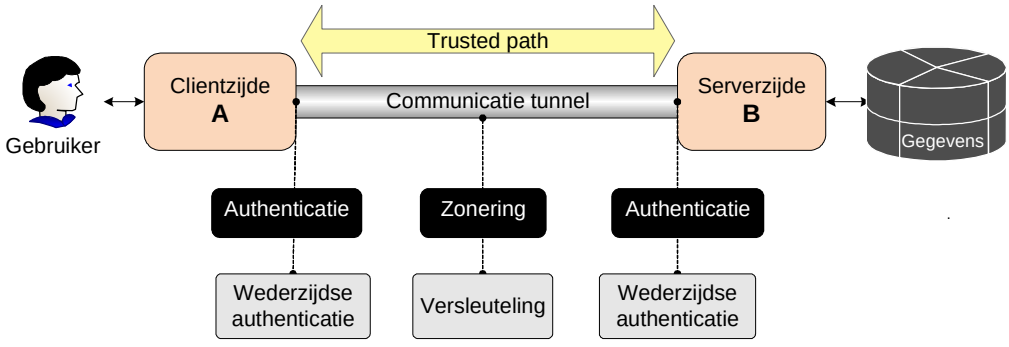
De figuur schetst de omgeving waarin het probleem zich voordoet

Probleem

Welk risico moet worden gereduceerd? Wat gaat er mis waardoor er risico's kunnen ontstaan?

Oplossing

Welke IB-functies en IB-mechanismen dragen bij aan de oplossing?



De figuur schetst de oplossing

Afwegingen

Wat zijn de voor- en nadelen en welke doorslaggevende argumenten zijn gehanteerd voor de keuze van de uitgewerkte oplossing?

Voorbeelden

Een patroon bewijst zijn waarde door het bestaan van een aantal beproefde toepassingsvoorbeelden. Per oplossingstype kunnen verschillende varianten worden beschreven in een patroon.

Oplossing gespecificeerd in een tabel

Voor patronen en beschouwingsmodellen waarbij meerdere IB-functies van toepassing zijn, wordt in een tabel de verschillende IB-mechanismen per functieblok gespecificeerd. Alleen relevante IB-functies worden vermeld in de kopregel.

Functieblok	Zonering	Authenticatie	Vastleggen gebeurtenissen	Controleren Alarmeren	Systeem integriteit
Clientzijde	- Data encryptie - Sessie encryptie - Netwerk encryptie - Lijn encryptie	- wederzijdse authenticatie - 1, 2 of 3-factor - context based aanmelden	- Beheerhandelingen - Verbindingen	- Handhaven IB-functies - Afwijkingen op beleid	- Hardening - Applicatie patch
Toegangspad	- shttp https - TLS tunnel - IPSec tunnel - Proprietary tunnel - Closed Usergroup	nvt	nvt	nvt	Infrastructuur firmwarepatches
Serverzijde	- Data encryptie - Sessie encryptie - Netwerk encryptie - Lijn encryptie	- wederzijdse authenticatie - 1, 2 of 3-factor - context based controleren	- Beheerhandelingen - Verbindingen	- Handhaven IB-functies - Afwijkingen op beleid	- Hardening - Applicatie patch

IB-Functies

IB mechanismen

Functieblok of onderdeel van het te beveiligen object, waarin de IB-mechanismen zijn verwerkt

IB-mechanismen waarmee de beveiligingsfunctie wordt gerealiseerd

IB-functies die van toepassing zijn bij deze oplossing

De tabel specificeert de oplossing per functieblok

Implicaties

Deze rubriek geeft aan welke impact de realisatie van een patroon heeft op zijn toepassingsgebied en wat de eventuele randvoorwaarden zijn. Met impact wordt bedoeld: wat *moet de organisatie doen* om gebruik te kunnen maken van de geboden oplossing van een patroon, oftewel: “Wat moet men doen om het voor elkaar te krijgen?” Bij de implicaties wordt ook de dynamiek van de oplossing beschreven, oftewel: wat zijn de gedragskenmerken tijdens operationeel gebruik?

Gerelateerde patronen

Van welke patronen is het functioneren van de oplossing van het beschreven patroon afhankelijk? Omschrijving van de relatie met andere patronen.

Leeswijzer patronen

Modellering. Voor de patronen in dit document is er voor gekozen om de modellering niet te baseren op de architectuurstandaard *ArchiMate.* Dat betekent overigens niet dat ArchiMate voor afbeelden van IB-patronen niet bruikbaar zou kunnen zijn. Bij dit document is gekozen voor een meer illustratieve tekenwijze, die ook te begrijpen is voor gebruikers die ArchiMate niet kennen, of waarvoor deze architectuurstandaard leidt tot te abstracte beelden. Als blijkt dat er vraag naar is, dan wordt er alsnog een ArchiMate versie van deze IB-patronen uitgebracht.

IB-functies Bij patronen die ketens van bedrijfsfunctionaliteiten of componenten weergeven, worden de IB-functies en -mechanismen aangegeven onder de functieblokken waar ze betrekking op hebben.

Bij de patronen van koppelvlakken en beschouwingsmodellen, zijn de IB-functies en IB-mechanismen per functieblok afgebeeld in een tabel.

Bij patronen die specifiek één IB-functie invullen, zoals IAM, PKI, Logging en SIEM, worden IB-functies niet als zwarte blokken weergegeven; er is immers maar één IB-functie werkzaam. De mechanismen worden benoemd en toegelicht in de figuren en oplossingsbeschrijving.

Rubrieken: Als een rubriek in een patroon niet van toepassing is, dan wordt deze weggelaten.

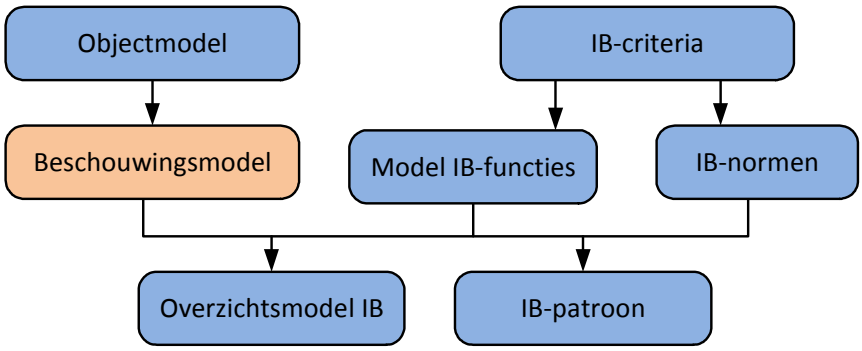
DEEL 1: BESCHOUWINGSMODELLEN

Context

Een beschouwingsmodel maakt onderdeel uit van de *NORA aanpak voor IB-architectuur*, zoals hieronder is aangegeven.

Doel van een beschouwingsmodel is het afbeelden van IB-*mechanismen* die IB-*functies* uitvoeren in IT-ketens of onderdelen daarvan.

Beschouwingsmodellen geven in de functieblokken van generieke infrastructuur aan waar de beveiligingsfuncties aangrijpen. Evenals bij patronen wordt vanuit een probleemstelling een oplossing gegeven. De overige patroonrubrieken ontbreken in de beschouwingsmodellen. In een tabel wordt per functieblok aangegeven welk mechanisme de IB-functies realiseren.



NORA aanpak IB-architectuur

Toepassing van beschouwingsmodellen

In dit document is het beschouwingsmodel als eerste gebruikt om een generieke afbeelding te maken van het IT-landschap van een organisatie: het *beschouwingsmodel Zonering*. Dit model wordt in de patronen van Deel 2 telkens gebruikt als context. De IB-functie Zonering bepaalt daarbij de logische indeling van het model. Per zone kan een bepaald *vertrouwensniveau* worden gerealiseerd.

De overige beschouwingsmodellen uit dit document beelden IB-functies en IB-mechanismen af in de belangrijkste bouwblokken van de generieke infrastructuur; zie onderstaand overzicht.

Deel 1. Beschouwingsmodellen

1. Beschouwingsmodel zonering: *Beschrijft de basistopologie van een bedrijfsnetwerk.*
2. Client
3. Server
4. Server Virtualisatie
5. Netwerk
6. Draadloze netwerken
7. Printer

Beschrijft hoe de IB-patronen in samenhang werkzaam zijn in de delen waaruit generieke infrastructuur is opgebouwd

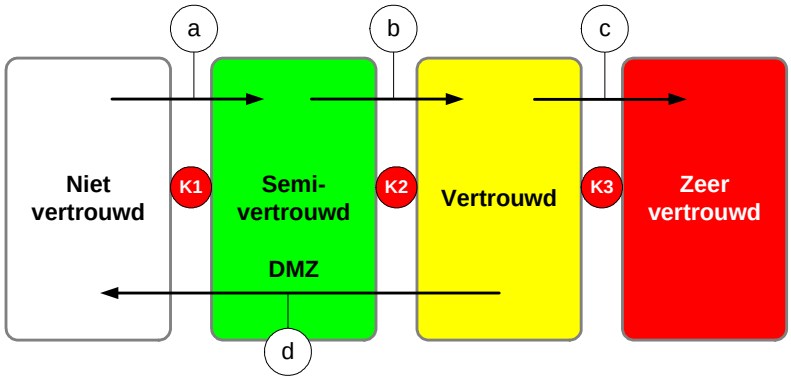
1. Zonering

Basismodel van zonering

Het beschouwingsmodel Zonering is een abstractie van een IT-landschap, waarin standaard zones worden onderkend. Een zone is een afgebakend netwerk van IT-voorzieningen, waarin gegevens vrijelijk kunnen worden uitgewisseld. Gegevensuitwisseling met andere zones verloopt via gedefinieerde koppelvlakken. Het model dient als vaste context voor een reeks van IB-patronen en kan worden beschouwd als een standaard oplossing, die niet in één enkel IB-patroon wordt beschreven, maar in een hele reeks.

Het primaire doel van zonering is *isoleren van risico's* zodat bedreigingen en incidenten uit de ene zone niet kunnen doorwerken in de andere zone. Zonering maakt daarmee mogelijk dat de volgende vier vertrouwensniveaus onderscheiden kunnen worden: Niet vertrouwd, Semi-vertrouwd, Vertrouwd en Zeer vertrouwd. Deze vertrouwensniveaus komen tot uitdrukking in de maatregelen die worden getroffen in de koppelvlakken Kx.

Bij het uitwerken van veel IB-patronen gebruiken we een beschouwingsmodel, dat is afgeleid van onderstaand basismodel. De figuur laat zien dat de toegang vanuit de niet vertrouwde omgeving (extern) naar de vertrouwde omgeving (intern) *in lagen* is opgebouwd. Een beveiligingslaag wordt gevormd door een set van maatregelen, die de zone afbakenen en door maatregelen in het verbindende koppelvlak K, weergegeven door K1, K2 en K3 in de figuur.



Basismodel zonering

Mocht één laag worden doorbroken, dan voorkomt de volgende beveiligingslaag in deze structuur dat bedrijfsprocessen en gegevens direct kunnen worden benaderd vanuit de niet vertrouwde zone. De gelaagdheid is tevens gebaseerd op het stapsgewijs communiceren van niet vertrouwd naar vertrouwd en omgekeerd, zie (a), (b), (c) en (d). De pijlrichting geeft het initiatief van informatie-uitwisseling aan.

Niet vertrouwde zone: Deze zone, ook bekend als de externe zone, bevat systemen, die niet onder het beveiligingsregime en de (beheer) verantwoordelijkheid vallen van de organisatie. Het internet is een voorbeeld van een niet vertrouwde zone, waarin klanten of partners vanuit hun eigen omgeving communiceren met de organisatie.

Semi-vertrouwde zone: Bevat systemen die onder het beveiligingsregime en verantwoordelijkheid van de organisatie staan, maar waar geen productiedata mag worden bewerkt en opgeslagen. Een DMZ (Demilitarized zone) is een voorbeeld van een semi-vertrouwde zone. Semi-vertrouwd houdt in dat opgeslagen data beperkt is tot publieke informatie.

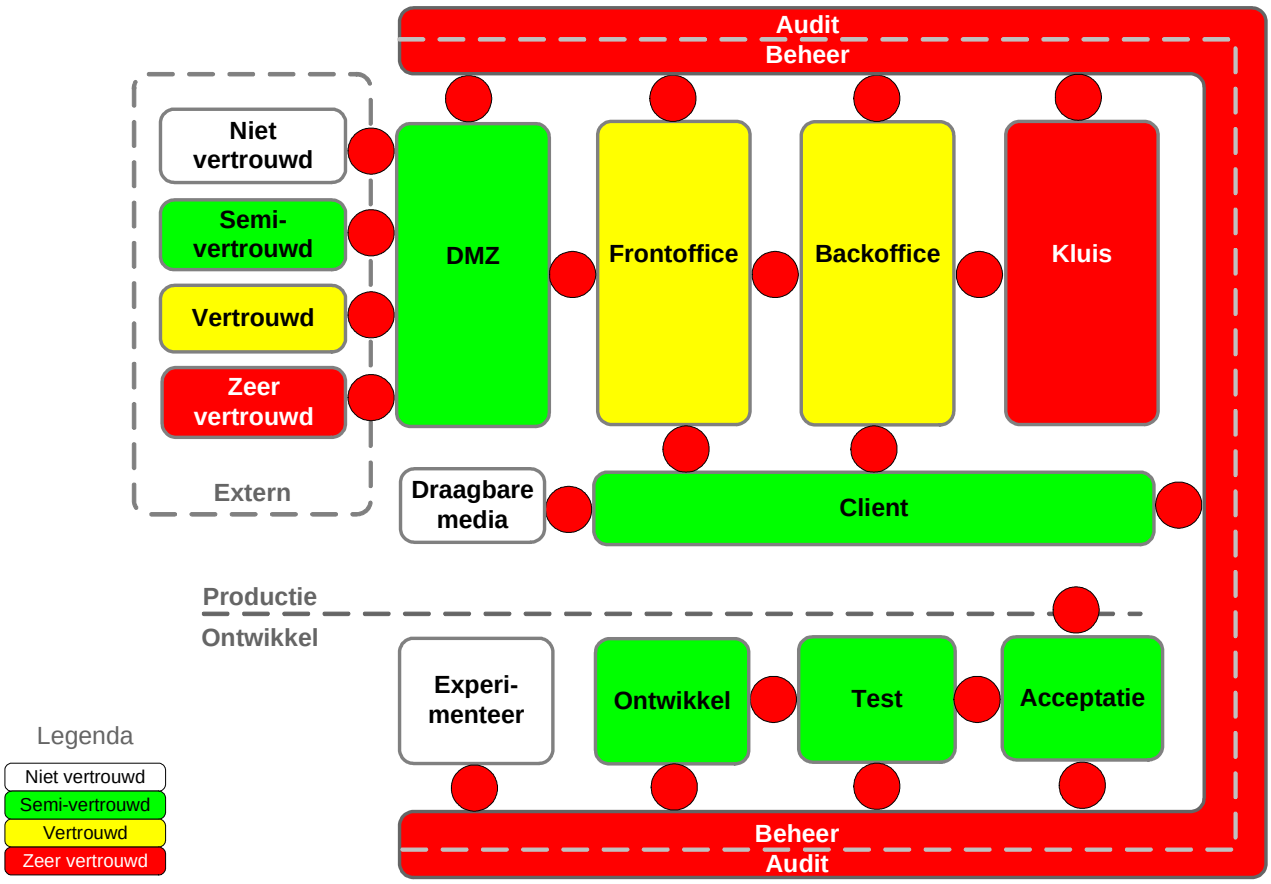
Vertrouwde zone: Deze zone bevat alle informatieverwerkende systemen voor de primaire bedrijfsvoering en staat onder het beheer en controle van de organisatie. Bij grotere organisaties wordt deze zone soms onderverdeeld in de (sub)zones: Frontoffice, Midoffice en Backoffice. Deze onderverdeling sluit tevens goed aan bij het ontwerp van Multi-tier oplossingen. De vertrouwde zone omvat in volume het overgrote deel van de bedrijfsinformatie.

Zeer vertrouwde zone: In deze extra beveiligde zone wordt uitsluitend bedrijfskritische informatie opgeslagen, m.a.w. de "kroonjuwelen" van een organisatie. Deze informatie is cruciaal voor het voortbestaan van de organisatie. Communicatie met deze zone is mogelijk voor een beperkt aantal systemen vanuit de vertrouwde zone, waarbij de gegevensuitwisseling wordt gecontroleerd. Ook de beheeromgeving valt onder de categorie 'zeer vertrouwd'.
In de koppelvlakken K1, K2 en K3 zijn allerlei filterfuncties opgenomen, die er voor zorgen dat de communicatie wordt getoetst aan het voor de organisatie geldende IB-beleid. Bepalend daarbij zijn de communicatie*protocollen* en de communicatie*richting*. De koppelvlakken bevatten naast filterfuncties ook sensoren die de afwijkend gedrag opmerken, daarover informatie vastleggen en potentiële doorbraken

signaleren aan een intern Computer Emergency Response Team (CERT).
In deze opstelling kan inkomend verkeer vanuit de niet vertrouwde zone (a) alleen communiceren met systemen in de Semi-vertrouwde zone (DMZ). Vanuit de DMZ kan de communicatie worden doorgezet naar de zone Vertrouwd (b).
Door beveiliging *gelaagd* in te richten, kunnen risico's beter worden beheerst dan met de traditionele zonering volgens het "kasteelmuur" principe. Daar geldt: je bent buiten (extern) óf je bent binnen (intern).

Beschouwingsmodel zonering

Vanuit het gelaagde basismodel is in onderstaande figuur een zoneringmodel uitgewerkt, dat toepasbaar is als beschouwingsmodel voor een willekeurig grote organisatie.



Beschouwingsmodel Zonering

Met de kleuren gerelateerd aan de Jericho[1] classificering, is hierboven de gelaagdheid van het gewenste vertrouwensniveau aangegeven. Wat opvalt is dat maar een beperkt deel van de IT-omgeving als 'vertrouwd' is aan te merken. Toegevoegd aan het basismodel zijn de zones voor interne en externe clients en zones voor derden die informatie uitwisselen met de organisatie. De systeemontwikkelomgeving van de organisatie is aangegeven als een afzonderlijk cluster van zones, met koppelingen naar elkaar en naar de productieomgeving. Tenslotte is een beheer en auditzone toegevoegd waaraan alle zones gekoppeld zijn.

Elk koppelvlak kent specifieke afspraken voor gecontroleerde doorgang. Zo is het niet mogelijk om vanuit een willekeurige zone via de Beheerzone toegang te krijgen naar een andere zone.
Door de complexe werkelijkheid op deze manier in logische blokken op te knippen, wordt het IT-landschap overzichtelijk en toetsbaar op toepassing van beveiligingsrichtlijnen en maatregelen.

Vertrouwensniveaus

Evenals de basisopzet van zonering, kent het beschouwingsmodel zonering vier niveaus van vertrouwen, die tot uitdrukking komen in de maatregelen die worden getroffen in de opzet van de koppelvlakken.

[1] Jericho is een beveiligingsconcept voor "open netwerken"; zie jerichoforum.org

Beschrijving van de zones

Deze paragraaf beschrijft de betekenis van de ‘standaard’ zones van het beschouwingsmodel en het gehanteerde minimum beveiligingsniveau.

Extern: Dit domein omvat alles wat buiten de directe bescherming en het beheer van een organisatie valt en moet daarom als *niet vertrouwd*[2] worden aangemerkt. Vanuit een organisatie kunnen verschillende *communicatiekanalen* naar de buitenwereld worden ingericht: koppeling met een *niet vertrouwde* zone, een *semi-vertrouwde* zone, een *vertrouwde* zone en met een *zeer vertrouwde* zone. Wordt bijvoorbeeld het IT-beheer van een organisatie geheel uitbesteed, dan is daarvoor een *zeer vertrouwd* kanaal nodig naar de beheerserviceprovider. Ook voor uitwisseling van zeer vertrouwelijke informatie tussen organisaties is dit kanaal nodig. Organisaties die elkaar geheel vertrouwen, zorgen voor wederzijdse maatregelen en handhaving van het beveiligingsniveau, zodat bij de koppeling een beperkte grensbescherming nodig is. Ook organisaties die op het niveau van *semi-vertrouwd* informatie uitwisselen, nemen deze maatregelen, waarbij een beperkte grensbescherming nodig is. Samengevat ligt de zwaarte van de maatregelen voor koppeling met niet vertrouwde zones vooral op de grensbescherming *in* het communicatiekanaal. Bij de koppeling van vertrouwde zones ligt de focus vooral op beschermende maatregelen van het kanaal zelf (de sterkte van de tunnel).

DMZ: Dit domein is een neutraal gebied tussen de buitenwereld en de organisatie en fungeert voornamelijk als *doorgeefluik*. De buitenkant van een DMZ wordt gevormd door een grensbescherming met solide filterfuncties. Binnen de DMZ bevinden zich mechanismen voor filtering van protocollen en ongewenste communicatie, functies voor ontkoppeling (proxy), voor protocoltransformatie en misleiding van hackers en monitoring. De DMZ bevat in veel gevallen ook webservers, die publiek toegankelijke organisatiegegevens bevatten. Het beveiligingsniveau is semi-vertrouwd, omdat de aanwezige data in een DMZ in het uiterste geval als *opgeefbaar* moeten worden beschouwd. Als de grensbescherming aan de buitenkant namelijk 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 de vertrouwde domeinen.

Frontoffice: De frontoffice van een organisatie is een vertrouwde zone. Het bevat systemen die gericht zijn naar de buitenwereld, zoals webservers. In de frontoffice zijn zowel informatieverstrekkende webservers opgesteld als webservers die transacties van gebruikers kunnen doorzetten naar de backoffice. Vanuit de klant gerekend fungeert de frontoffice als ‘poort’; waar klantinformatie word verwerkt tot organisatie-informatie en omgekeerd. Het koppelvlak tussen front- en backoffice (6) fungeert als een netwerk of een ‘servicebus’, waarop de informatie vanuit de backoffice beschikbaar is. De frontoffice is een vertrouwd domein.

Backoffice: Deze zone bevat zowel ondersteunende systemen voor de frontoffice als systemen voor het vullen van de bedrijfskritische systemen die in de Data zone staan opgesteld. De backoffice is een vertrouwd domein, waar applicaties draaien voor normale bedrijfsvoering van de organisatie zelf.

Kluis: Deze zone bevat uitsluitend bedrijfsinformatie dat van vitaal belang is voor het voortbestaan van een organisatie. Het zijn de ‘kroonjuwelen’ van de organisatie. Communicatie met deze zone is mogelijk voor een beperkt aantal systemen vanuit de vertrouwde zone, waarbij de gegevensuitwisseling wordt gecontroleerd..

Client: Deze zone omvat de kantooromgeving met eindgebruiker-werkplekapparatuur, LAN-netwerken en netwerkprinters van een organisatie. Deze *eindgebruikers systeemomgeving* korten we af met de *client*. Dit domein moet worden aangemerkt als semi-vertrouwd in verband met de grote aantallen aansluitingen en de relatief grote kwetsbaarheid voor inbreuk. De controle op naleving van beveiligingsrichtlijnen in dit “kantoordomein” is doorgaans beperkt. Wanneer organisaties besluiten om medewerkers in een kantooromgeving te laten werken met systemen in de ontwikkel, test, acceptatie of beheerzone, dan dienen er aanvullende maatregelen genomen te worden om de voor de beveiligingsniveaus vereiste logische scheiding én scheiding van taken mogelijk te maken. Dit betreft zowel technische als organisatorische maatregelen.

Draagbare media: Clientapparatuur is afhankelijk van de soort voorzien zijn van DVD/Cd-Rom drives, geheugenslots, USB-interfaces en draadloze netwerkinterfaces zoals Wi-Fi en Bluetooth. Dit domein wordt beschouwd als niet vertrouwd, omdat ze met uitzondering van specifiek door organisatie uitgereikte versleutelde USB-sticks niet vallen onder het beheer de eigen organisatie. Om te voorkomen dat

[2] Extern is niet synoniem voor “alles wat niet te vertrouwen is”. Een veilig netwerkkanaal, aangeboden door een service provider valt ook onder het externe domein.

schadelijke code via deze media de client binnendringt, worden deze interfaces op basis van beleidregels (policy) niet- of slechts beperkt opengesteld en vindt inspectie plaats op alle data dat via het koppelvlak van client naar draagbare media binnenkomt of uitgaat.

Beheer: Deze zone is *zeer vertrouwd*, omdat beheerders met hogere privileges hun werk moeten kunnen uitvoeren. De toegang tot clients van beheerders is afgeschermd van gewone kantoortaken zoals die uitgevoerd kunnen worden vanaf de interne client. Met behulp van functiescheiding en technische maatregelen worden beheertaken strikt gescheiden van auditwerkzaamheden. De beheerfuncties die via remote beheer clients of interne clients kunnen worden uitgevoerd, zijn wat betreft bevoegdheden beperkt ten opzichte van de bevoegdheden van beheerders binnen de beheerzone van een organisatie.

Audit: Deze zone wordt gebruikt voor het scheiden van monitoring en verificatiefuncties van de operationele beheertaken. Audit informatie vanuit logfiles, mag niet – of niet ongemerkt kunnen worden gewijzigd door beheerders of eindgebruikers. De voor audit doeleinden verzamelde informatie wordt in de auditzone geaggregeerd en beveiligd opgeslagen en verlaat deze zone via het netwerk niet meer in de oorspronkelijke vorm.

Experimenteeromgeving: Deze zone is een laboratoriumomgeving, die fysiek is gescheiden van de overige omgevingen. Vanwege het experimentele karakter van de IT-middelen en werkprocessen binnen deze omgeving (ook wel laboratorium genoemd) is dit een *niet vertrouwd* domein.

Ontwikkelomgeving: In deze zone worden nieuwe producten ontwikkeld en beproefd, of staan systemen afgeschermd in afwachting van goedkeuring voor toepassing in de productieomgeving van een organisatie. Het ontwikkeldomein is als *semi-vertrouwd,* geclassificeerd, omdat er met utilities en tools gewerkt moet worden die in productieomgevingen niet- of zeer beperkt toegepast mogen worden.

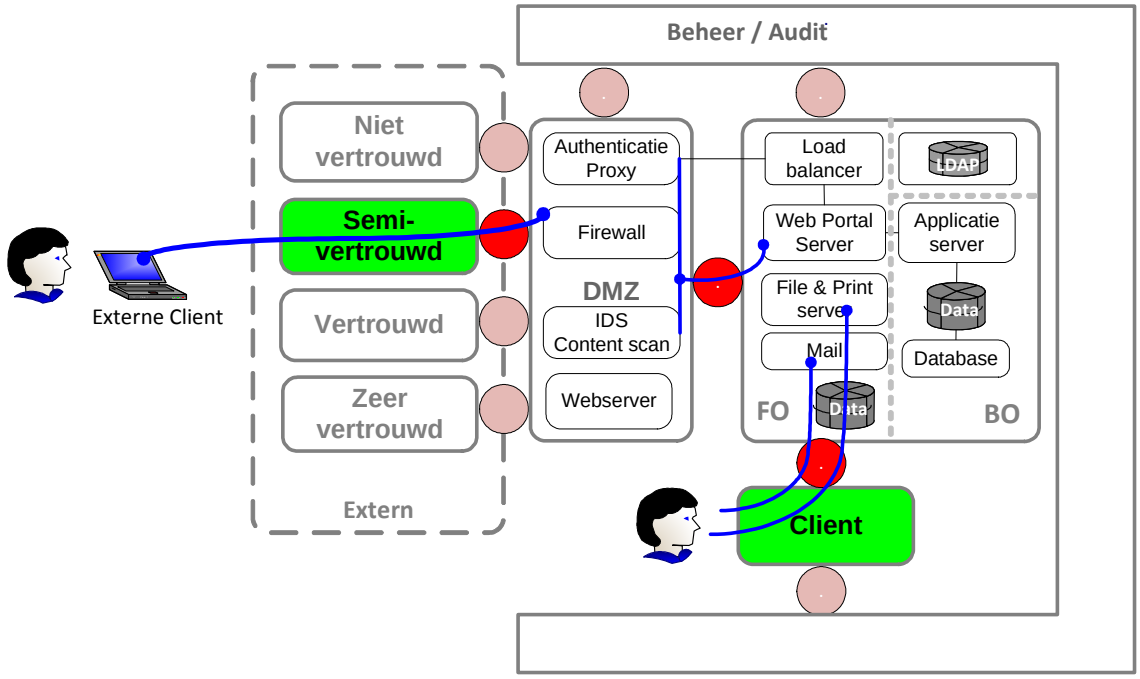
Testomgeving: In deze zone worden systemen functioneel en technisch beproefd of ze aan de eisen voldoen. Het vertrouwensniveau van dit domein wordt bepaald door de noodzakelijke geïsoleerde opstelling en omdat in deze zone geen productiedata mag worden bewerkt of worden opgeslagen.

Acceptatieomgeving: Dit domein is het ‘voorportaal’ van de productieomgeving. Hier worden systemen gecertificeerd op het voldoen aan de eisen van de productieomgeving. Het vertrouwensniveau is ook hier semi-vertrouwd, omdat ook hier geen productiedata mag worden opgeslagen.
De acceptatieomgeving is wat betreft maatregelen vergelijkbaar met de productieomgeving om een realistische bedrijfssituatie te kunnen simuleren.

2. Client

Context

Onder een *client* verstaan we *computers* die bedrijfsfuncties en -gegevens voor eindgebruikers persoonlijk toegankelijk maken. Clients komen in de bedrijfsomgeving zowel in het interne domein als in het externe domein voor, zowel draagbaar als vast. Gebruikers hebben vanuit clients, op basis van hun autorisaties toegang tot bedrijfsapplicaties. In alle gevallen is er sprake van het raadplegen of bewerken van bedrijfsfuncties of bedrijfsgegevens door interne of externe medewerkers of contractors.



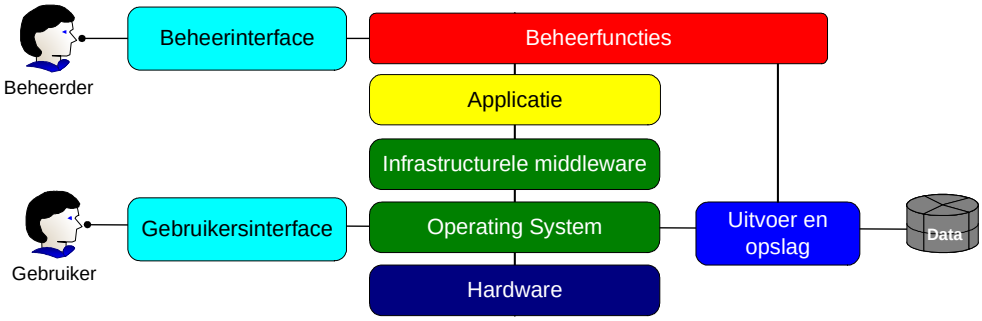
Clients van een organisatie

Probleem

1. **Variërende awareness en IT- deskundigheid van eindgebruikers** veroorzaakt besmetting (virus en malware), waardoor ongeautoriseerde toegang mogelijk is, dataverlies ontstaat of dat IT-services en gegevens niet beschikbaar zijn.
2. **Kwetsbaarheden in uitvoerbare code** zorgt voor mogelijkheden voor inbreuk van buitenaf. Met name code voor clients blijkt vanwege de opzet in de praktijk zeer kwetsbaar. De uitvoerbare code betreft Operating Systemen en applicaties.
3. **Meer functionaliteit ingeschakeld dan nodig** voor de bedrijfsvoering, waardoor mogelijkheden tot diefstal of inbreuk toenemen.
4. **Beperkte beveiligingsmogelijkheden** van Mobiele apparaten maakt PDA's, tablets en laptops extra kwetsbaar voor dataverlies en inbreuk.

Oplossing

Clients kunnen beschouwd worden als een stelsel van functieblokken. Elk functieblok is voor de uitvoering van z'n taak uitgerust met beveiligingsfuncties. Per beveiligingsfuctie is in onderstaande tabel aangegeven welke IB-mechanismen per functieblok van toepassing zijn. Beheerfuncties zijn uitgewerkt in het patroon "Interne koppelvlakken met beheer en audit".



Functieblokken van een client met zijn interfaces

Functieblok	Continuïteit	Geprogramm. controles	Zonering	Filtering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Controleren Alarmeren	Systeem integriteit
Beheer interface	nvt	Vragen om toestemming van gebruiker	nvt	Telefonisch of chatcontact met helpdesk	nvt	Gescheiden account voor beheer- en gebruikersfunct.	Logging van elke beheerhandeling	Handhaven van IB-functies	nvt
Invoer en gebruikers interface	nvt	nvt	Media-encryptie	Virus en malware scanning + Personal firewall	1- of 2-factor	Minimaliseren rechten	nvt	nvt	nvt
Applicatie	Broncode deponeren	Controle op: - Invoer - Verwerking - Uitvoer	nvt	nvt	nvt	-Gebruikers accounts -Functionele accounts	-Vollopen buffers -IB events -Applicatielog	Handhaven IB -functies	-Hardening -Sandbox -Applicatiepatch
Infrastruct. middleware	Rollback vanaf image op disk	- Deployment - Configuratie	- TLS/SSL - Alleen noodzakelijke functionaliteit	Intrusion detectie Personal firewall	- Pincodeopstart - Systeem ww	Gebruikers account voor toegang tot applicaties	Virus/Malware meldingen Personal firewall meldingen	Alarm op virus/ malware	-Hardening -Sandbox -Systeempatch -Vulnerabilityscan
Operating System	Rollback vanaf image op disk	nvt	Ongebruikte poorten uitgeschakeld of verwijderd	nvt	-Pincode -opstart -Systeem ww	Gebruikers account toegang tot apparaat	OS logging beveiligingsevents	Handhaven IB-functies	-Hardening -Codescan/hash -OS-patch -Vulnerabilityscan
Hardware	Reserve onderdelen	nvt	Afgesloten systeemkast	nvt	-BIOS ww -Tokens	Fysieke sleutel	-Sylog -Klok NTP, temperatuur, defecten	CPU load, buffer - overflow, netwerk-bandbreedte	-Hardening -Firmwarepatch
Uitvoer en opslag	Backup&Restore automatisch of op gebruikers commando	nvt	Mediaencryptie" - HDD / SSD - CD/DVD/Bray - USB devices	nvt	Ww gescheiden van toepassing-gegevens opgeslagen	Temp-bestanden alleen voor systeembeheer toegankelijk	nvt	nvt	Foutloos berichtenverkeer en opslag (RAID)

IB-Functies

IB mechanismen

Maatregelen per functieblok voor clients

Afwegingen

Niet alle maatregelen zijn van toepassing op elk type client. Per type; vast of mobiel, PDA, Tablet, Laptop, PC-werkstation of Linux-werkstation zal op basis van een risicoafweging bepaald moeten worden welke maatregelen dienen te worden toegepast.

Implicaties

PDA's of smartphones worden vaak niet als 'client' beschouwd, maar moeten afhankelijk van de ontsluiting van bedrijfsfuncties en gegevens wel degelijk als zodanig worden ingericht, beheerd en gebruikt. Met name voor opslag van attachments, gebruikersgegevens en telefoonboeken fungeren deze devices minimaal als opslagmedia en thin-client, met toepassing van pincode voor toegang tot het apparaat, toegangscontrole voor bedrijfsapplicaties en sterke versleuteling van gegevensopslag.

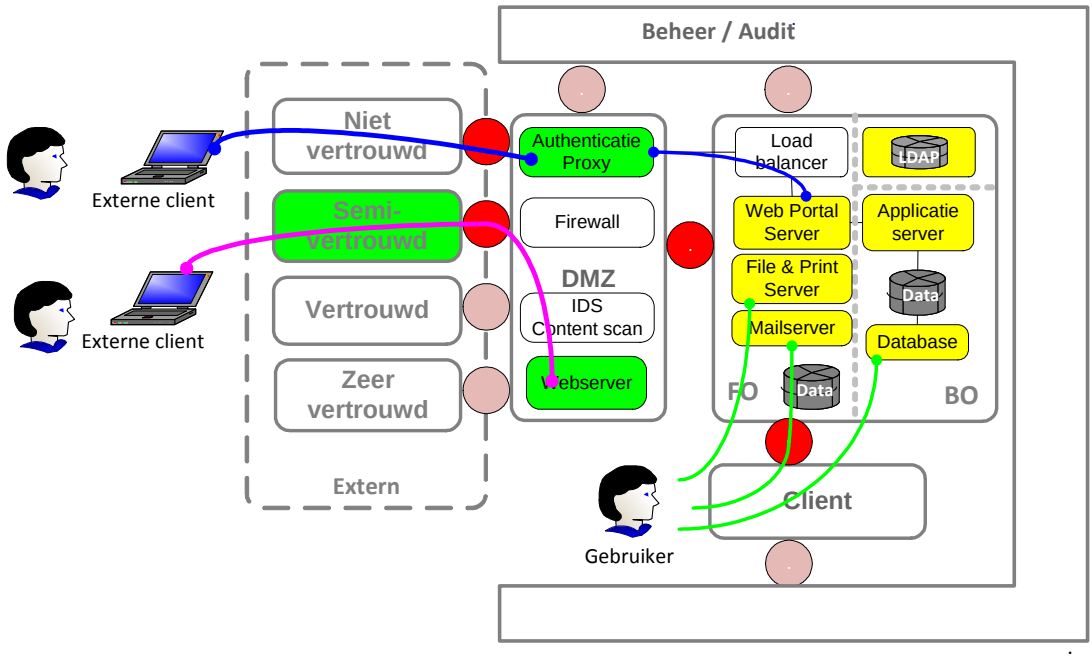
3. Server

Context

Servers zijn computers die *via* clients applicatieve diensten beschikbaar stellen aan eindgebruikers of aan andere computersystemen. De gekleurde blokken in onderstaande figuur zijn voorbeelden van verschillende typen servers in de netwerktopologie van een organisatie.

Een gebruiker logt vanuit internet aan op een authenticatieserver. Deze server geeft de relevante gebruikersgegevens door aan een portal-toegangsserver, die op zijn beurt applicatieve diensten vanuit backoffice servers beschikbaar stelt. De onderste gebruiker is een medewerker van een vertrouwde partij en zoekt via dat kanaal informatie op een webserver van de partnerorganisatie.

Dit beschouwingsmodel beschrijft alle *infrastructurele* IB-problemen en oplossingen, die servers gemeenschappelijk hebben en daarom als 'generiek' gekenmerkt kunnen worden.



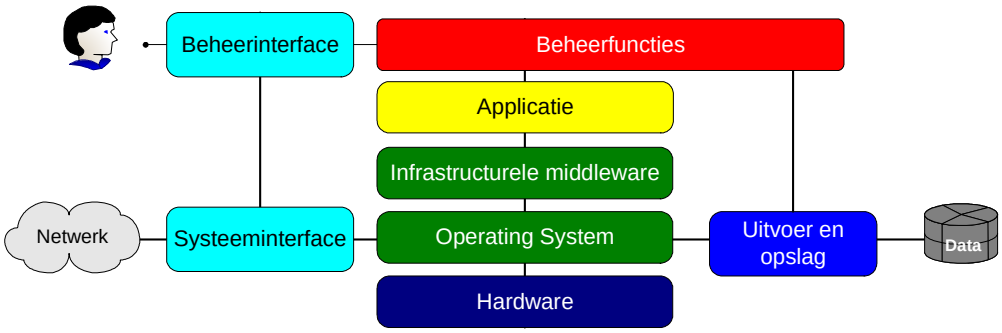
Servers van een organisatie

Probleem

1. **Kwetsbaarheden in uitvoerbare code** zorgt voor mogelijkheden tot besmetting (virus en malware) waardoor ongeautoriseerde toegang kan plaatsvinden en dataverlies of datalekkage kan ontstaan. De uitvoerbare code betreft Operating Systemen en applicaties.
2. **Meer functionaliteit ingeschakeld dan nodig** is voor de bedrijfsvoering, waardoor mogelijkheden tot diefstal of inbreuk toenemen.
3. **Gevoelig voor aanvallen van buitenaf**, zoals (D)DoS en SYN (Synchronous) flood, met name servers in de DMZ. Distributed Denial-of-service aanvallen (D)DoS, zijn pogingen om dienstverlening via computers of netwerken van computers onmogelijk te maken voor de bedoelde gebruikers. Wat er gebeurt is dat het doelsysteem verzadigd wordt met dummy-*communicatieverzoeken*, zodat het systeem overbelast raakt en de bedoelde gebruiker uiteindelijk geen dienst kan afnemen. Iets vergelijkbaars gebeurt met Synchronous flood (SYN), waarbij het doelsysteem TCP-SYN pakketjes ontvangt, SYN-ACK pakketjes terugstuurt, maar nooit een ACK bevestiging krijgt omdat de SYN-ACK pakketjes door de hacker (-tool) naar een fout adres gerouteerd worden. De server raakt vervolgens overbelast omdat het toch blijft proberen voor elk communicatieverzoek een ACK bevestiging terug te krijgen.
4. **Single point of Failure** in de informatieketen (SpoF), afhankelijk van de functie van de server.

Oplossing

Servers kunnen worden beschouwd als een stelsel van functieblokken. Elk functieblok is voor de uitvoering van z'n taak uitgerust met beveiligingsfuncties. Per beveiligingsfuctie is in onderstaande tabel aangegeven welke IB-mechanismen per functieblok van toepassing zijn. Beheerfuncties zijn uitgewerkt in het patroon *Interne koppelvlakken met beheer en audit*.



Functieblokken van een Server met zijn interfaces

Functieblok	Continuïteit	Geprogramm. controles	Zonering	Filtering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Controleren Alarmeren	Systeem integriteit
Beheer interface	Inband & outband beheerinterface	- Deployment - Configuratie	Fysiek	nvt	2-factor	Gescheiden account voor beheer- en gebruikersfunct.	Logging van elke beheerhandeling	Alarm op ongeautoriseerde beheerhandeling	nvt
Systeem interface	-Dubbele poorten -Input buffering	nvt	Media-encryptie	-Virusscan -Malwarescan -Spam filter -Contentscan	1- of 2-factor	Minimaliseren rechten	Vollopen buffers -IB events	-Drempelwaarden	Noodstop, Foutloos berichtenverkeer
Applicatie	- Uitwijkgeschikt - Load balancing - Broncode deponeren	Controle op: - Invoer - Verwerking - Uitvoer	nvt	nvt	nvt	-Gebruikers accounts -Functionele accounts	-Vollopen buffers -IB events -Applicatielog	Systemresources Drempelwaarden Handhaven IB - functionaliteit	-Hardening -Sandbox -Appl.patch
Infrastruct. middleware	- Uitwijk voorz. - Update/rollback	- Deployment - Configuratie	-TLS/SSL, -Alleen noodzakelijke functionaliteit activeren	IDS, Firewall	LDAP, DNS, PKI	-Systeem-autorisaties -Functionele accounts	-Syslog -Vollopen queues -IB events	Systemresources Drempelwaarden Handhaven IB - functionaliteit	-Hardening -Sandbox -Systeempatch -Vulnerabilityscan
Operating System	- Uitwijk voorz. - Update/rollback	nvt	Ongebruikte poorten uitgeschakeld of verwijderd	nvt	-Pincode -opstart -Systeem ww	Systeem-autorisaties	-Syslog -Logging -IB events	Systemresources Drempelwaarden Handhaven IB - functionaliteit	-Hardening -Codescan/hash -OS-patch -Vulnerabilityscan
Hardware	- Uitwijk voorz. - Dubbele PSU en netwerk interface - Fysieke of geogr. scheiding	nvt	Afgesloten systeemkast	nvt	-BIOS ww -Tokens	Fysieke sleutel	-Sylog -Klok NTP, temperatuur, defecten	CPU load, buffer - overflow, netwerk-bandbreedte	-Hardening -Firmwarepatch
Uitvoer en opslag	-Backup/Restore -RAIDx mirroring	nvt	Mediaencryptie	nvt	Ww gescheiden van toepassing-gegevens opgeslagen	Temp-bestanden alleen voor systeembeheer toegankelijk	-Bewaartermijn -Vollopen media -Rollback	Alarm vollopen disk, tape en queues	Foutloos berichtenverkeer en opslag (RAID)

IB-Functies

IB mechanismen

Maatregelen per functieblok voor servers

Afwegingen

Niet alle maatregelen zijn relevant voor- en toepasbaar op elk type server. Per variant; applicatieserver, fileserver, mailserver of communicatieserver van het platformtype PC-OS server, UNIX-Midrange of Mainframe, zal op basis van een risicoafweging bepaald moeten worden welke maatregelen worden toegepast.

Voorbeelden

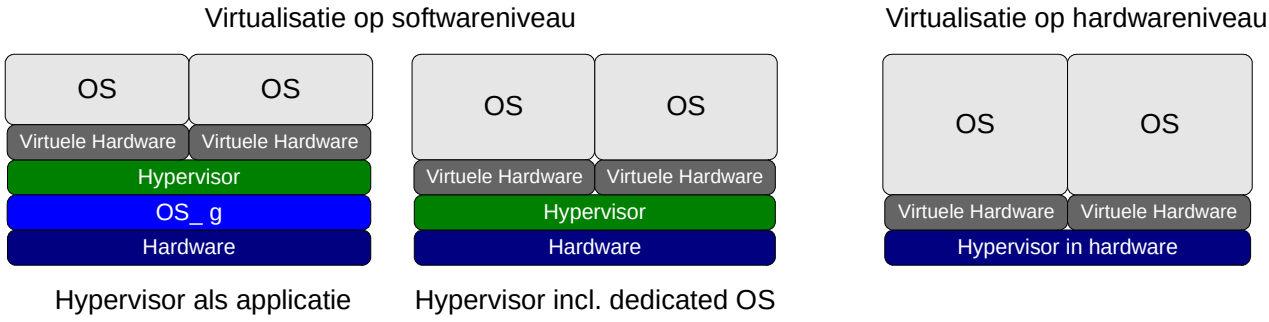
Applicatieserver, Fileserver, Mailserver, Domain server, Communicatieserver

4. Server virtualisatie

Context

Organisaties worden om economische en beheersmatige redenen gedwongen om steeds meer samen te werken en om rekencentra te centraliseren. Ze hebben vaak grote aantallen servers in beheer, waarbij voor hetzelfde bedrijfsdoel meerdere uitvoeringen van dezelfde installatie bestaan. Inmiddels zijn er z.g. virtualisatietechnieken ontwikkeld, waarbij centralisatie van hardware gecombineerd kan worden met het laten voortbestaan van autonome server-installaties voor onafhankelijk van elkaar functionerende bedrijfsprocessen.

Virtualisatie is het plaatsen van meerdere instances (zelfstandige installaties) van een Operating Systeem (OS) inclusief de daarop gehoste applicatie door een virtualisatielaag (Hypervisor) op één en dezelfde hardware. Binnen deze instances van operating systeem en virtuele hardware kunnen infrastructurele services, applicatie hosting en terminal services worden gebruikt.
Belangrijkste doelen van virtualisatie zijn centralisatie van IT services, waardoor belangrijke kostenbesparingen kunnen worden bereikt door eenheid van installatie, beheer en beveiliging.



Virtualisatie technieken

De virtuele systemen draaien volledig onafhankelijk van elkaar. De *Hypervisor* verzorgt de verdeling van resources over de virtuele systemen. De hardware kan hierdoor meer efficiënt en flexibeler worden gebruikt. Er is virtualisatie mogelijk op *software* niveau en op *hardware* niveau.

Bij virtualisatie op *software niveau* worden meerdere instances van een OS aangeboden door een softwarematige virtualisatielaag. Die laag kan op twee manieren worden aangeboden;

- Hypervisor als applicatie; waarbij de hypervisor zelf draait binnen de context van een generiek operating system (OS_g), zoals gebruikt wordt bij fileservers, applicatieservers en werkstations.
- Hypervisor inclusief dedicatie OS; waarbij de hypervisor word geleverd inclusief een mini / dedicated operating systeem, zoals het geval is bij fileservers en applicatieservers.

Bij virtualisatie op hardware niveau worden meerdere instances van een OS aangeboden door één hardwarematige virtualisatielaag. Dat houdt in dat de hypervisor ‘rechtstreeks’ op de hardware draait, zoals het geval is bij mainframes. Omdat de virtualisatielaag hardwarematig is, kost dit nauwelijks extra processorcapaciteit. Een nadeel is dat niet alle hardware hypervisor functies ondersteunt.

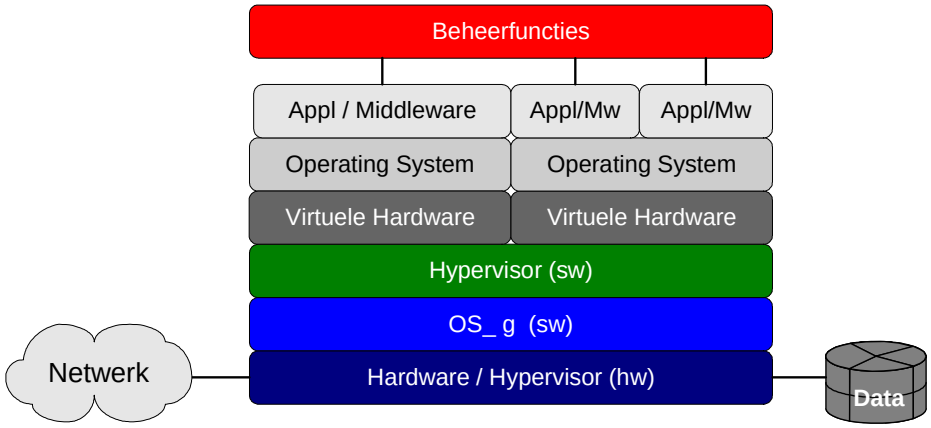
Probleem

In principe verschillen beveiligingsproblemen bij virtualisatie van servers niet van de problemen bij individuele servers. Ze zijn alleen beter te beheersen omdat veel maatregelen infrastructureel van aard zijn en de IT-services op één en hetzelfde hardware platform worden geïmplementeerd.

1. **Single Point of Failure (SPoF)**. Specifiek voor virtualisatie is de kwetsbaarheid als SPoF van de functieblokken of IT-services. Dit zijn de gemeenschappelijke *hardware*, het daarop rustende *Operating Systeem gemeenschappelijk* (OS_g) en de *Hypervisor*. Valt één van deze functieblokken uit, dan vallen daarmee alle virtuele services uit.
2. **Het verstoppen van services in de massa**. Het snel kunnen genereren en afvoeren van een virtueel systeem voor geheime doeleinden, m.a.w. het verstoppen van services in de massa van virtuele systemen. Het gemak van virtualisatie is op zich weer een complicerende beheerfactor, d.w.z. houd maar eens overzicht (in de tijd) van al deze instances en wat daarop gebeurt.

Oplossing

Per virtualisatietechniek zijn in de tabel hieronder maatregelen genoemd in *aanvulling* op de maatregelen van de patronen *Server*, *Client* en *Netwerk* services.



Functieblokken virtualisatie

Onderstaande tabel geeft per functieblok aan welke generieke maatregelen genomen moeten worden. De niet afgebeelde beveiligingsmaatregelen (voor Operating System en Middleware) zijn dezelfde als aangegeven bij server, client en netwerken. Sommige maatregelen zijn afhankelijk van de functies die de fabrikant daarvoor meelevert.

Functieblok	Continuïteit	Zonering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Controleren Alarmeren	Systeem integriteit
Beveiliging van beheerfuncties	In- en outband beheerinterface	Fysieke scheiding	2-factor	Gescheiden account voor beheer- en gebruikersfunct.	Logging elke beheerhandeling	-Ongeautoriseerde beheerhandeling -Handh.IB-funct.	-Hardening -Patches
Virtuele hardware	Fabrikant afhankelijk	Logische scheiding	Systeem ww	nvt	Syslog	-Signaleren van nieuwe & vervallen instances -Drempelwaarden	-Hardening -Patches
Hypervisor	Fabrikant afhankelijk	nvt	Systeem ww	Minimaliseren rechten	Vollopen buffers -IB-events	-Signaleren van nieuwe & vervallen instances -Drempelwaarden	-Hardening -Patches
OS_ g	- Uitwijk voorz. - Update/rollback	Ongebr. poorten uitgeschakeld of verwijderd	- Pincode -opstart - Systeem ww	Systeem-autorisaties	- Syslog: - IB-events - buffers	-System resources -Drempelwaarden -Handh.IB-funct.	-Hardening -Code scan/hash -OS-patches -Vulnerabilityscan
Hardware / Hypervisor	- Uitwijk voorz. - Dubbele hardw. - Fysiek/geograf. scheiding	Afgesloten systeemkast	- BIOS ww - Tokens	Fysieke sleutel	- Sylog: - klok - temperatuur, - defecten	Alarm CPU load, bufferoverflow en netwerkband-breedte	-Hardening -Firmware patches

IB-Functies

IB mechanismen

Maatregelen per functieblok voor virtualisatie

Voorbeelden

- Virtualisatie van clients voor telewerken en remote beheer.
- Mainframe omgevingen, met logische partitionering.
- Database virtualisatie.

Implicaties

Virtualisatie impliceert dat het beheer en de eisen voor beveiliging van de te virtualiseren systemen op orde is. Virtualisatietechnieken vereisen vaak leveranciersafhankelijke beveiligingsmaatregelen en richtlijnen, met name voor hardening van de verschillende functieblokken en beveiliging tot en met de eindpunten.

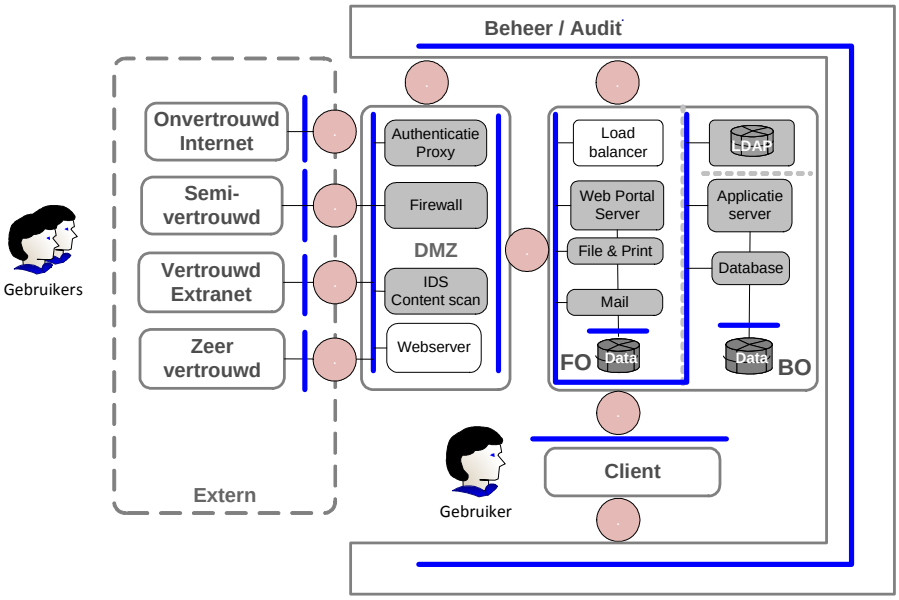
Gerelateerde patronen

- Server; die de beveiligingsfuncties per gevirtualiseerde server beschrijft.
- Client; idem voor gevirtualiseerde clients.

5. Netwerk

Context

Netwerken maken wereldwijde communicatie mogelijk tussen alle denkbare IT-apparaten. In dit patroon beschouwen we een netwerk als een communicatiepad tussen twee koppelvlakken of de onderlinge verbinding van systemen en/of koppelvakken binnen een bepaalde zone. Netwerken worden opgebouwd uit segmenten, waarbij meerdere systemen logisch met elkaar gekoppeld zijn op een segment. Onderstaande figuur schetst de belangrijkste netwerksegmenten binnen een bedrijfsomgeving.



Netwerken binnen een bedrijfsomgeving

Probleem

Bedrijfsnetwerken zijn onderdeel van IT-ketens en bestaan uit netwerksegmenten gescheiden door koppelvlakken. Deze koppelvlakken hebben zowel *koppel*- als *ontkoppel*functies. Toch heeft de actuele informatiebeveiliging van het ene segment invloed op de beveiliging van de informatie in het andere segment. Per netwerksegment zijn de volgende problemen van belang:

1. **Negatieve beïnvloeding** beveiligingsniveaus door koppeling van netwerken.
2. **Meer connectiviteit dan nodig is** voor de bedrijfsvoering.
3. **Illegaal gebruik** en onderbrekingen door ongeautoriseerde connectiviteit.
4. **Inbreuk via afluisteren** van getransporteerde data (Sniffing).
5. **Kwetsbaarheden in uitvoerbare code** (Netwerk-OS- en firmwarecode).
6. **Logische inbreuk** op netwerkelementen, routers, switches en netwerkkabels.
7. **Fysieke inbreuk** en illegale verbinding of wijzigingen van de netwerktopologie.

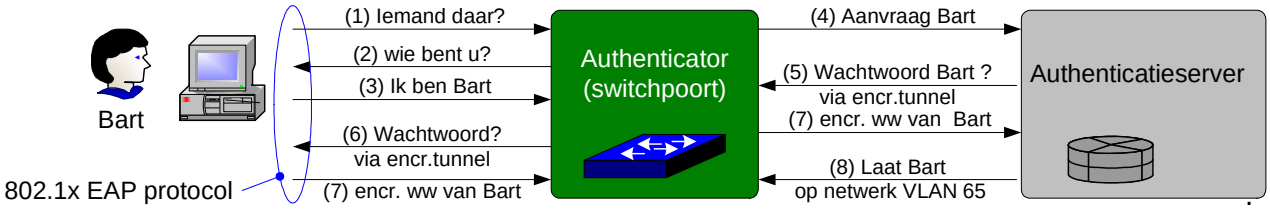
Oplossing

Probleem 1: de onderlinge beïnvloeding van netwerksegmenten, wordt in eerste instantie opgelost door passende maatregelen te nemen in de koppelvlakken (zie patronen koppelvlakken). Voor de resterende risico's op dat gebied helpt een evenwichtige verdeling van beveiligingsfuncties over de gekoppelde functieblokken van het netwerk.

Probleem 2 en 3: worden enerzijds opgelost door 'hardening' en anderzijds door *netwerkauthenticatie*. Hardening is in dit verband het doelbewust inperken van connectiviteit, zoals afsluiten van open poorten. In een omgeving van flexwerkplekken en frequent veranderende kantooromgevingen is dit echter niet haalbaar. Netwerkauthenticatie wordt ingevuld met *Port Based Network Acces Control* (PNAC) 802.1x. PNAC is een robuuste oplossing dat ongeautoriseerde toegang voorkomt. Port based Network Access Control (PNAC) is beschreven in de IEEE 802.1x standaard. Alvorens via een *client* toegang verkregen wordt tot netwerkservices, moet de gebruiker zich identificeren en authenticeren, waarna op basis van

netwerkautorisaties toegang verleend wordt. Deze maatregel is kostbaar, vergt authenticatieservers (zoals RADIUS), vergt extra beheerlast en wordt door een beperkt aantal netwerkleveranciers gerealiseerd.

PNAC past een 'handshake' techniek toe om gebruikersinformatie uit te wisselen. Daarbij worden twee basiselementen gebruikt: de *authenticator*, meestal een netwerkswitch- of router en een *authenticatieserver*, bijvoorbeeld een RADIUS server. De authenticatie verloopt via een standaard 802.1x protocol: Extensible Authentication Protocol (EAP), beschreven in RFC 3748.



Communicatiestappen van PNAC 802.1x

In de getekende acht stappen wordt gebruiker Bart toegang verleend tot het netwerk op VLAN 65. PNAC 802.1x is een relatief nieuwe- en kostbare techniek. Op elk werkstation moet een 802.1x client draaien en soortgelijke code op de host systemen. 802.1x wordt niet door alle bestaande apparatuur ondersteund. Overwogen moet worden of de kosten en technische implicaties van deze techniek opwegen tegen de extra beveiliging die langs deze weg wordt verkregen.

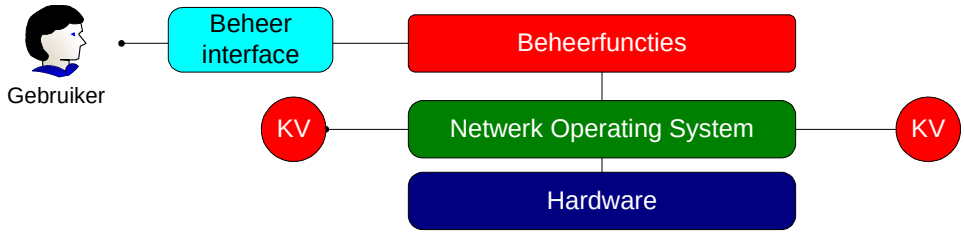
Door gebruikers in groepen in te delen, kunnen Virtuele LAN's (VLAN) worden opgezet. De gebruikers van verschillende groepen 'zien' elkaar niet, maar kunnen wel als groep met elkaar werken. Voor authenticatie van *servers* of andere nodes aan netwerken is een eenvoudige variant op PNAC beschikbaar, die gebruik maakt van het *Media Access Control* (MAC)-adres van de netwerkcontroller. Deze techniek heet MAC-Authentication Bypass (MAB). Daarvoor moet een database met MAC-adressen worden beheerd.

Probleem 4: is beheersbaar door versleuteling toe te passen op netwerkniveau.

Probleem 5 en 6: Kwetsbaarheden van uitvoerbare code zijn te beheersen door het tijdig testen en aanbrengen van patches op de firmware en hardening zoals minimalisering van functionaliteit.

Probleem 6: Logische inbreuk en illegale wijzigingen zijn beheersbaar via toegangsbeveiliging tot systeemfuncties en via monitoring en alarmering op netwerk-managementsystemen.

Probleem 7: Fysieke inbreuk is beheersbaar door patchkasten en datacommunicatieruimten af te sluiten en sleutelbeheer toe te passen en door monitoring.



Functieblokken van een netwerk met zijn interfaces

Beheerfuncties zijn uitgewerkt in het patroon *Interne koppelvlakken met beheer en audit*.

Functieblok	Continuïteit	Zonering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Controleren Alarmeren	Systeem integriteit
Beheer interface	Beheer van topologie inzichtelijk en actueel	Encryptie van beheercomm.	2-factor	Gescheiden account voor beheer- en gebruikersfunct.	Logging van beheerhandeling netwerknodes	Handhaven van IB-functionaliteit	nvt
Network Operating System	Rollback updates	-Segmentering -Quarantaine mogelijkheid -Ondersteuning van tunneling	Geautoriseerde apparatuur Netwerk - authenticatie 802.1x	Beheeraccount voor toegang tot het apparaat	NOS logging beveiligingsevents	Belasting geautomatiseerd meten/uitlezen via SNMP Handhaving IB-functies	-Hardening -Code scan van NOS-patches
Hardware	-Reserve onderdelen -Dubbel segment -Stabiele tijdbron voor timestamps	-Lijnencryptie (opt) -Afgesloten systeemkast / patchkast	BIOS wachtwoord	Fysieke sleutel systeem/patchkast	nvt	Ondersteunt centraal wachtwoord management	-Hardening, -Firmware patches

IB- functies

IB- mechanismen

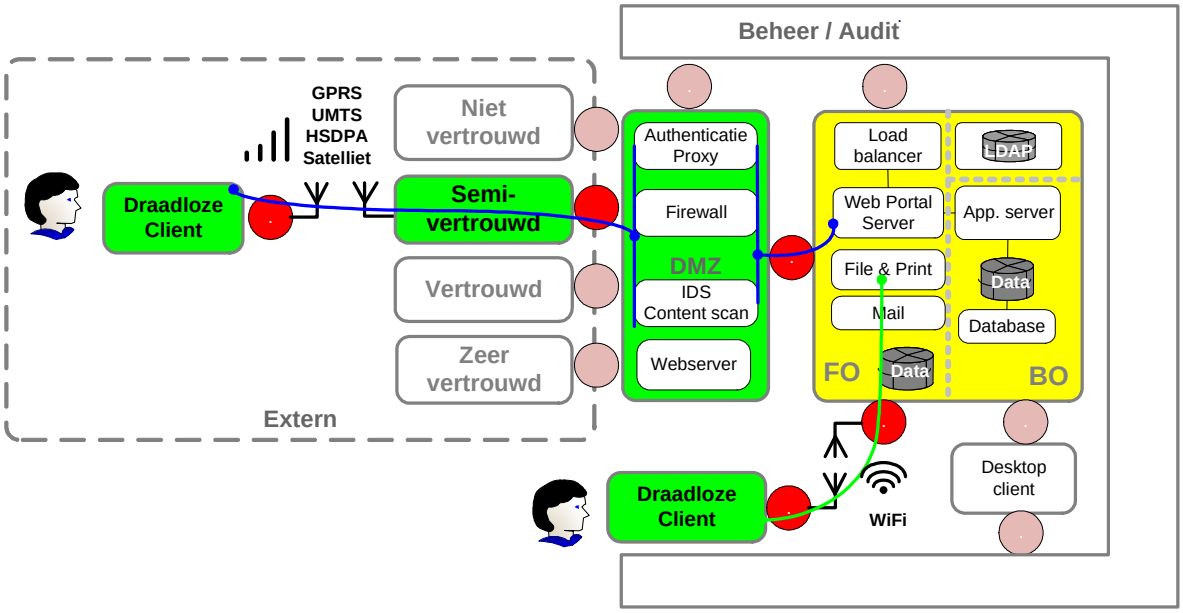
Maatregelen per functieblok voor netwerken

6. Draadloze netwerken

Context

Draadloze netwerken nemen bij zowel organisaties als in de privésfeer in een zeer snel tempo de functie van bedrade netwerken over. Gebruikers willen op elke plaats en op elk moment via hun eigen apparaat toegang kunnen hebben tot elkaar, tot bedrijfsinformatie en tot informatie op het Internet. De drijfveer is flexibiliteit en de vaste overtuiging dat mobiel werken de samenwerking en bedrijfscontinuïteit verbetert. Mensen kunnen hun werk mee naar huis nemen.

Draadloze netwerken zijn vrijwel overal te benaderen en gelijktijdig te gebruiken op hetzelfde apparaat. Voorbeelden zijn de GPRS, UMTS, HSDPA en Wi-Fi hotspot-diensten van service providers, 'Wi-Fi hotspots' in de trein, of in restaurants en Wi-Fi netwerken binnen organisaties en in de privésfeer. Hoewel draadloze telefonie via C2000, GSM of DECT ook vertrouwelijkheidsrisico's kent, adresseert dit beschouwingsmodel alleen draadloze datanetwerken.



Draadloze netwerken voor een organisatie

Probleem

Nu draadloze netwerken steeds meer een 'vast' onderdeel worden van de IT-infrastructuur van organisaties, wordt het ontwerp, de juiste implementatie en het beheer van deze netwerken inclusief de mobiele clients steeds belangrijker en stelt hoge eisen aan infrastructuur, beveiligingsfuncties, administraties, beveiligingsbeleid en het handhaven daarvan. Mobiele apparaten zijn de nieuwe netwerkperimeters geworden, met een beperkte robuustheid en beheerbaarheid.

De belangrijkste problemen bij draadloze netwerken- en mobiele apparaten als PDA's zijn:

1. **Inbreukgevoeligheid** van draadloze netwerken, waardoor risico's van beschikbaarheid, vertrouwelijkheid en integriteit van de communicatie.
2. **Beperkte opslagbeveiliging** van mobiele apparaten. De gegevens worden niet standaard beveiligd opgeslagen. Gevolg: risico's voor de vertrouwelijkheid en 'lekkage' van gevoelige gegevens.
3. **Beperkte zonering**. In hetzelfde mobiele apparaat kunnen meerdere mobiele netwerken actief zijn, waardoor als gevolg van gebrekkige zoneringsmogelijkheden in het apparaat risico's optreden van het lekken van gevoelige gegevens.
4. **Beperkte authenticatie** van PDA's en smartphones. De mogelijkheden hiervoor blijven achter bij authenticatie van laptops, waardoor risico's ontstaan van vertrouwelijkheid van gevoelige gegevens.
5. **Variabele bandbreedte** en locatieafhankelijkheid van communicatiemogelijkheden, met als gevolg beschikbaarheidsrisico's van bedrijfsfuncties.
6. **Draait in 'one user content'.** Het operating systeem van mobiele apparaten als PDA's en smartphones is gemaakt voor exclusief gebruik van slechts één eindgebruiker.

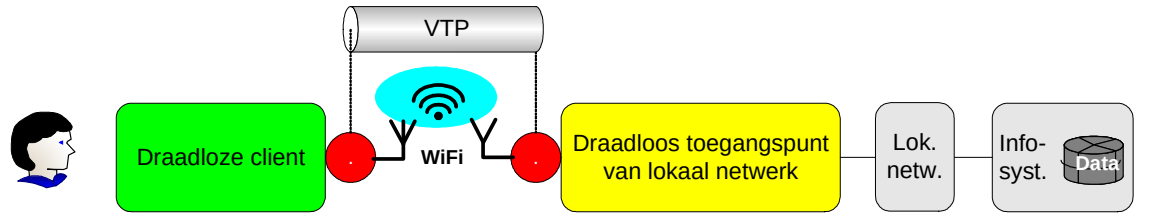
Oplossing

Lokaal datanetwerk: Wi-Fi

Oplossing probleem 1, *Inbreukgevoeligheid* is traditioneel het belangrijkste probleem van draadloze lokale netwerken, maar omdat er steeds betere netwerkprotocollen worden ontwikkeld zoals WPA 2, verschuift de urgentie van onze aandacht naar oplossingen van de inherente risico's van het mobile apparaat zelf. De inbreukgevoeligheid en de mogelijkheden voor aftappen van het draadloze netwerk wordt gereduceerd door versleuteling van de communicatie en het up to date houden van firmware. Het aldus verkregen afgeschermd communicatiepad van client naar draadloos toegangspunt noemen we een *Vertrouwd Toegangspad* (VTP).

Om afluisteren zo veel mogelijk te voorkomen, wordt het netwerk zodanig ingedeeld, dat er zo weinig mogelijk straling buiten de *fysiek beveiligde zone* van een organisatie terecht komt. Richtantennes en ontwerptools voor de fysieke netwerktopologie helpen daarbij.

Soms is die zone gesitueerd een bepaalde ruimte in een gebouw, dat b.v. met meerdere organisaties wordt gedeeld, maar soms omvat de zone een hele campus. Met behulp van speciale beheertools is het stralingsdiagram van Wi-Fi netwerken nauwkeurig vast te stellen.
De beschikbaarheid wordt gegarandeerd door te zorgen dat er geen *dode* plekken in het stralingsdiagram van Wi-Fi netwerken voorkomen en dat het netwerk qua nuttige bandbreedte geografisch zo goed mogelijk is afgestemd op het gebruik binnen de organisatie.



Functieblokken van een Wi-Fi draadloos netwerk

Functieblok	Continuïteit	Zonering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Alarmering	Systeem integriteit
Draadloze client	nvt	-Beginpunt VTP -Encryptie data -Virus- en malware scanning	-2-factor PIN + Wachtw. -2-zijdig, afhankelijk van opzet VTP	Netwerkautorisatie	Conform beschouwings-model Werkplek	Handhaven van IB-functionaliteit	Firmware patches
Draadloos netwerk	-Overlapping stralingsdiagram -Meerdere kanalen bruikbaar	-802.11x encryptie -Straling afschermen voor externe zone	802.11x - authent.	nvt	nvt	nvt	-Hardening -Codescan patch -NOS-patches
Draadloos toegangspunt lokaal netwerk	-Fail-over van toegangspunten -Geen SPOF -Tijdsynchronisatie	-Eindpunt VTP -Ecryptie data -VPN	2-zijdig, afhankelijk van opzet VTP	Netwerkautorisatie	Conform beschouwings-model Server	Alarmering beschikbaarheid en systeemfuncties	-Hardening -Firmware patches

IB-functie

IB-mechanismen

Maatregelen per functieblok voor Wi-Fi netwerken

Oplossing probleem 2; *Beperkte opslagbeveiliging* van data op PDA's of Smartphones wordt opgelost door ingebouwde beveiligingsmogelijkheden van het apparaat die niet door de gebruiker uit zijn te schakelen, zodat bij verlies of diefstal van het apparaat de opgeslagen informatie niet in de handen van onbevoegden kan komen. Aanvullende *applicaties* installeren voor versleuteling van data en het kunnen wissen van de data op afstand (remote wipe).

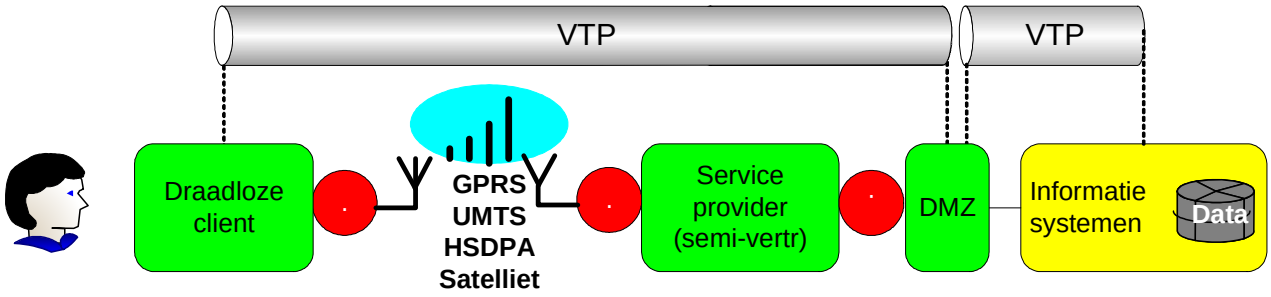
Oplossing probleem 3; *Beperkte zonering* is enerzijds op te lossen door houding en gedrag van de gebruiker als het gaat om installatie van (illegale) of overbodige software op de PDA/Smartphone of laptops. *Hardening* wordt toegepast door verwijdering van overbodige functionaliteit. Scanning op malware helpt om de beperkingen van de mobiele client te compenseren.

Oplossing probleem 4; *Beperkte authenticatie* is op te lossen door productselectie van apparaten die over degelijke ingebouwde authenticatiemogelijkheden bezitten en/of het apparaat op Vertrouwd Toegangs Pad (VTP) - niveau zich te laten authenticeren aan het bedrijfsnetwerk. Bij Wi-Fi wordt het beoogde VTP opgelost binnen de 801.11 standaard. Voor apparaten die tevens gebruikt worden voor publieke netwerken wordt het VTP op een hoger niveau opgelost, zoals sommige smartphone leveranciers standaard aanbieden.

Oplossing probleem 5; *Variabele bandbreedte*. Oorzaken hiervan bij Wi-Fi bedrijfsnetwerken zijn: (1) een *variabele veldsterkte* van het RF signaal zijn óf (2) dat er *teveel gebruikers* via één aansluitpunt de verbinding met het bedrijfsnetwerk gebruiken. (1) is op te lossen door de *topologie* van het netwerk te verbeteren. De stralingsdiagrammen moeten elkaar bij voorkeur overlappen zodat er geen 'dode gebieden' in de netwerktopologie ontstaan. (2) is te verbeteren door gebruikers fysiek te verplaatsen óf door meer aansluitpunten te activeren in een bepaalde ruimte. De performance en beschikbaarheid van het draadloze netwerk kan wat dit probleem betreft verbeterd worden door applicaties zodanig te ontwerpen of in te kopen, dat korte (een te bepalen time-out) onderbrekingen in de communicatie geen verstoring oplevert in het gebruik van de applicatie.

Publiek draadloos datanetwerk: UMTS etc.

Oplossing probleem 1: *Inbreukgevoeligheid* is bij de moderne publieke mobiele netwerken niet echt een issue, omdat de protocollen volwassen zijn en de communicatie standaard versleuteld is. Het zwakste punt ligt voor dit probleem bij de draadloze client zelf. Trojaanse paarden en andere malware kunnen voor de hacker toch mogelijkheden bieden om direct dan wel indirect de verkeersstroom af te luisteren. Alle in de figuur geschetste beveiligingsfuncties van de client moeten worden ingezet om dit probleem te voorkomen. De zone van de serviceprovider wordt als semi-vertrouwd beschouwd, maar valt verder buiten de scope van de probleemstelling.



Functieblokken van toegang tot informatiesystemen via een publiek draadloos netwerk

Functieblok	Continuïteit	Zonering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Alarmering	Systeem integriteit
Draadloze client	nvt	-Beginpunt VTP -Encryptie data -VPN	2-factor	nvt	Conform beschouwingsmod. Werkplek	Handhaven van IB-functionaliteit	-Hardening -OS-patches
Draadloos netwerk	Twee technieken; UMTS/HSDPA primair en Satelliet als uitwijkverbinding	Enbedded encryptie	Enbedded authenticatie	Enbedded autorisatie	nvt	nvt	-Hardening -Code scan van NOS-patches
DMZ (koppelvlak semi vertrouwd)	-Dubbele kanalen -Load balancing	-VTP eind/begin -Reversed proxy -Pakket/Appl insp. -NAT	VPN afhankelijk	nvt	Afwijkend communicatie gedrag	-Netwerk IDS -Overschrijding drempelwaarden -Handhaven IB-functionaliteit	-Hardening, -Patches
Informatie systeem	nvt	VTP eindpunt	Gebruikers authenticatie	nvt	Conform beschouwingsmod. Server	Conform beschouwingsmod. Server	-Hardening, -Firmware patches -Stand. protocol ondersteuning

IB-functies

IB-mechanismen

Maatregelen per functieblok voor publieke draadloze netwerken

Oplossing probleem 2 en 3: *Beperkte opslagbeveiliging* en Beperkte zonering verschillen wat betreft de oplossing niet van Wi-Fi gebruik. (zie hierboven)

Oplossing probleem 4: *Beperkte authenticatie* is op te lossen door productselectie van apparaten die over een degelijke ingebouwde authenticatiemogelijkheden bezitten en tevens door op VTP- niveau het apparaat zich te laten authenticeren aan het bedrijfsnetwerk. Merk op dat het VTP bij publieke netwerken vanaf de client helemaal doorloopt tot aan de vertrouwde zone van een organisatie, met een inspectieonderbreking in de DMZ. Zie hiervoor het patroon: Koppelvlak Semi-vertrouwde derden.

Het VTP wordt bij voorkeur op een zo hoog mogelijk niveau opgelost, zodat het transparant kan zijn voor de Service Provider en de technische infrastructuur van de organisatie. 2-factor authenticatie wordt hierbij een standaard maatregel. Dit kan via internet naar het bedrijfsnetwerk en met behulp van een token, waarbij men minder onafhankelijk is van het mobiele apparaat en het type netwerk. Voorwaarde is wel dat bedrijfsapplicaties ook op deze wijze ontsloten kunnen worden.

Oplossing probleem 5: *Variabele bandbreedte*. In het publieke domein is de oorzaak: variabele dekking alleen door de service provider op te lossen. De bedrijfscontinuïteit kan wat dit probleem betreft verbeterd worden door applicaties zodanig te ontwerpen of in te kopen, dat korte (een te bepalen time-out) onderbrekingen in de communicatie geen verstoring opleveren in het gebruik van de applicatie.

Oplossing probleem 6: *Draait in 'one user content'* wordt procedureel opgelost. Mobiele apparaten worden voor strikt persoonlijk gebruik uitgereikt en als zodanig ingezet in het bedrijfsproces.

Afwegingen

Mobiele datacommunicatie is een relatief jonge technologie die nog volop in ontwikkeling is met evidente kwetsbaarheden. De kwetsbaarheden in de beveiliging van de communicatieketen worden voor het belangrijkste deel veroorzaakt door de beperkte (ingebouwde) mogelijkheden van het mobiele apparaat, de PDA, Smartphone, tablet of Laptop + Dongle.

De inherent grotere kwetsbaarheid van mobiele datacommunicatie als geheel moet bewust afgewogen worden tegen de gevoeligheid van de 'draadloos' open te stellen bedrijfsinformatie. M.a.w. gebruiken we mobiele datacommunicatie uitsluitend voor mail verkeer, sociale media en scherminformatie óf ook voor uitwisselen van bestanden? Met de komst van tablets, uitgevoerd met Wi-Fi of HSDPA modules lijkt deze vraag alweer een gepasseerd station, maar afdoende beveiligingsmaatregelen ontbreken nog steeds, waardoor de vraag welke informatie je draadloos wilt uitwisselen onverkort actueel blijft.

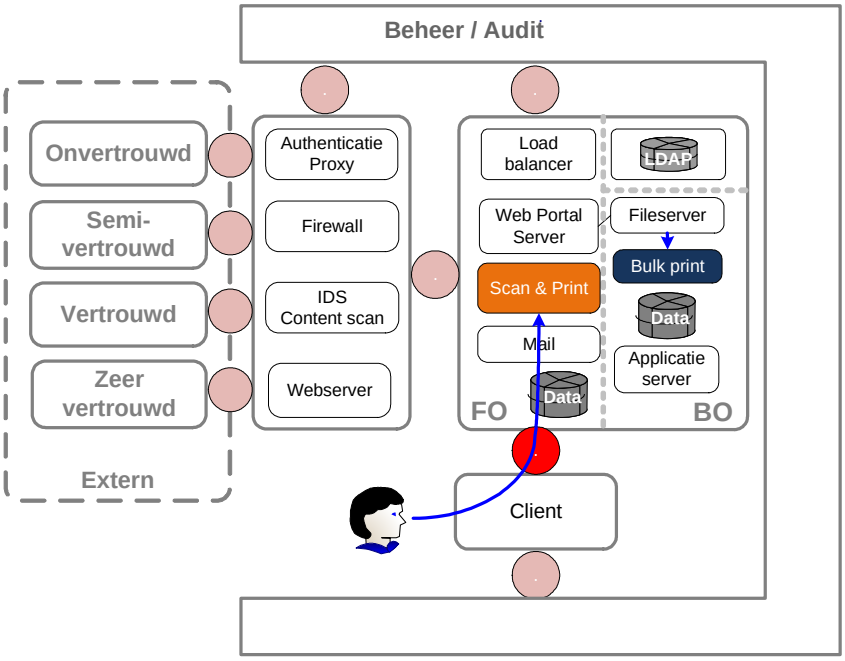
Gerelateerde patronen

- Beschouwingsmodel Client
- Vertrouwd Toegangs Pad (VTP)
- Beschouwingsmodel Netwerk
- Beschouwingsmodel Server

7. Printer

Context

Overal in de organisatie waar documenten worden afgedrukt of ge(re)produceerd komen printers voor. Netwerkprinters worden vaak gecombineerd met kopieermachines, als z.g. *multifunctionals*. Deze apparaten kunnen zowel documenten printen, scannen, mailen en reproduceren van een hardcopy. Naast het 'personal printing' wordt er in organisaties ook grootschalig geprint, bijvoorbeeld voor het afdrukken van formulieren, brochures, rekeningen bankafschriften en voorbedrukte salarisstroken.



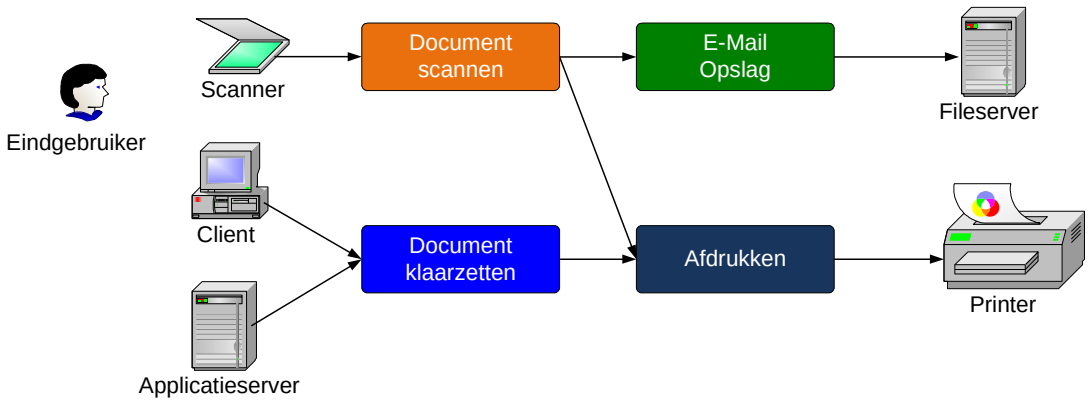
Omgeving van printfuncties

Probleem

Printers zijn door eindgebruikers op verschillende manieren te benaderen, zowel fysiek als logisch. Langs die weg is de input en de output van printers in te zien en te manipuleren.

Oplossing

De printfunctie kent in bedrijven twee ketens: een scanketen en een printketen. De beveiliging van client, servers en netwerken is beschreven in de desbetreffende beschouwingsmodellen.



Functieblokken van een printerketen

De functie "Document klaarzetten" maakt applicatief onderdeel uit van de document aanleverende toepassing, waar gegevensrelevante invoer-, uitvoer en verwerkingscontroles plaatsvinden.

Functieblok	Continuïteit	Zonering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Controleren Alarmeren	Systeem integriteit
Document scannen	nvt	Logische scheiding	Systeem wachtwoord	nvt	Syslog	-Drempelwaarde	-Hardening -Patches
E-Mail Opslag	nvt	nvt	Systeem wachtwoord	Minimaliseren rechten	-Vollopen buffers -IB-events	-Drempelwaarde	-Hardening -Patches
Document klaarzetten	nvt	Ongebruikte poorten zijn uitgeschakeld of verwijderd	Via OS van werkstation	-Gebruikers autorisatie -Systeem-autorisatie	Syslog: -Printopdracht -IB-events -Buffers	-Drempelwaarde	nvt
Afdrukken	-Dubbele papiercassette -Reservedelen	Fysieke afscherming van werkstations	-Pincode -Token	Fysieke sleutel	Sylog: -Printerstatus -Temperatuur -Defecten	-Printerstatus -Bufferoverflow -Papierbak leeg	-Hardening -Patches

IB-Functies

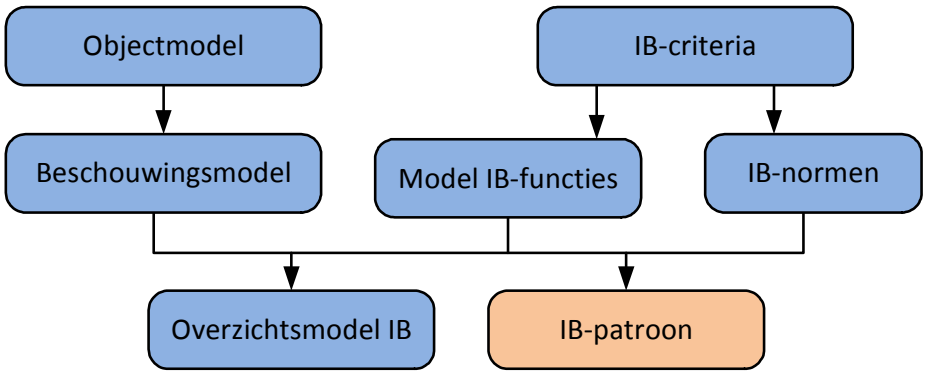
IB- mechanismen

Maatregelen per functieblok voor printerketens

DEEL 2: PATRONEN

Context

Een patroon maakt onderdeel uit van de *NORA aanpak voor IB-architectuur*, zoals hieronder is aangegeven.



NORA aanpak IB-architectuur

Een IB-patroon, als onderdeel van de IB-architectuur is een standaard beschrijving van een probleem en oplossing binnen een bepaalde context, met als doel dat de oplossing algemener inzetbaar wordt. Patronen zijn te beschouwen als *bouwstenen* op architectuurniveau.

Patronen in thema's

Dit document beschrijft patronen in een viertal thema's zoals hieronder is aangegeven. De doelstelling van elk thema is onderin het overzicht cursief aangegeven.

Deel 2. Thema's en patronen	
Koppelvlakken 8. Themapatroon Koppelvlakken 9. Externe koppelvlakken 10. Interne koppelvlakken voor de productieomgeving 11. Interne koppelvlakken voor de ontwikkelomgeving 12. Interne koppelvlakken met beheer en audit 13. Koppelnetwerken met vertrouwde organisaties *Beschrijft gecontroleerde doorgang tussen de zones*	**Logische toegang** 14. Thema Identity & Access Management (IAM) 15. Identity Management (IdM) 16. Access Management (AM) 17. Federated Identity & Access Management 18. Single Sign-On /Single Sign-Off (SSO) 19. Portaal - toegang server 20. Vertrouwd toegangspad (VTP) *Beschrijft vertrouwde toegang tot infrastructuur en applicaties*
Encryptie 21. Themapatroon Encryptie 22. Symmetrische encryptie 23. Public Key Infrastructure (PKI) 24. Elektronische handtekening 25. Sleutelhuis 26. Secure Email *Beschrijft de borging van vertrouwelijkheid en integriteit van gegevens*	**Logging, Monitoring en Continuïteit** 27. Logging 28. Security Information Event Management (SIEM) 29. Themapatroon Bedrijfscontinuïteit (BCM) 30. Backup & Restore strategie 31. Disaster Recovery 32. Uitbesteding IT-diensten *Beschrijft vastlegging en controle van gebeurtenissen en maatregelen voor bedrijfscontinuïteit*

8. Thema Koppelvlakken

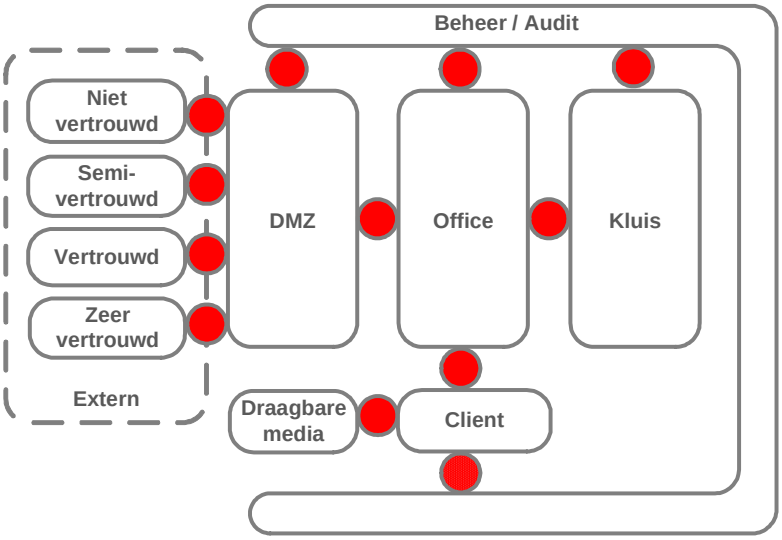
Leeswijzer
Dit is een **themapatroon**, dat voor de algemene probleemstelling van koppelvakken een oplossing biedt. Onderliggende patronen bieden oplossingen voor specifieke soorten van koppelvlakken. Dit themapatroon geeft voor alle koppelvlakpatronen aan welke IB-criteria van toepassing zijn.

Criteria

Beschikbaarheid, Integriteit, Vertrouwelijkheid

Context

Overal waar digitale gegevens via netwerken worden uitgewisseld, zijn koppelpunten nodig. Deze koppelpunten zijn enerzijds bedoeld om een *gecontroleerde doorgang* mogelijk te maken van het ene netwerk naar het andere en anderzijds om de netwerken ten opzichte van elkaar *af te schermen* of om verantwoordelijkheidsgebieden af te bakenen. Deze koppelpunten noemen we koppelvlakken. Het meest bekende koppelvlak is de aansluiting van de vertrouwde (privé) omgeving van een PC-werkstation aan het niet vertrouwde (publieke) internet. In het zoneringsmodel zijn de koppelvlakken tussen de zones als rode bollen gemarkeerd. Ook volgens de *Jericho Forum Commandments* voor toekomstige 'open netwerken', zijn koppelvlakken nog steeds noodzakelijk, alleen dan worden ze geïntegreerd in de beveiliging van elk aangesloten werkstation of hostsysteem.



De omgeving van koppelvlakken

Dit patroon beschrijft koppelvlakken als thema. In de onderliggende patronen worden de verschillende soorten van koppelvlakken besproken, inclusief de belangrijkste verkeersstromen.

Probleem

Binnen een zone kan data vrijelijk tussen systemen worden uitgewisseld. Wanneer echter uitwisseling tussen twee of meer zones nodig is, dan moet ergens een 'opening' worden gemaakt in de afscherming van de zones en dient er voor één of meerdere netwerkprotocollen een doorgang te worden gemaakt. Het *openbreken* van zones en rechtsreeks koppelen en uitwisselen van informatie introduceert een scala aan problemen, die beveiligingsrisico's kunnen veroorzaken:

Samengevat zijn de *generieke* problemen van koppelvlakken:

1. Het ***verschil in vertrouwensniveau van de zones vervalt*** bij een rechtstreekse (netwerk) koppeling, waardoor het effectieve vertrouwensniveau gelijk is aan het laagste vertrouwensniveau van alle gekoppelde zones. Daardoor kan de vertrouwelijkheid van de informatie in zones met een oorspronkelijk hoger vertrouwensniveau niet meer worden gewaarborgd.
2. Rechtstreekse koppelingen van zones impliceert dat de individuele zones samengevoegd worden tot één logische zone. Daarbij ***vervalt de scheiding van verantwoordelijkheden*** voor de beveiliging binnen de individuele zones.

3. Met een rechtstreekse (netwerk)koppeling is er ***geen controle*** op- of beheersing mogelijk van de *integriteit*-, *validiteit*- of *classificatie* van de uitgewisselde gegevens tussen de gekoppelde zones.
4. Met een rechtstreekse netwerkkoppeling kunnen ***ongewenste vormen van communicatie*** zoals DoS[3] aanvallen, pogingen tot inbreuk en poortscans etc. niet worden voorkomen.
5. Informatie kan ***weglekken*** bij de opening die gemaakt is in de zones en onderweg van de ene naar de andere zone.
6. Een koppelvlak is een ***Single Point of Failure***. Wanneer er onverhoopt een storing optreedt in één koppelvlak, dan wordt de hele communicatieketen van zones daardoor negatief beïnvloed.

Niet alle (zes) hiervoor genoemde problemen zijn voor elk koppelvlak op elke locatie in dezelfde mate van toepassing.

Oplossing

Per probleem of groep van problemen zijn de volgende standaard maatregelen van toepassing:

Problemen 1, 2, 3, 4 worden opgelost door uitsluitend informatie-uitwisseling toe te staan voor geautoriseerde netwerk- en communicatieprotocollen. Daarvoor wordt ***filtering*** toegepast, zowel op netwerk als applicatieniveau, dat tevens zorgt voor zonering. Bijvoorbeeld: we laten alleen *http* verkeer door vanaf het niet vertrouwde externe domein.

Problemen 1, 2, 4 worden opgelost door *rechtstreekse* communicatie van een lager naar een hoger vertrouwensniveau te voorkomen. Daarvoor wordt ***zonering*** toegepast op basis van een proxyfunctie. De verbinding wordt onderbroken en vervolgens vanuit de proxy weer opnieuw opgebouwd.

Problemen 1,2,5: worden opgelost door verkeersstromen in twee richtingen te ***versleutelen*** (vertrouwde zone), zodat informatie veilig over een niet vertrouwd netwerk kan gaan.

Probleem 3: wordt opgelost door *in- en uitgaande* gegevens te ***inspecteren*** op virussen, malware en ander vormen van kwaardaardige code en inspectie op inhoudelijke afwijkingen van het beveiligingsbeleid (policy).

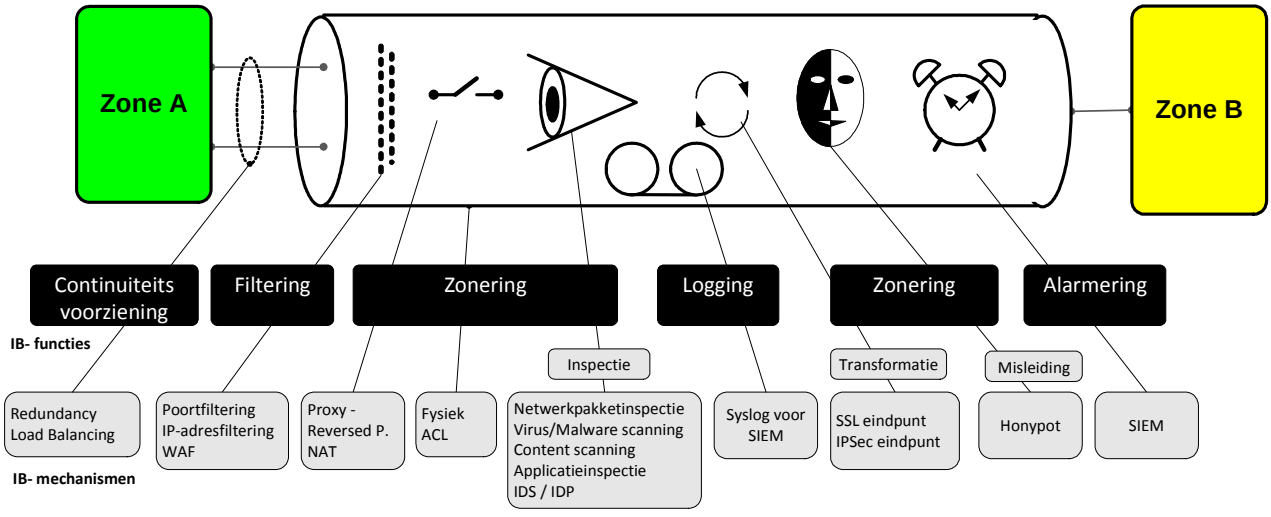
Probleem 4: wordt opgelost door *binnenkomende* communicatie te ***inspecteren*** op afwijkingen van het normale (gewenste) gedrag. Aanvullend worden informatie(systemen) en netwerken op een passieve of actieve manier ***onzichtbaar*** gemaakt voor onbevoegden om hackers te ***misleiden***.

Probleem 5: word opgelost door de koppeling van zone naar zone op te zetten als een ***zeer vertrouwde*** verbinding, waarmee lekkage van informatie vanuit het koppelvlak zelf wordt voorkomen. Het koppelvlak zelf wordt beschouwd als een ‘Beheerzone’ met het bijbehorende vertrouwensniveau.

Probleem 6: wordt opgelost door koppelingen waar nodig ***redundant*** (dubbel) uit te voeren.

Uitgangspunten;

- Het beveiligingsniveaus tussen gekoppelde zones verschilt maximaal één vertrouwensniveau. Uitzondering zijn de koppelvlakken voor beheer en audit.
- Niets wordt doorgelaten tenzij dit is toegestaan.



Betekenis van de symbolen van IB- mechanismen in een ‘kanaal’ weergegeven

De hierboven genoemde maatregelen zijn geïmplementeerd in de basiselementen van een standaard koppelvlak zoals in de figuur in de vorm van een *beveiligd kanaal* is aangegeven.

[3] DoS: Denial of Service attack

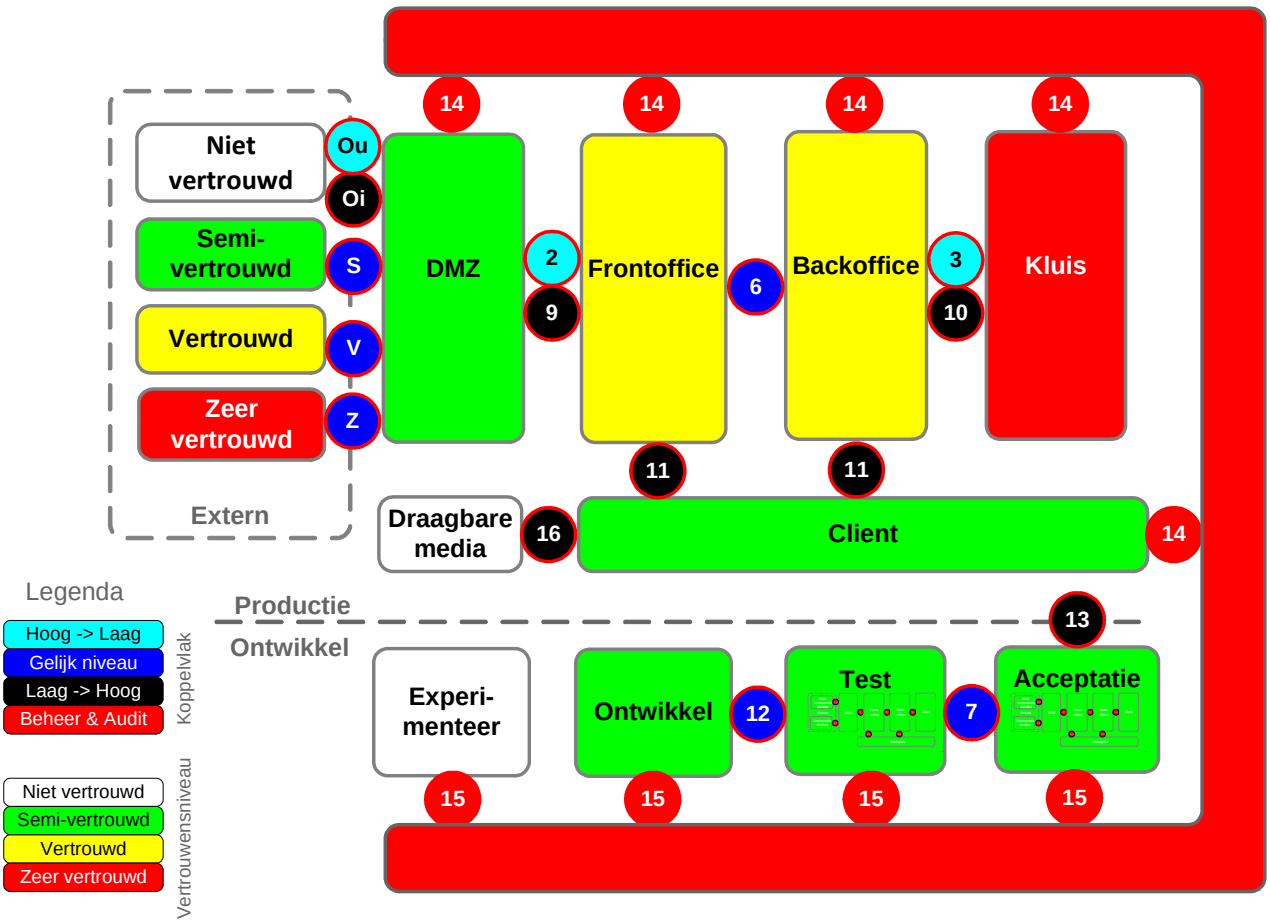
De communicatierichting en het verschil in vertrouwensniveau wat daarbij overbrugd moet worden, is bepalend voor de maatregelen die je neemt in het koppelvlak. Daarom zijn er op een aantal grensvlakken twee koppelvlakken getekend. Voorbeeld: de communicatie via koppelvlakken Ou en Oi gebeurt op hetzelfde grensvlak, maar voor de beveiliging van *binnenkomend* verkeer dat via Oi en DMZ loopt moet veel meer gebeuren dan voor *uitgaand* verkeer dat via de DMZ en Ou verloopt.

Wanneer het verschil in vertrouwensniveau als criterium wordt gesteld voor de rubricering van koppelvlakken, dan zijn er slechts vier fundamenteel verschillende typen koppelvlakken te onderscheiden; namelijk op het grensvlak van communicatie:

- koppeling van een *hoger* naar een *lager* vertrouwensniveau (lichtblauw)
- koppeling tussen *gelijke* vertrouwensniveaus (donker blauw)
- koppeling van een *lager* naar een *hoger* vertrouwensniveau (zwart)
- koppeling vanuit *Beheer-* of *Audit*zone naar andere zones (rood)

Voor de koppelvlakken die *op hetzelfde niveau* in twee richtingen communiceren is slechts één koppelvlak getekend, omdat ze voor wat betreft het vertrouwensniveau bi-directioneel kunnen zijn. Of dat in de praktijk ook zo wordt geconfigureerd hangt af van de situatie. Voorbeeld: vanuit de Acceptatieomgeving zal in de regel niet gecommuniceerd worden naar de Testomgeving, maar wel andersom.

De rode rand om het koppelvlak geeft aan dat het koppelvlak zelf als ‘beheerzone’ is geconstrueerd. De DMZ is een bijzondere zone, die qua grensbescherming niet zinvol los gezien kan worden van de aanpalende koppelvlakken Ou, Oi, S, V, Z, 2 en 9. Daarom bevatten die koppelvlakken in de detailpatronen tevens de relevante IB-functies uit de DMZ.



Koppelvlakken in de infrastructuur van een organisatie

Binnen de zones Test en Acceptatie is de zonering van de organisatie ook weer getekend, omdat daar de zonering van de organisatie wordt gesimuleerd om applicaties en infrastructuur realistisch te kunnen testen.

De koppelvlakmaatregelen zijn in de hierna volgende patronen voor de belangrijkste soorten informatiestromen uitgewerkt:

- Bestandsuitwisseling; file en printservices
- Berichtenverkeer; XML, smtp S/ MIME, ebMS/ MQ/ SOAP
- Webverkeer; http(s) SOAP/ WSDL

Afwegingen

Koppelvlakken kunnen vanuit verschillende criteria worden gerubriceerd. In dit themapatroon inclusief onderliggende koppelvlakpatronen is gekozen voor rubriceren op het verschil in *vertrouwensniveau* aan beide zijden van het koppelvlak, waarbij koppelvlakken voor Beheer en Audit een uitzondering vormen.

Een ander criterium waarmee koppelvlakken kunnen worden gerubriceerd is de beoogde vertrouwensniveaus zelf. Dit levert echter meer varianten op en is minder generiek toepasbaar. Voor de opzet van een koppelvlak is immers niet de ‘absolute waarde’ van het vertrouwensniveau aan weerzijden van het koppelvlak van belang, maar het verschil in vertrouwen dat door het betreffende koppelvlak overbrugd moet worden.

Een belangrijke factor is de *afbakening van verantwoordelijkheden* door het koppelvlak. Een voorbeeld daarvan is de koppeling van de (zeer) vertrouwde partner en de ingang (DMZ) van de eigen organisatie. Beiden hebben ze hetzelfde vertrouwensniveau, maar ze vallen onder de verantwoordelijkheid van verschillende organisaties. Alleen al om die reden impliceert dat aanvullende maatregelen, zoals b.v. virus en malware scanning en screening van de uitgewisselde informatie (applicatie inspectie), tenzij hierover afspraken worden gemaakt.

Het koppelvlak heeft als belangrijke functie het afbakenen van de beheerverantwoordelijkheden. Zonder effectief beheer is beveiliging niet te garanderen.

Het verkeersstroomtype ‘streaming data’ is niet meegenomen in de beschouwing van verkeersstromen, maar kan desgewenst worden toegevoegd in de patronen.

Voorbeelden

- Interne koppelvlakken
- Externe koppelvlakken
- Koppelnetwerken met vertrouwde organisaties

Implicaties

Het waar mogelijk toepassen van ‘standaard’ koppelvlakken en de daaruit volgende reductie van het aantal verschillende koppelingen, impliceert dat organisaties moeten standaardiseren op drie á vier vertrouwensniveaus voor de verschillende zones. De winst daarvan is dat de infrastructuur beter beveiligd kan worden omdat de omvang van complex beheer afneemt.

9. Externe koppelvlakken

Context

Elke organisatie met klantprocessen op basis van elektronische communicatie, heeft één of meerdere koppelingen ingericht met de buitenwereld. Tot enkele jaren geleden waren dat koppelingen, die voor elk informatiesysteem apart werden ingericht. In verband met de toenemende dreigingen, kostenbesparingen en reductie van complexiteit, zoeken organisaties nu steeds meer naar oplossingen in de vorm van één centraal koppelvlak, uitgevoerd als een groep van *kanalen* waarmee de communicatie naar buitenwereld mogelijk worden gemaakt.

Het begrip *kanaal* is hier van toepassing omdat afhankelijk van het type doorgang de beoogde koppeling van de zones als het ware dwars door een aantal zones met koppelvlakken heen loopt.

Probleem

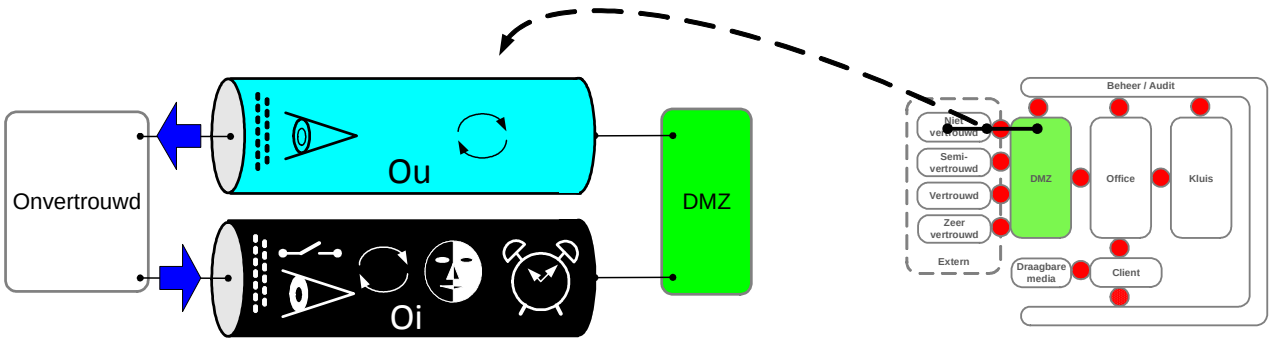
Alle generieke problemen van koppelvlakken zijn benoemd in het themapatroon. De tabel hieronder geeft vanuit die opsomming een overzicht van welke problemen bij welk type kanaal relevant zijn (√).

Voor het kanaal naar *niet vertrouwd* zijn de problemen in belangrijke mate afhankelijk van de *communicatierichting*. De overige kanalen koppelen zones van hetzelfde vertrouwensniveau. In de praktijk verschillen de problemen voor ingaand- en uitgaand verkeer bij koppeling van zones met dezelfde vertrouwensniveau‘s niet zoveel van elkaar, zodat ze in het patroon niet afzonderlijk van elkaar zijn benoemd.

nr	Probleem	Oi	Ou	S	V	Z
1	Bij een rechtstreekse koppeling van zones vervalt het verschil in vertrouwensniveau	√	nvt	nvt	nvt	nvt
2	Bij een rechtstreekse koppeling van zone vervalt scheiding van verantwoordelijkheden	√	√	nvt	nvt	nvt
3	Bij rechtstreekse koppeling van zones is er geen controle mogelijk op integriteit, validiteit, classificatie van gegevensuitwisseling	√	√	√	√	√
4	Bij een rechtstreekse koppeling van zones kunnen ongewenste vormen van communicatie niet worden voorkomen	√	nvt	√	√	√
5	Informatie kan weglekken bij de ‘doorgang’ die gemaakt is tussen de zones	√	√	√	√	√
6	Koppelvlakken zijn single point of failure die de hele keten kunnen beïnvloeden	√	√	√	√	√

Oplossing

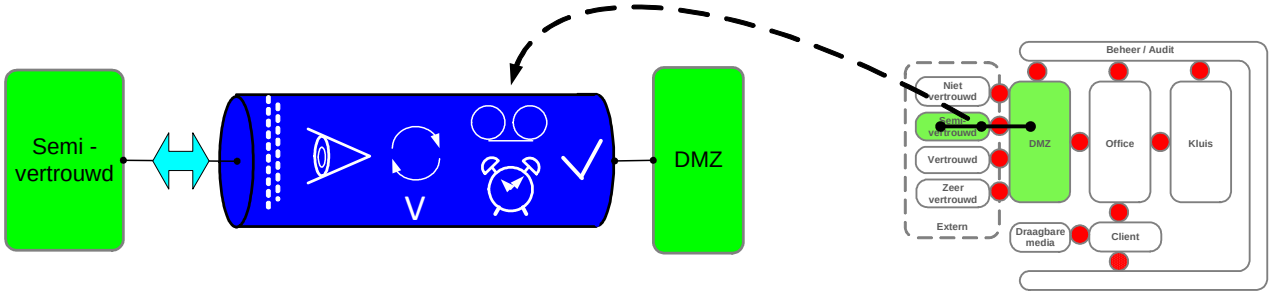
Kanaal naar Niet vertrouwd.
Dit kanaal wordt ingericht met de mechanismen zoals hieronder met symbolen is aangegeven. Zie voor de specificatie van mechanismen per type kanaal de onderstaande tabel. Het lichtblauwe kanaal Ou, dat de communicatie van *binnen naar buiten* mogelijk maakt, bevat o.a. filtering, inspectie op virussen en Network Address Translation (NAT). Het zwarte kanaal van *buiten naar binnen* bevat vrijwel alle denkbare mechanismen voor grensbescherming. De IB-objecten van de mechanismen voor beide kanalen zijn opgesteld in de DMZ.



Kanaal (Ou en Oi) naar een niet vertrouwde zone

Kanaal naar Semi-vertrouwd.
Voor dit kanaal wordt een versleutelde *netwerktunnel* opgezet tussen de *externe* semi-vertrouwde zone en de DMZ, dat zelf ook semi-vertrouwd is. De netwerktunnel kan worden gerealiseerd via zowel publieke- als private netwerken. Dit kanaal wordt met mechanismen ingericht, die werkzaam zijn in beide communicatierichtingen. Voor koppeling met deze semi-vertrouwde zones zijn mechanismen voor misleiding niet nodig. Er bestaat in deze configuratie immers al een bepaalde mate van vertrouwen.

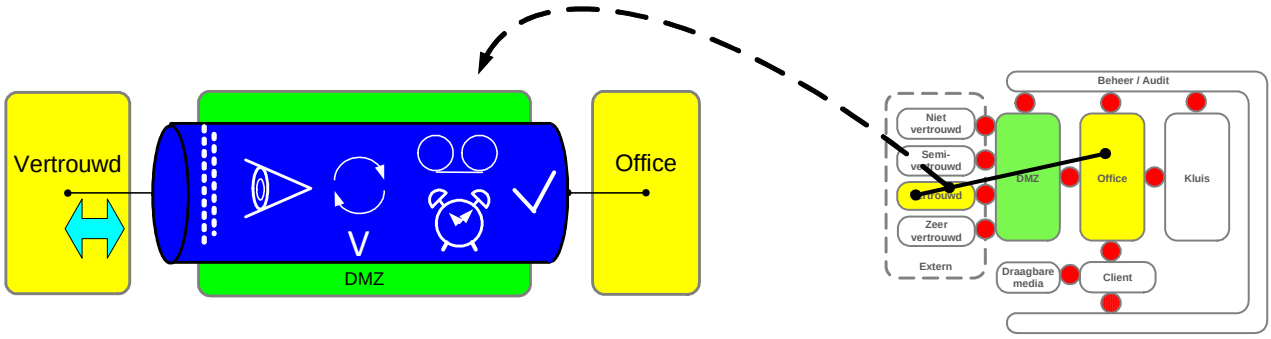
In deze en volgende patronen is steeds één kanaal getekend, omdat we daarin steeds zones koppelen met hetzelfde vertrouwensniveau. De set van benodigde maatregelen in de vorm van IB-mechanismen zijn hierbij grotendeels identiek voor zowel in- als uitgaand verkeer. De IB mechanismen onder verantwoordelijkheid van de eigen organisatie worden in de DMZ gerealiseerd.



Kanaal (S) naar een Semi-vertrouwde zone

Aan de ‘overzijde’ van het kanaal, zal de andere partij doorgaans maatregelen nemen die gelijkwaardig zijn aan die van de eigen organisatie. In het patroon naar niet vertrouwd is gedefinieerd wat er per organisatie nodig is om de *eigen* verantwoordelijkheid te kunnen nemen. Elkaar vertrouwende partijen kunnen afspreken dat men dan wel *minder* of juist *aanvullende* maatregelen neemt op datgene wat in deze patronen is aangegeven.

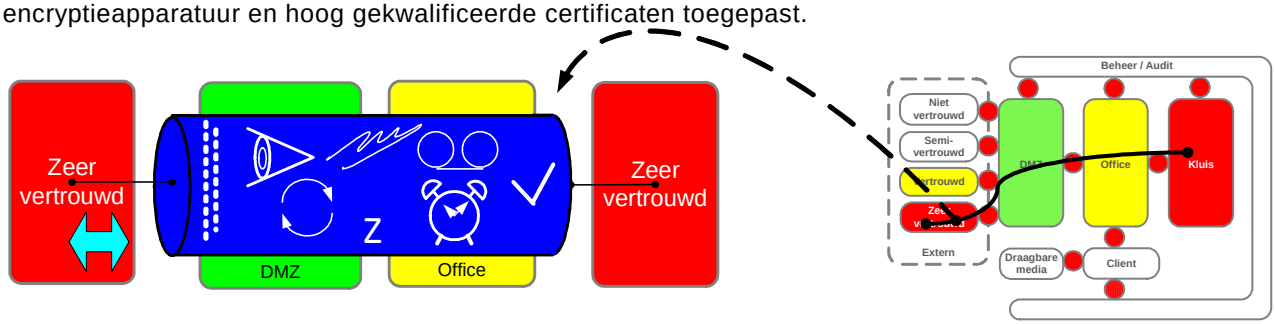
Kanaal naar Vertrouwd.
Voor dit kanaal wordt een versleutelde *netwerktunnel* opgezet tussen de *externe*- en *interne* vertrouwde zone. Dat kunnen zowel vertrouwde zones van *partners* zijn als externe locaties van de organisatie zelf. De netwerktunnel kan zowel via publieke als private netwerken worden gerealiseerd.



Kanaal (V) naar een Vertrouwde zone

De reden om het communicatiekanaal op deze manier af te beelden is dat de IB-mechanismen gedeeltelijk in de DMZ en gedeeltelijk aan het eindpunt zijn gerealiseerd.

Kanaal naar Zeer vertrouwd.
De opzet van dit kanaal heeft veel overeenkomsten met de koppeling van vertrouwde zones, maar bevat extra maatregelen voor het transport van hoog geclassificeerde gegevens. Minimaal is daarvoor nodig: versleuteling van de getransporteerde data, toepassing van private- in plaats van publieke netwerken en afhankelijk van de classificatie van de te transporteren gegevens worden hoog gekwalificeerde encryptieapparatuur en hoog gekwalificeerde certificaten toegepast.



Kanaal (Z) naar een Zeer vertrouwde zone

Het kanaal verbindt een externe, zeer vertrouwde, zone met een intern zeer vertrouwde zone. Dat kan een zone zijn met productiedata, maar ook een beheerzone ten behoeve van een externe beheerserviceprovider.

Onderstaande tabel geeft per IB-functie een overzicht van de toegepaste IB-mechanismen per kanaal.

	Continuïteit	Zonering	Filtering	Onweerlegbaarheid	Vastleggen gebeurtenissen	Alarmering	Systeem integriteit
Ou	Dubbele uitvoering van infrastruct. voorziening	-Proxy (WAF) -Transformatie (NAT) -SSL-/IPSec beginpunt	-Poortfiltering -IP-adresfiltering -Virus/malware scan	nvt	Van policy afwijkend communicatiegedrag	-IB-events -Drempelwaarden -Handhaving IB-funct.	-Hardening -Patches
Oi	- Dubbele uitvoering van infrastruct. voorziening - Load balancing	-Reversed Proxy (WAF) -Pakket- Appl. inspectie -Transformatie (NAT) -SSL-eindpunt -Misleiding (Honypot)	-Geautoriseerde protocollen -Virus/malware/ contentscanning -Poort / IP-adresfiltering	nvt	Van policy afwijkend communicatiegedrag	-Intrusion Detection -IB-events -Drempelwaarden -Handhaving IB-funct.	-Hardening -Patches
S	- Dubbele uitvoering van infrastruct. voorziening - Load balancing	-Reversed Proxy (WAF) -Pakket- Appl. inspectie -Transformatie (NAT) -SSL-/ IPSec eindpunt	-Geautoriseerde protocollen -Virus/malware/ contentscanning -Poort / IP-adresfiltering	nvt	Van policy afwijkend communicatiegedrag	-Intrusion Detection -IB-events -Drempelwaarden -Handhaving IB-funct.	-Hardening -Patches
V	- Dubbele uitvoering van infrastruct. voorziening - Load balancing	-Transformatie (NAT) -IPSec tunnel (VPN) -ACL	-Poortfiltering -IP-adresfiltering -Virus/malware scan	Elektronische handtekening (optioneel)	Van policy afwijkend communicatiegedrag	-Alarm op System-resources en drempelwaarden -Vulnerabilityscan -Handhaving IB-funct.	-Hardening -Patches
Z	Dubbele uitvoering van infrastruct. voorziening	-Transformatie (NAT) -IPSec tunnel (VPN) -Dataencryptie	-Poortfiltering -IP-adresfiltering -Virus/malware scan	Elektronische handtekening	Van policy afwijkend communicatiegedrag	-Alarm op System-resources en drempelwaarden -Vulnerabilityscan -Handhaving IB-funct.	-Hardening -Patches -Hoge klasse certificaat -Hoge klasse encryptie hardware/software

IB-Functies

IB-mechanismen

Maatregelen per extern kanaal

De informatiestromen door de koppelvlakken kunnen in drie hoofdgroepen worden samengevat:
- Bestandsuitwisseling; file en printservices
- Berichtenverkeer; XML, smtp S/MIME, ebMS/ MQ/ SOAP
- Web verkeer; http(s) SOAP/ WSDL

Afwegingen

Kanaal Niet vertrouwd
De koppelvakken van dit kanaal komen in elke organisatie voor en verschillen per situatie.
Dit is het meest complexe en gevoelige koppelvlak van alle koppelvlakken, waardoor een eventuele uitbesteding van dit koppelvlak met de grootste zorg (blijvend) moet worden behandeld. Bepalend daarbij is de gevoeligheid van de bedrijfsprocessen en het kunnen voortbestaan van de organisatie als gegevens onverhoopt lekken naar concurrenten. Globaal gezien worden echter steeds dezelfde maatregelen genomen per verkeersstroom.

Semi-vertrouwd
Er bestaan veel varianten van dit koppelvlak en verschillende redenen om dit type koppelvlak in te zetten. Voor alle varianten geldt dat het vertrouwen in de beveiligingsmaatregelen aan de andere zijde van het kanaal beperkt *is* of *kan zijn*. Voorbeeld daarvan is een mobiele- of telewerker, die buiten het beveiligingsregime van de organisatie werkt met IT-middelen en data. De telewerker beschikt daarom over een *beperkte set van IT-functies*, zoals bijvoorbeeld alleen mail en browsen van het intranet. Andere voorbeelden zijn partners die gegevens uitwisselen of gebruik maken van elkaars IT-functies, maar dat er slechts tot op 'semi-vertrouwd' niveau zekerheid bestaat over de wederzijds genomen maatregelen. Nog een andere reden is een *bewuste scheiding* van *verantwoordelijkheden*. Deze situatie kan zelfs bestaan bij de koppeling van werkmaatschappijen binnen hetzelfde concern, met name wanneer de bedrijfsprocessen duidelijk van elkaar verschillen of wanneer organisaties in een beginstadium van fusie verkeren.

Vertrouwd
Als deze koppeling wordt toegepast, dan moet er een grote mate van vertrouwen bestaan tussen de verbonden organisaties. Ze koppelen immers hun vertrouwde- veelal *productieomgevingen* aan elkaar. In situaties, waarbij SAAS geleverd wordt aan een derde partij, moet worden overwogen of aanvullende maatregelen nodig zijn zoals het inrichten van een gescheiden vertrouwde zone, waarbinnen SAAS-systemen staan opgesteld.

Dit patroon gaat voor de eenvoud van afbeelding uit van verschillende organisaties met een gelijkwaardige dataclassificatie en vertrouwensniveau. Dit is in grote lijnen van toepassing voor veel gelijkwaardige grote organisaties en voor 95% van de overheidsinstanties onderling.

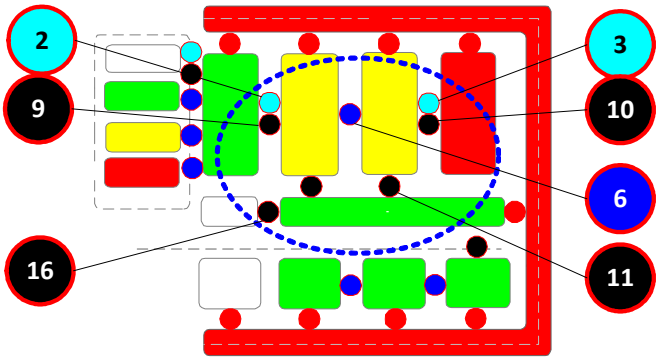
Implicaties

De maatregelen van de kanalen Semi-vertrouwd, Vertrouwd en Zeer Vertrouwd zijn afgestemd tussen de partners en er bestaan zekerheden over de handhaving van het beveiligingsniveau aan beide kanten. Hierover dienen contracten of convenanten te worden gesloten waarin geregeld is dat er een TPM wordt afgegeven door een geregistreerde partij over de naleving van een afgesproken normenset.

10. Interne koppelvlakken voor de productieomgeving

Context

De omgeving van ‘interne koppelvlakken’ is alles wat zich in de *productieomgeving* bevindt. De koppelvlakken van Beheer/Audit horen hier niet bij. Die koppelvlakken worden apart beschreven in een volgend patroon.



Interne koppelvlakken voor de productieomgeving

Probleem

Bedrijfsprocessen moeten met elkaar kunnen communiceren zonder dat ongewenste beïnvloeding de continuïteit van de bedrijfsvoering in gevaar kan brengen.
Problemen samengevat: **1, 2** en **3** (zie probleembeschrijving themapatroon Koppelvlakken)

Oplossing

Voor alle koppelvlakken geeft onderstaande tabel een overzicht van mogelijke maatregelen per intern koppelvlak. Zie verder de figuren in het themapatroon voor de positionering van het koppelvlak.

	Continuïteit	Zonering	Filtering	Vastleggen gebeurtenissen	Alarmering	Systeem integriteit
2	Dubbele netwerk verbinding	-Proxy (WAF) -Pakket- Appl. inspectie -SSL- eindpunt	-Poort / IP-adresfiltering	Van policy afwijkend communicatiegedrag	-Intrusion Detection -IB-events -Drempelwaarden -Handhaving IB-funct.	-Hardening -Patches
3	Dubbele netwerk verbinding	-ACL -VPN	-Poortfiltering	Van policy afwijkend communicatiegedrag	Alarm op afwijkend communicatiegedrag en drempelwaarden	-Hardening -Patches
6	Dubbele netwerkverbinding	-ACL -VPN	-Poortfiltering	Van policy afwijkend communicatiegedrag	Alarm op afwijkend communicatiegedrag en drempelwaarden	-Hardening -Patches
9	- Dubbele uitvoering van infrastructurele voorzieningen - Load balancing	-SSL beginpunt -ACL	-Poortfiltering -IP-adresfiltering	Van policy afwijkend communicatiegedrag	-Intrusion Detection -Alarm op events en drempelwaarden	-Hardening -Patches
10	nvt	-ACL -VPN	-Poortfiltering -IP-adresfiltering	Van policy afwijkend communicatiegedrag	Alarm op afwijkend communicatiegedrag en drempelwaarden	-Hardening -Patches
11	nvt	-ACL -VPN	Port based Network Access Control 802.1x	Van policy afwijkend communicatiegedrag	Alarm op afwijkend communicatiegedrag	-Hardening -Patches
16	nvt	-ACL -Media encryptie	Virus/malware scan	-USB access -Media access	Alarm op afwijkend communicatiegedrag	-Hardening -Patches

IB-Functies

IB-mechanismen

Maatregelen per intern koppelvlak voor productieomgeving

Voor de inrichting van koppelvlak 11 zijn twee oplossingsrichtingen mogelijk:

1. IB-functies inrichten per LAN segment waaraan de clients gekoppeld zijn.
2. IB-functies inrichten voor elke client afzonderlijk.

Koppelvlak 11 ondersteunt de datastromen: *Bestand*, *Bericht* (mail) en *Web* verkeer. Aanvullend moet dit koppelvlak voor de legacy systemen ook terminal verkeer ondersteunen zoals b.v. IBM-3270 of leverancier specifieke Client-Server protocollen. Dit laatste geldt ook voor koppelvlakken 3 en 6.

Koppelvlak 16 omvat de externe (hardware-) interfaces van de client. Dit zijn o.a. USB poorten die beveiligd of uitgeschakeld zijn en centraal worden beheerd. In dit patroon is aangenomen dat de Wi-Fi functie is uitgeschakeld. Wanneer draadloze netwerken gebruikt worden, dan moeten de koppelvlakken 11 en 16 aanvullende IB-functies bevatten om ‘backdoors’ in het bedrijfsnetwerk te voorkomen.

Afwegingen

Welke oplossingsrichting (1 of 2) voor koppelvlak 11 gekozen wordt, hangt af van het aantal clients (1000 clients of meer), de acceptabele beheerlast, en draagbaarheid van licentiekosten voor de objecten die de IB-functies uitvoeren.

Versleuteld bestands- of berichtenverkeer moet voor zover toegepast, worden ondersteund door de koppelvlakken 2, 3, 6, 9, 10 en optioneel ook 11. Hierboven wordt aangenomen dat web services in de DMZ of in de frontoffice zijn gesitueerd.

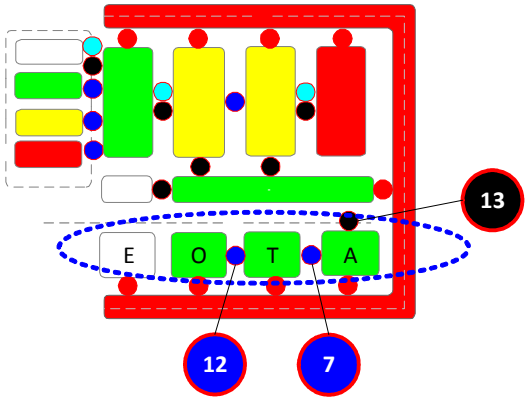
De te nemen maatregelen voor de inrichting van interne koppelvlakken (productieomgeving) zullen vanwege risicoacceptatie per organisatie doorgaans meer verschillen dan het geval is voor externe koppelvlakken. Vaak bestaat er geen zonering van Frontoffice-Backoffice, maar is daar sprake van één vertrouwde zone. In dat geval vervalt koppelvlak 6 en zullen er evenredig meer eisen gesteld worden aan koppelvlak 9.

Koppelvlak 11, die het kantoornetwerk en de netwerksegmenten van de productieomgeving verbindt, is om netwerktechnische redenen zoals performance niet altijd voorzien van beveiligingsfuncties. Omdat een netwerk van eindgebruikers feitelijk als een *semi-vertrouwde* omgeving beschouwd moet worden, heeft het niet beveiligen van koppelvlak 11 zowel impact op de benodigde maatregelen binnen de vertrouwde omgeving van FO/BO als voor de logische toegang tot zeer vertrouwde zones als de Kluis.

11. Interne koppelvlakken voor de ontwikkelomgeving

Context

De *ontwikkelomgeving* is een belangrijk onderdeel van een grote organisatie. Nieuwe IT-services moeten zich enerzijds ongestoord kunnen ontwikkelen, maar binnen de fasen van die ontwikkeling moet ongewenste beïnvloeding worden voorkomen. Ook de transitie van nieuwe functies naar het productiedomein moet gecontroleerd plaatsvinden. Vaak vindt de ontwikkeling van IT-services geheel of gedeeltelijk buiten de organisatie plaats. Zie hiervoor het patroon “Uitbesteding IT-diensten”.



Interne koppelvlakken voor de ontwikkelomgeving

Probleem

Ontwikkeling van bedrijfsprocessen en IT-middelen moet kunnen plaatsvinden zonder ongewenste onderlinge beïnvloeding van de verschillende ontwikkelfasen en verantwoordelijkheden.
In de ontwikkelomgeving gaat die beïnvloeding over de aantasting van de beoogde *Systeemintegriteit*.
Problemen samengevat: **1, 2** en **3** (zie probleembeschrijving themapatroon Koppelvlakken)

Oplossing

Voor alle koppelvlakken geeft onderstaande tabel een overzicht van beoogde maatregelen per intern koppelvlak. Zie verder de figuren in het themapatroon voor de positionering van het koppelvlak.

De experimenteerzone (E) is geïsoleerd opgesteld. Behalve met een beheerfunctie is deze zone niet gekoppeld aan andere zones van de organisatie. De Ontwikkel (O), Test (T) en Acceptatiezone (A) zijn onderling gekoppeld. De verbinding met de productieomgeving is ‘los’ getekend, omdat die verbinding fysiek wel bestaat, maar logisch is ontkoppeld. Grote systemen zoals Mainframes hebben ingebouwde (logische) ontwikkelomgevingen, die qua zonering minimaal aan dezelfde eisen moeten voldoen als van toepassing is op fysiek ingerichte- of logisch ontkoppelde ontwikkelomgevingen.

	Zonering	Filtering	Vastleggen gebeurtenissen	Alarmering	Systeem integriteit
7	VPN	Poort / adresfiltering	Van policy afwijkend communicatiegedrag	-Afwijkend communicatiegedrag -Handhaving IB-funct.	-Hardening -Patches
12	VPN	Poort / adresfiltering	Van policy afwijkend communicatiegedrag	Afwijkend communicatiegedrag	-Hardening -Patches
13	Fysieke overdracht of logische ontkoppeling	Procedurele invulling	Procedurele invulling	Procedurele invulling	-Hardening -Patches -Handhaven IB-funct.

IB-Functies

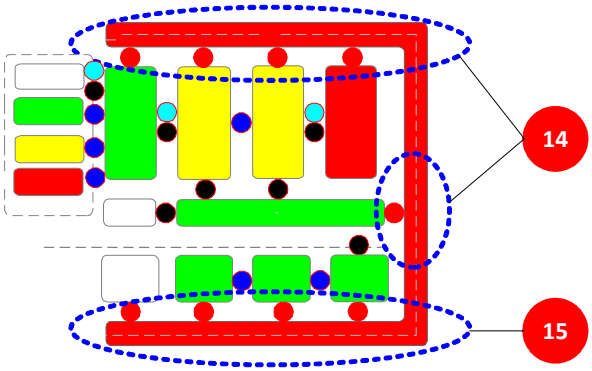
IB-mechanismen

Maatregelen per intern koppelvlak voor ontwikkelomgeving

12. Interne koppelvlakken met beheer en audit

Context

Overal vanuit de infrastructuur moeten koppelingen zijn gemaakt met de beheer- en auditomgeving. Koppelvlakken zijn handmatig of online gekoppeld met het beheerdomein. Zowel in het productie- als het ontwikkeldomein vindt infrastructuurbeheer plaats, maar doorgaans gescheiden van elkaar. Ook bij werkzaamheden voor Beheer en Audit worden functies gescheiden van elkaar uitgevoerd.
Kort samengevat is het beheerkoppelvlak het koppelpunt tussen de handmatige of geautomatiseerde beheerhandeling ‘ergens in het productienetwerk’ en het te beheren doelsysteem. Dit geldt ook voor ontwikkelomgevingen.



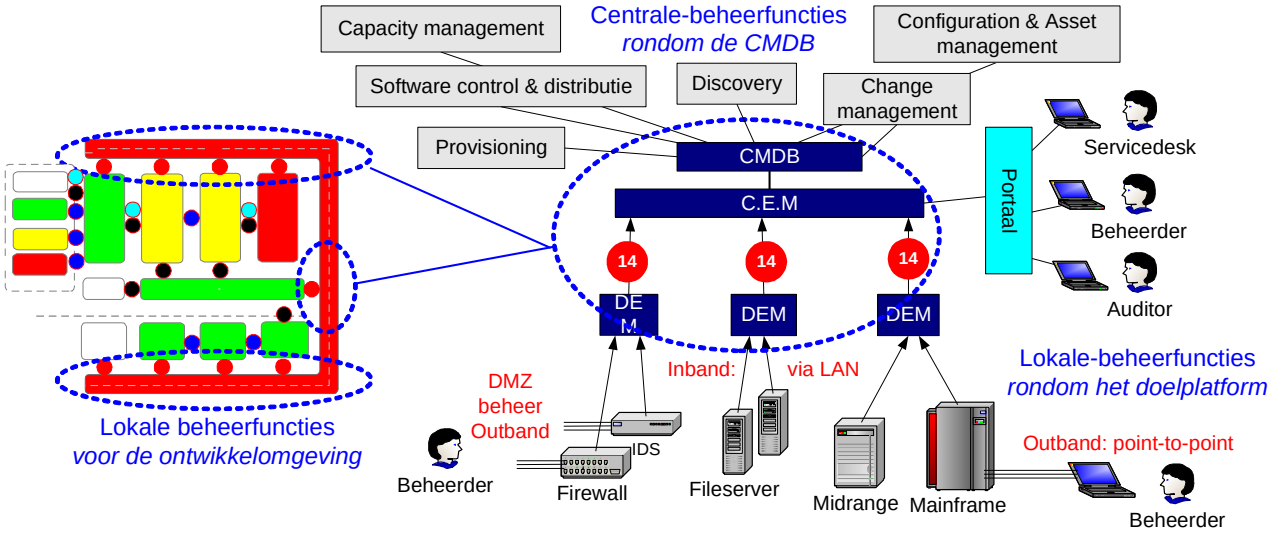
Omgeving beheerkoppelvlakken

Probleem

De belangrijkste koppelvlak gerelateerde problemen die voor infrastructuurbeheer en –audit opgelost moeten worden zijn: **1,2,3 en 5** (zie probleembeschrijving themapatroon Koppelvlakken). Daar komt bij dat audits slechts van waarde zijn wanneer beheerders de verkregen beveiligingsinformatie uit de systemen niet kunnen manipuleren.

Oplossing

De oplossing van dit patroon richt zich met name op Infrastructuurbeheer. De communicatie van de beheerorganisatie met de te beheren platformen kan door ontwikkelingen in de markt in toenemende mate geautomatiseerd plaatsvinden.



Koppelvlakken voor infrastructuurbeheer

Geautomatiseerd configuratiebeheer is noodzakelijk geworden door de complexiteit van IT infrastructuren. De overheid van de VS zet druk op standaardisatie van beheerprotocollen. De beheerkoppelvlakken moeten deze protocollen ondersteunen. Via dezelfde interfaces kan vanuit de IT-infrastructuur zowel beheer- als beveiligingsinformatie worden verzameld door een *Event Manager*, die z’n data doorgeeft aan een rapportagetool, of een *Securitymanagement-datawarehouse*.
Auditors hebben toegang tot deze informatie.

De figuur geeft een voorbeeld van de communicatie van beheer en auditinformatie vanuit de doelsystemen in de zones: DMZ, FO, BO en de Kluis. De Domein Element Manager (DEM) bundelt systeemspecifieke gegevens en stuurt deze naar de Centrale Element Manager (CEM). Een centrale rol in het geheel vervult de Configuratie Management Database (CMDB). Via een portaal op deze database krijgen bevoegde functionarissen toegang tot de betreffende beheerfuncties op de doelsystemen.

De IB-functies in het beheerkoppelvlak 14 zijn van veel factoren afhankelijk, o.a. of beheerders via een *inband* of *outband* netwerkverbinding communiceren. Inband is communiceren via een LAN productiesegment, op basis van TCP/IP waar ook andere systemen op gekoppeld zijn. Outband is een fysiek van het LAN gescheiden, veelal synchrone of asynchrone point-to-point verbinding tussen het beheerwerkstation en het te beheren systeem of centrale beheertool.
Voor outband communicatie is een beveiligd koppelvlak niet nodig. Beheerwerkzaamheden via deze interface worden in de directe nabijheid van het systeem uitgevoerd. Als maatregel resteert dan logging in het doelsysteem (Syslog). Centrale beheersystemen voor meerdere platformen communiceren vrijwel altijd inband. Voor inband communicatie via het LAN gelden de risico's zoals hierboven genoemd. De maatregelen daarvoor zijn samengevat in onderstaande tabel. De meest gebruikte protocollen voor inband communicatie zijn: Simple Network Management (*SNMP*) en Security Content Automation (*SCAP*).
Outband communicatie is leverancier specifiek, op basis van synchrone- of asynchroon communicatie via een bussysteem.

	Continuïteit	Zonering	Filtering	Vastleggen gebeurtenissen	Alarmering	Systeem integriteit
14	Inband + outband koppeling	-Inband koppeling -Outband koppeling -Fysieke scheiding	-Poortfiltering -Geautoriseerde protocollen: -SNMP, SCAP	Vastleggen van communicatiegedrag dat afwijkt van policy	Ongeautoriseerde beheerhandelingen	-Hardening -Patches

IB functies / mechanismen

Maatregelen voor beheerkoppelvlakken

Afwegingen

De beheerzone is geen fysiek- of logisch aaneengesloten zone zoals het zoneringsmodel suggereert. In de praktijk zullen er rond de verschillende platformen, zoals Windows, Midrange en Mainframe beheerclusters gevormd zijn die als gescheiden beheerdomeinen fungeren. Per situatie moet bekeken worden wat voor de afscherming van beheer en productiewerkzaamheden de beste zonering is.
Soms hebben organisaties separate LAN segmenten voor beheerwerkzaamheden ingericht, waarbij de systemen aan de 'achterkant' zijn gekoppeld met het beheernetwerk en aan de 'voorkant' met het productie LAN.
Wanneer een centraal beheerplatform is ingericht zoals geschetst in de bovenstaande figuur, dan bestaat het beheercluster om de systemen heen nog steeds. Het cluster dient in dat geval als 'uitwijk' en voor beheerhandelingen, die (nog) niet ondersteund worden door het centrale platform.

Voorbeelden

In elke organisatie zijn koppelingen gemaakt tussen IT-systemen en beheersystemen.

Implicaties

Beheerinfrastructuur- en -protocollen en beheerinterfaces op doelplatformen zijn in beperkte mate gestandaardiseerd. Organisaties zullen keuzes moeten maken welke risico's het zwaarst wegen voor de doelplatformen en in hoeverre men een strategie kiest voor inrichting van een CMDB.

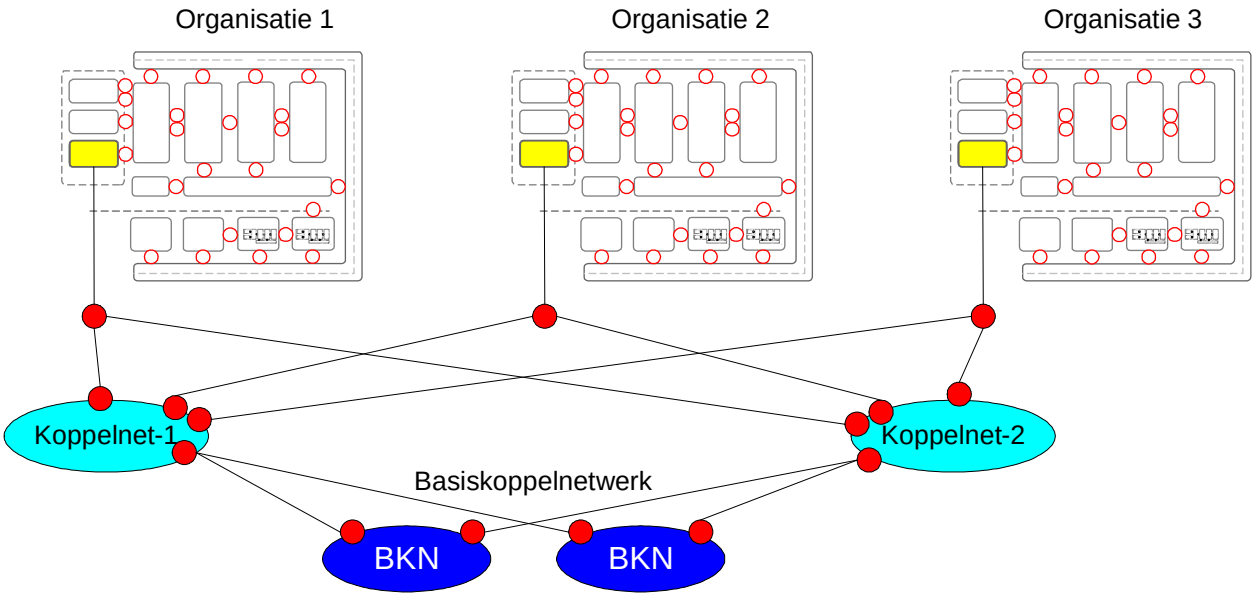
Informatiebeveiliging kan niet zonder *beheer* en voor grote en/of complexe infrastructuren is een actuele CMDB met de daaraan gekoppelde beveiligingsplatformen zoals een SIEM[4] onmisbaar!
Het ontwikkeldomein heeft vanwege functiescheiding bij voorkeur gescheiden beheer ten opzichte van het productiedomein. Voor releasemanagement hebben grote ontwikkelorganisaties een separate CMDB, waardoor het beheer goed is te scheiden.

[4] SIEM: Security Information Event Management; securitymanagement platform

13. Koppelnetwerken met vertrouwde organisaties

Context

Koppelnetwerken zijn voorzieningen waarop verschillende organisaties zijn aangesloten met als doel om te communiceren met andere, veelal tot hetzelfde branche c.q. overheid behorende organisaties via besloten datanetwerken. De aangesloten organisaties kunnen elkaar vertrouwen. Een koppelnetwerk verbindt bedrijfsnetwerken op een betrouwbare, uniforme wijze en kan alleen bestaan op basis van samenwerking en toepassing van een set afspraken waarin de aansluitvoorwaarden en toegestane communicatie beschreven worden. Dit noemen we de *koppelnetstandaard*. Een koppelnetwerk vervult feitelijk een backbone-functie.



Koppelnetwerken

Probleem

Generieke koppelvlakgerelateerde problemen zijn **1, 2** en **6** (zie probleembeschrijving themapatroon). Toegespitst op koppelnetwerken betekent dit:

- Uitval van de koppeling met het centrale koppelnetwerk heeft impact voor een groot aantal organisaties die via het koppelpunt met elkaar communiceren.
- Koppelnetwerken maken veelal gebruik van *Private space* adressen (RFC 1918), waarbij overlappende IP adressen tussen de koppelnetwerken kunnen worden voorkomen. Het risico bestaat dat informatiestromen over de koppelnetten worden verstuurd, die niet voorkomen in de koppelnetstandaard. (*Request For Comments 1918* beschrijft “Address Allocation for Private Internets” en is uitgebracht door de Network Working Group).

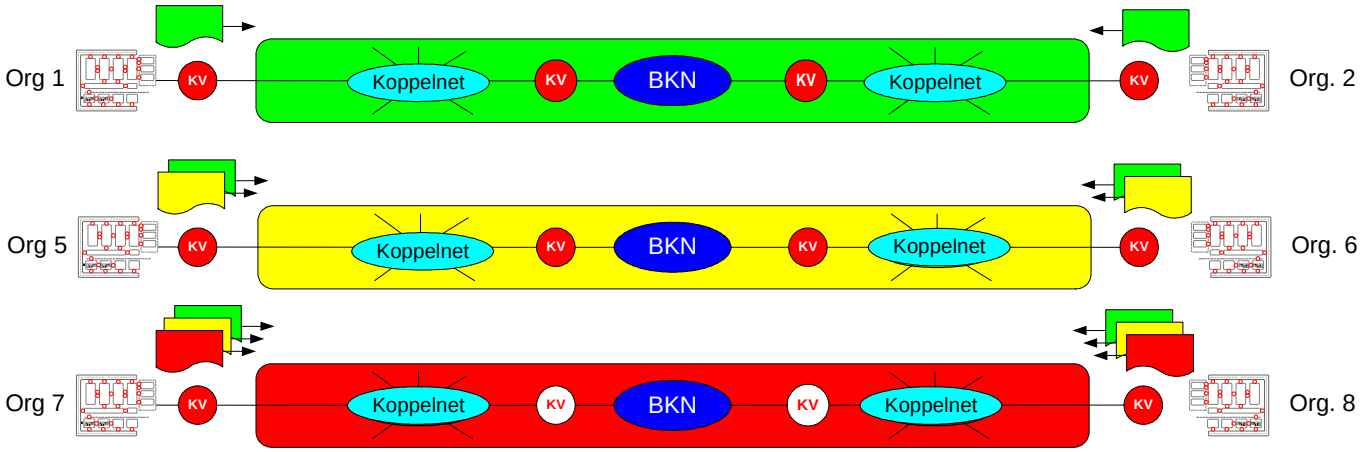
Oplossing

Door het hanteren van een centraal koppelpunt; het basiskoppelnetwerk (BKN), wordt het totale stelsel van koppelingen beheersbaar en worden beheersafspraken tussen de koppelnetwerken gemaakt zoals:

- Beheerders van koppelnetwerken willen binnenkomend verkeer kunnen reguleren, om de continuïteit van het eigen netwerk te kunnen waarborgen.
- Voor informatiestromen gelden per zone verschillende vertrouwensniveaus. Door het verschil in vertrouwensniveau dient niet generiek, maar specifiek te kunnen worden gereguleerd welke verkeersstromen tussen de zones zijn toegestaan.
- Omwille van de continuïteit van de totale keten van informatie-uitwisseling is het van belang de koppelvlakken met een hoge beschikbaarheid uit te voeren. Dit kan op basis van redundantie en automatische omschakeling.

Informatie kan via koppelnetten worden uitgewisseld over meerdere compartimenten of zones. Voor het begrip *compartimentering* wordt in de PvIB patronen het begrip *zonering* gebruikt.
De basis van het koppelnetwerk bestaat daartoe uit een stelsel van drie ‘virtuele’ zones: *Semi-vertrouwd,*

Vertrouwd en Zeer-vertrouwd, waarover de data op hetzelfde niveau kan worden uitgewisseld.
Dit patroon is uitgewerkt voor de drie vertrouwensniveaus, t.b.v. organisaties die betrouwbaar met elkaar willen communiceren op basis van 'any-to-any'.



Vertrouwensniveau 's van koppelnetwerken

Organisatie 1, aangesloten op de zone *Semi-vertrouwd* (groen), mag data versturen met classificatie Laag (groen) wanneer het koppelvlak tussen de organisatie en zones voldoen aan de eisen die in dit patroon en het beleidsdocument van het koppelnetwerk zijn vastgelegd.

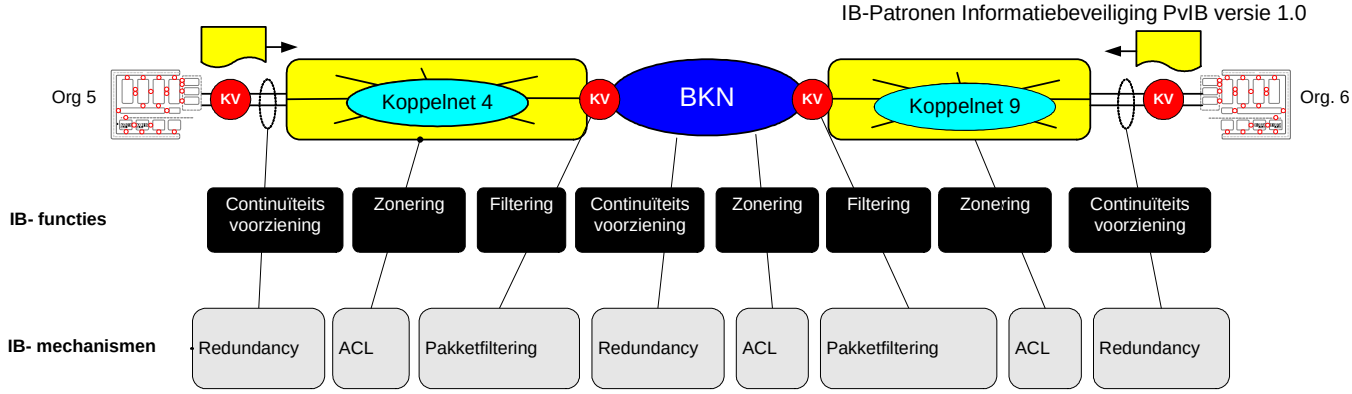
Binnen een zone zijn één of meerdere koppelnetwerken aanwezig, gekoppeld via een koppelvlak aan het Basis Koppelnet (BKN). De koppelvlakken zijn hierna beschreven. Communicatie tussen zones met verschillend beveiligingsniveaus is mogelijk. Hiervoor is grensbewaking op de koppelvlakken tussen de zones met verschillende niveaus nodig.

Niveau zone	Classificatie Gegevens	Koppeling zones	Inspectie & filtering		Verkeer			Opl.
					Web	Bericht	File	
Semi-vetrouwd	Laag	Semi-vertrouwd naar Semi-vertrouwd	-	Pakket filtering	x	-	-	A
Semi-vertrouwd	Laag	Semi-vertrouwd naar Vertrouwd	IDS/IDP	Pakket inspectie	x	-	-	B
Vertrouwd	Laag	Vertrouwd naar Semi-vertrouwd	-	Pakket filtering	x	-	-	A
Vertrouwd	Basis	Vertrouwd naar Vertrouwd	-	Pakket filtering	x	x	x	A
Vertrouwd	Basis	Vertrouwd naar Zeer vertrouwd	IDS/IDP	Pakket inspectie	x	x	x	B
Zeer vertrouwd	Basis	Zeer vertrouwd naar Vertrouwd	-	Pakket filtering	x	x	x	A
Zeer vertrouwd	Hoog	Zeer vertrouwd naar Zeer vertrouwd	-	Pakket filtering	x	x	x	A

Wanneer data van een lagere zone naar een hogere zone wordt gestuurd, dan moet *pakketinspectie* worden uitgevoerd. Wanneer er tussen zones van gelijk niveau of van een hoger naar een lagere zone data gestuurd wordt, volstaat *pakketfiltering*. Voor de onderlinge uitwisseling van *Hoog* geclassificeerde gegevens wordt altijd versleuteling gebruikt, bijvoorbeeld in de combinatie van data encryptie en tunnel encryptie.

<u>Oplossing A: BKN-Koppelnetwerk koppelvlak tussen zones met hetzelfde vertrouwensniveau</u>
Het koppelvlak bevat geen aanvullende beveiligingsmaatregelen voor de integriteit en vertrouwelijkheid van de verstuurde informatie.
De set van maatregelen bestaat samengevat uit:

- Het filteren van inkomende verkeer op basis van poorten, die gebruikt worden door de applicaties die toegestaan zijn op het koppelvlak.
- Het doorlaten van het Koppelnetwerk IP-adresreeksen en het blokkeren van organisatie-intern gebruikte IP adresreeksen.
- Pakketfiltering zorgt er voor dat alleen de toegestane protocollen over het Koppelnetwerk gaan, met uitsluitend Koppelnetwerk-publieke IP-adresreeksen. De reeks dient zo groot mogelijk gekozen te worden om de beheersbaarheid en continuïteit te waarborgen.
- Filtering van binnenkomend verkeer kan worden gereguleerd op basis van Access Control List (ACL) op een router. In het BKN hoeft standaard niet te worden gefilterd. Filtering kan in de koppelnetten worden verzorgd. Het pakketfiltering mechanisme kan per zone worden ingeregeld
- Continuïteit van de totale keten van informatie-uitwisseling wordt gewaarborgd door toepassing van redundantie en automatische omschakeling.

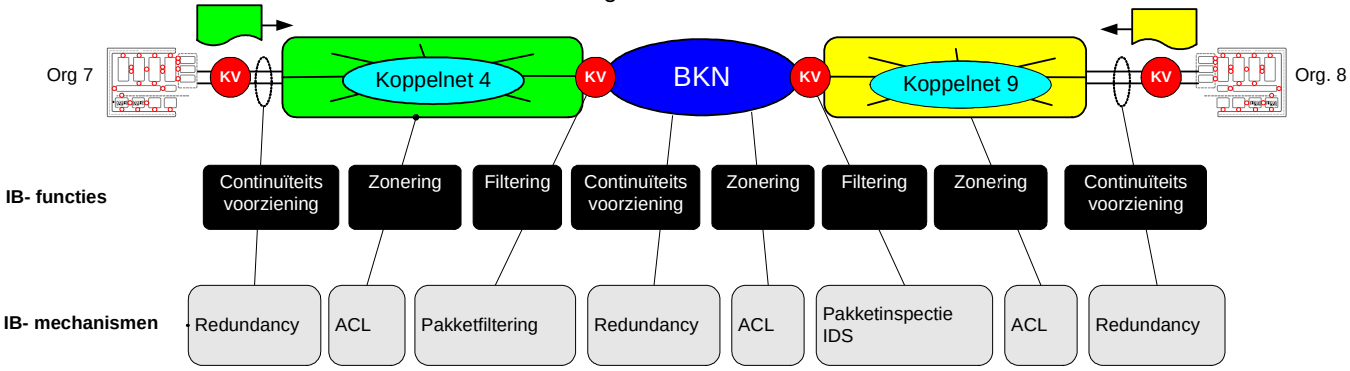


Oplossing A: Koppelvlak tussen zones met hetzelfde vertrouwensniveau

Oplossing B: BKN-Koppelnetwerk koppelvlak tussen zones met verschillende vertrouwensniveaus

Organisaties, aangesloten op een koppelnetwerk, kunnen met elke andere daarop aangesloten organisatie communiceren via besloten datanetwerken. Een voorbeeld daarbij is de rijksoverheid, lokale overheden en organisaties met een publieke taak. De data die wordt uitgewisseld is geclassificeerd als *Basis*. De zones waarover de informatie wordt uitgewisseld hebben in dit voorbeeld *verschillende* vertrouwensniveaus. De volgende mechanismen worden daarvoor ingezet:

- Filtering en continuïteitsvoorzieningen zoals hiervoor genoemd bij oplossing A.
- De filtering op de overgang van een lager naar een hoger beveiligingsniveau wordt uitgevoerd met pakketinspectie.
- Pakket inspectie wordt centraal in het BKN verzorgd.
- In de koppelnetten wordt pakketfiltering toegepast. Pakketfiltering zorgt er voor dat alleen de toegestane protocollen over het koppelnetwerk worden toegestaan met de daarvoor toegestane publieke IP-adresreeks(en). De doorgelaten reeks dient zo groot mogelijk gekozen worden om beheersbaarheid en continuïteit te waarborgen.
- Intrusion Detection (IDS) wordt standaard ingezet voor monitoring van beveiligingsincidenten.
- Continuïteit van de totale keten van informatie-uitwisseling wordt gewaarborgd door toepassing van redundantie en automatische omschakeling.



Oplossing B: Koppelvlak tussen zones met verschillende vertrouwensniveaus

Afwegingen

Bij deze koppelvakken zijn de verschillende type verkeersstromen niet uitgewerkt, omdat het stelsel van beveiligingsfuncties voor koppelnetwerken hiervoor transparant moet zijn. Dat neemt niet weg dat de koppelnetwerken meestal wel een beperkte, afgesproken set van communicatieprotocollen ondersteunen. Die set maakt onderdeel uit van de aansluitvoorwaarden van het koppelnetwerk

Voorbeelden

- Haagse Ring OSB/Diginetwerk; standaard van het College Standaardisatie voor de e-Overheid.
- Gemnet: Besloten overheidsnetwerk voor elektronische diensten en toepassingen
- Suwinet: Elektronische infrastructuur, gebruikt door CWI, UWV en gemeenten krachtens wet SUWI
- OOV Koppelnetwerk voor Openbare Orde en Veiligheid van Politie, Brandweer, Rampenbestrijding en de Geneeskundige Hulpverlening bij Ongevallen en Rampen.

Implicaties

Organisaties moeten (kunnen) voldoen aan de aansluitvoorwaarden van het koppelnetwerk en dienen tevens bereid te zijn tot samenwerking om mogelijk te maken dat het stelsel van netwerken effectief kan functioneren en de overeengekomen specificaties aan de eindpunten gegarandeerd blijven.

14. Thema Identity & Access Management (IAM)

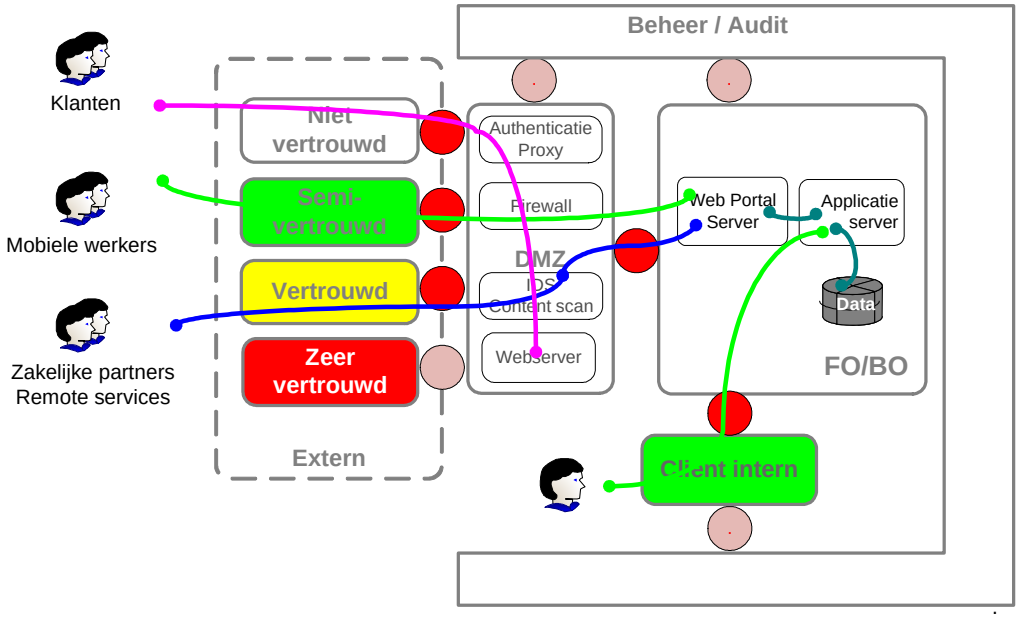
Leeswijzer
Dit **themapatroon**, beschrijft de algemene probleemstelling van Identity & Access Management (IAM) Onderliggende patronen geven de uitwerking van Identity Management (IdM), Access Management (AM) en Federated Identity & Access Management.

Criteria

Integriteit, Vertrouwelijkheid, Controleerbaarheid

Context

Organisaties bezitten een groot aantal gegevens(verzamelingen), diensten en IT-middelen, die waarde vertegenwoordigen. Deze objecten spelen een rol in bedrijfsprocessen of ze zijn producten van bedrijfsprocessen. Een organisatie kent personen zoals medewerkers of klanten die gebruik moeten maken van deze objecten. Organisaties bieden diensten aan voor andere organisaties zoals business partners. Ook zijn er systemen en services die toegang moeten hebben tot de verschillende objecten. Personen, (partner)organisaties en actieve systemen zijn *actoren* en worden in deze context benoemd als *subjecten.* Afhankelijk van de situatie, opereren actieve systemen en services als object óf als subject. In de patronen van het thema IAM ligt de focus op het subject *Persoon*. In de overige patronen voor Logische toegang, zoals Portaal en Vertrouwd Toegangspad ligt de focus op het subject *Systeem*.



Aan personen en systemen wordt toegang verleend tot diensten en gegevens

Probleem

Aan het ontsluiten van gegevens en IT-functies zijn risico's verbonden. Diverse wet- en regelgeving verplichten organisaties om aan te tonen dat men grip heeft op: *"Welke medewerkers (of systemen) hebben toegang tot welke gegevens en welke IT-functies?"*. De problemen zijn als volgt samengevat:

1. **De identiteit van een subject is niet uniek**. Van één bepaald subject zijn vaak meerdere identiteiten binnen een organisatie geregistreerd.
2. **Registratieprocessen bevatten niet alle subjecten** die behoren tot de organisatie.
3. **Samenhang ontbreekt** in registraties van identiteiten en hun toegangsrechten.
4. **Kwaliteit van identiteitsgegevens is ontoereikend.**
5. **Need to know dilemma.** Starre rollenmodellen werken contraproductief.
6. **Definiëren van toegangsrechten is een moeizaam en langdurig proces.**
7. **Management heeft geen overzicht** en inzicht in verstrekte toegangsrechten aan medewerkers.
8. **Autorisatieproces onwerkbaar**, hoge beheerlast en complexiteit door te hoge granulariteit.
9. **Procedures en/of technieken ontbreken** om vast te stellen tot welke gegevens subjecten zich toegang hebben verschaft en in hoeverre dit in strijd is met bedrijfsregels (beleid).
10. **Inspanning** voor handmatige uitvoering van wijzigingen wordt te groot.
11. **Toegangsrechten worden niet ingetrokken** wanneer medewerkers deze voor hun werk niet meer nodig hebben, of wanneer ze de organisatie verlaten.

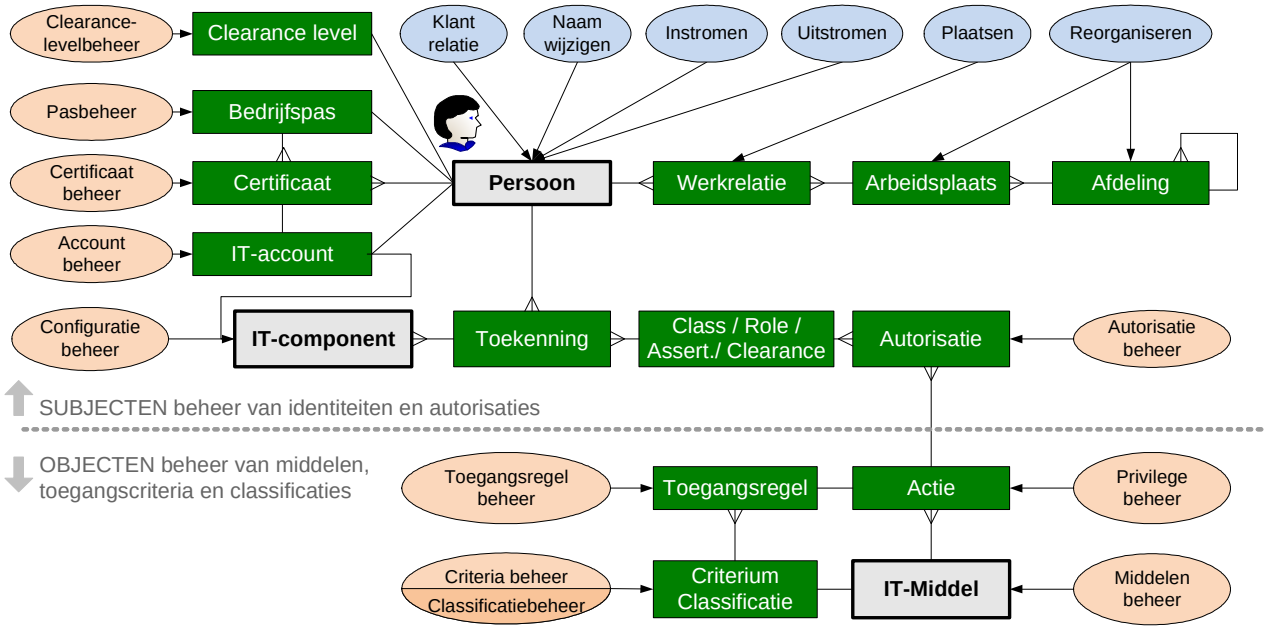
Oplossing

De oplossing van de problemen rond toegangsbeheersing wordt gevonden in een architectuur waarin drie groepen beheerprocessen worden onderscheiden:
1. Beheer van identiteiten van subjecten (Identity Management, IdM);
2. Beheer van toe te wijzen gebruiksrechten op objecten (behorend bij functioneel applicatiebeheer);
3. Beheer van de toegangsrechten / regels voor toegang (Access Management, AM).

Onderstaande figuur schetst IAM beheerprocessen. In het AM patroon is uitgewerkt dat autorisaties op basis van verschillende kenmerken worden verleend. Deze figuur geeft inzicht in de verschillende processen die nodig zijn om subjecten op gecontroleerde wijze toegang te geven tot de middelen (objecten) die zij nodig hebben om hun taak uit te kunnen voeren.

Links en bovenin de figuur staan de processen, die leiden tot te beheren gegevens per entiteit: Clearance, Pasbeheer en Certificaatbeheer zijn optioneel. Niet elke organisatie gebruikt dit. Midden in de figuur staan de autorisatiebeheerprocessen. Onder de stippellijn staat het (functioneel) beheer van objecten en beheer van de toe te wijzen gebruikersrechten op deze objecten.

Rondom de entiteit ‘Actie’ wordt de Access Management functie ‘runtime’, d.w.z. realtime-processing uitgevoerd (door het informatiesysteem).



Beheerprocessen van IAM

De tabel geeft een toelichting op de entiteiten uit bovenstaande figuur op alfabetische volgorde.

Entiteit	Toelichting
Actie	Een handeling die een subject met een middel (object) kan uitvoeren, waarop een autorisatie of toegangsregel van toepassing kan worden verklaard.
Afdeling	Een organisatorische eenheid als onderdeel van de afdelingshiërarchie van een organisatie.
Arbeidsplaats	Een unieke positie binnen en afdeling waarop een persoon kan worden geplaatst c.q. te werk gesteld.
Autorisatie	Een aan een class/ rol/ claim/ clearance verleend recht tot het uitvoeren van een actie op een IT-middel
Bedrijfspas	Het persoonsgebonden identiteitsbewijs van personen die een werkrelatie hebben met de organisatie, voorzien van Public Key certificaten.
Certificaat	Een persoonsgebonden of Server gebonden Public Key – certificaat, dat voor personen geïnstalleerd is op de bedrijfspas of een andere tokenvorm als drager, eventueel gekoppeld aan het IT account fungeert dit als authenticatiemiddel. Voor IT-componenten wordt het certificaat geïnstalleerd in een Hardware Security Module (HSM) of als z.g. ‘software certificaat’ in de systeemprogrammatuur.
Criterium	Een eigenschap die iets of iemand kan bezitten en relevant is voor het definiëren van toegangsregels.
IT-Account	Een persoonsgebonden account waarmee een persoon inlogt op de IT-client of het IT-portaal.
IT-Middel (object)	Een applicatie, fysiek object, service of gegevens, waar de natuurlijke persoon (of IT-component) toegang toe moet hebben om zijn actie uit te kunnen voeren. Middelen beheer wordt buiten de scope van IAM uitgevoerd, voor zowel IT-componenten als voor gegevens.
Persoon (subject)	Een natuurlijke persoon die een formele en geregistreerde werkrelatie heeft met de organisatie

Class / Role Assertion / Clearance	Abstractie, die wordt gehanteerd om samenhangende sets van autorisaties te bundelen en die inzicht verschaft “uit hoofde waarvan” personen, waaraan de class / role / assertion / clearance is toegekend, de desbetreffende autorisatie hebben ontvangen.
Clearance level	Vertrouwensniveau, dat een persoon is toegekend en gelijk is aan het *maximale* classificatieniveau van het te behandelen gegeven of bedrijfsproces: b.v.: *Confidentieel*, *Geheim* of *Zeer geheim*. Het wordt toegekend als resultaat van een veiligheidsonderzoek (AIVD/ MIVD en VOG van gemeente).
IT-component (subject)	Een IT-component is een geregistreerd applicatieproces of onderdeel van de IT- infrastructuur, dat toegang kan worden verleend tot de entiteit IT-Middel.
Toegangsregel	Beschrijft criteria waaronder bepaalde acties op een middel mogen worden uitgevoerd
Toekenning	Koppeling van een rol aan een persoon. Deze koppeling kan gelijk zijn aan de plaatsing van de persoon voor arbeidsplaats gerelateerde rollen, maar hieronder vallen ook de toekenningen van niet-arbeidsplaats gebonden rollen aan personen.
Werkrelatie	Een plaatsing c.q. tewerkstelling van een persoon op een arbeidsplaats binnen de organisatie.

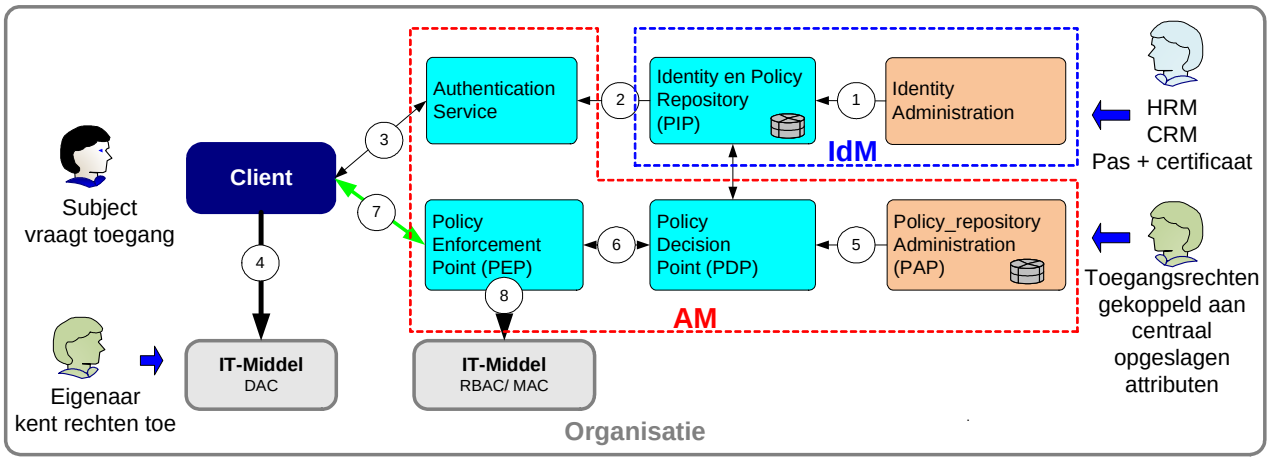
De entiteit *Persoon* kent drie beheerprocessen. Onder de noemer *Instromen* vallen de deelprocessen *Intake,* aanleveren van een *wettelijk identificatie document*, in het kader van de Wet ter voorkoming van Witwassen en Financieren van Terrorisme (WWFT) en uitgifte van een *Personeelsnummer*, als de persoon die nog niet had. De werkrelatie van een persoon op een arbeidsplaats bij de organisatie wordt beheerd middels het proces *Plaatsen*. De entiteit *IT-Component*, is een IT-Middel (m.u.v. gegevens), in de gedaante van een *subject*.

Het proces “Naam wijzigen” is van toepassing als een persoon gaat trouwen of scheiden en is een trigger voor het uitreiken van een nieuwe bedrijfspas met nieuwe certificaten en het wijzigen van de eigenschappen van het IT-account.

Identity Management (IdM), definitie:

Het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de identificatie en authenticatie van subjecten te faciliteren, te beheren en te controleren.

Onderstaande afbeelding schetst een eenvoudige IAM architectuur, die zowel de toegang tot oudere (legacy) systemen ondersteunt als de toegang tot moderne systemen.
M.u.v. ‘standalone’ objecten wordt voor vrijwel alle systemen een bepaalde vorm van IdM gebruikt. De HRM database met alle relevante persoonsgegevens wordt bij voorkeur als “authentieke bron” gebruikt voor het vullen van de Identiteiten en Policy Repository via koppelvlak (1). Deze repository vormt de kern van IAM, want in deze database worden alle toegangsgegevens opgeslagen van personen en systemen. De repository wordt in XACML termen het Policy Information Point (PIP) genoemd. Via koppelvlak (2) worden de IdM gegevens doorgegeven aan de Authenticatie service. Dit geautomatiseerd doorgeven wordt *provisioning* genoemd.



Eenvoudige IAM architectuur

Access Management (AM), definitie:

Het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de toegang tot en het gebruik van objecten (systemen en informatie) te faciliteren, te beheren en te controleren.

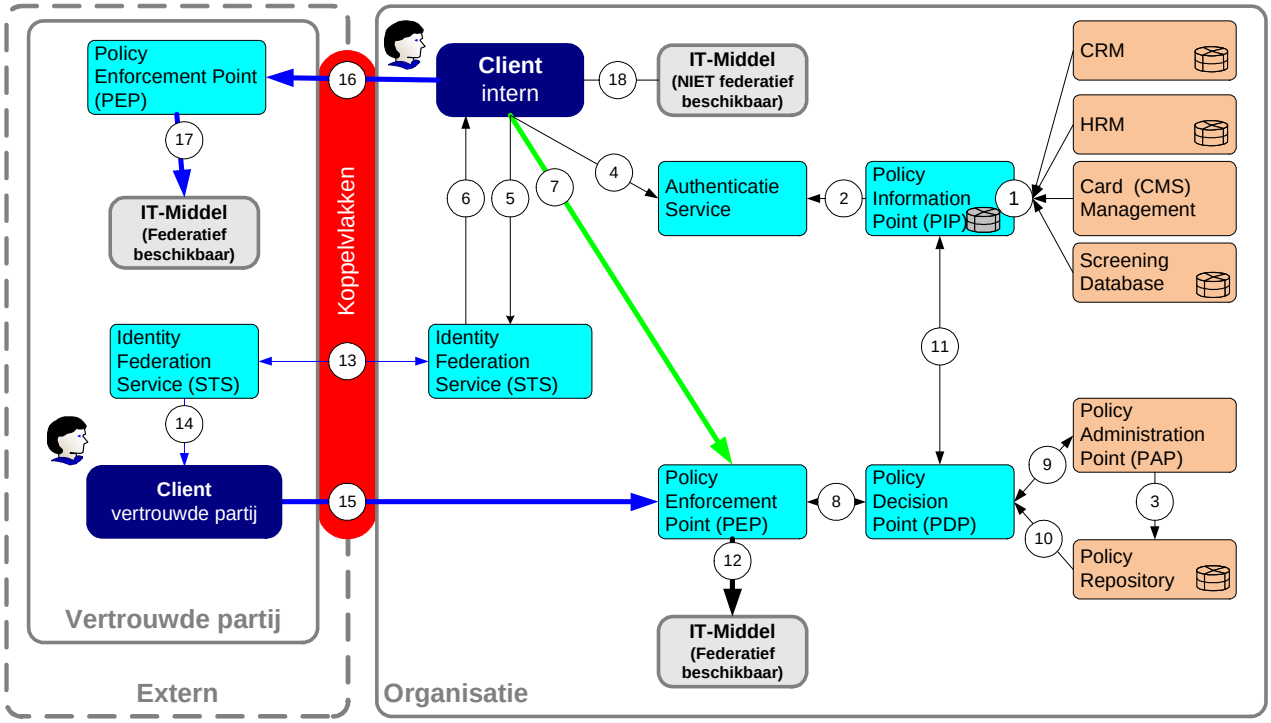
Uitgangspunt bij het verlenen van toegang zijn de z.g. *Policy ‘s* oftewel beleidsregels die vertaald zijn in autorisaties. De Authentication Service verzorgt via koppelvlak (3) de authenticatie van de personen die werken op de Client. Voor *legacy* systemen wordt na het authenticatie proces via koppelvlak (4) toegang verleend tot het IT-middel en daarmee de gegevens. De autorisatie wordt bij oudere systemen meestal binnen het IT-middel zelf gekoppeld aan het IT-account van het subject. Ook toegangsregels zijn specifiek voor het IT-middel gedefinieerd en geconfigureerd. De eigenaar vult de repository van zijn object met

toegangsrechten van geautoriseerde personen.

Wanneer authenticatie wordt verzorgd via *Kerberos*, dan wijkt het architectuurplaatje iets af van bovenstaande figuur; zie hiervoor het patroon SSO. De client haalt een *ticket* op van de *Ticket Granting Ticket* server, die acteert als Policy Enforcement Point (PEP). Deze ticket wordt aangeboden aan het IT-middel, waarmee toegang wordt verleend tot gegevens.

Gebruik makend van *XACML*, geeft het PDP op basis van toegangsregels via (8) toegang tot het IT-middel na authenticatie van de persoon en het besluit over de toegangsrechten vanuit de Policy Administration het Policy Decision Point: via koppelvlak (5) en (6). In overleg met eigenaren worden toegangsrechten gekoppeld aan rollen en centraal opgeslagen in een repository.

Onderstaande figuur schetst een IAM architectuur inclusief IAM-federatie functionaliteit. In de hierna volgende patronen wordt deze architectuur telkens in onderdelen toegelicht. De koppelvlaknummers zijn daarbij steeds dezelfde en hebben in alle volgende IAM-architectuurplaten dezelfde betekenis.
In het externe domein is alleen een “Vertrouwde partij” afgebeeld. De interactie met klanten en eigen medewerkers op externe clients is van een andere orde en is uitgewerkt in het patroon “Portaal en toegangsserver” en in het patroon “Koppelvlak semi-vertrouwde derden”.



IAM architectuur op basis van XACML

Deze IAM architectuur maakt het mogelijk dat applicaties wederzijds met vertrouwde partners kunnen worden gedeeld. Dat betekent dat eigen medewerkers applicaties van een *vertrouwde partij* kunnen gebruiken maar dat medewerkers van de vertrouwde partij op hun beurt ook de applicaties van de partnerorganisatie kunnen benaderen. De genummerde pijltjes in deze afbeelding geven weer welke interfaces ingericht moeten worden om flexibel informatie te kunnen delen in een federatief samenwerkingsverband. In de patronen Identity Management, Access Management en Federated IdM wordt de architectuur verder uitgewerkt.

Afwegingen

Het beheer over de IAM administraties kan op verschillende plaatsen in de organisatie worden belegd, bijvoorbeeld bij *“Enterprise userbeheer”*. De identiteit van personen die op de *personeelslijst* staan, worden beheerd door Human Resource Management (HRM). Doelgroepen zoals klanten, externe relaties worden in een andere repository beheerd zoals: Customer Relations Management (CRM). Vanuit deze repositories wordt het PIP gevoed. Afgewogen moet worden hoe met uitzendkrachten, contractors en medewerkers op projectbasis wordt omgegaan in de repositories. Deze personen moeten op een bij hun taak passende manier *op naam* worden geautoriseerd. Registratie van IT-componenten in de gedaante van *subject* en *object* wordt ondergebracht in de CMDB, als onderdeel van IT-service management.

Heeft een organisatie gekozen voor de invoering van IAM, dan is een stapsgewijze invoering belangrijk:
1) Start bij afdelingen of applicaties waar de grootste voordelen te behalen zijn en ga van daaruit verder uitbreiden.

2) Koppel invoering IAM aan nieuwbouw- of vernieuwingstrajecten, zodat desinvesteringen voor wijzigingen in bestaande architecturen zo veel mogelijk worden vermeden.
3) Bij legacy-applicaties moet een afweging plaatsvinden op basis van een business case. Daarbij worden de kosten verbonden aan de traditionele 'embedded' IAM van de applicatie vergeleken met de kosten voor het aanpassen van de applicatie. De overwegingen daarbij zijn het kwantitatieve deel (jaarlijks terugkerende kosten van een product) en het kwalitatieve deel (imago, wet- en regelgeving etc.).

Implicaties

- Veel systemen en applicaties worden geleverd met een ingebouwde autorisatiestructuur. Het aanpassen van deze systemen en applicaties om een meer centraal toegangsbeheer mogelijk te maken, kost veel geld en inspanning.
- De koppeling van systemen aan een IAM systeem leidt tot meer afhankelijkheden binnen de technische architectuur (nieuwe interfaces) en informatiearchitectuur (autorisatiemodellen zijn gekoppeld aan modellen van de applicaties). Aanvankelijk leidt dit tot een verhoging van de complexiteit, maar een juiste aanpak van IAM maakt deze complexiteit beheersbaar.
- Belangrijker nog dan de aanpassingen aan de informatie- en systeemarchitectuur zijn de afspraken over verantwoordelijkheden over de verschillende deelgebieden. Wie is verantwoordelijk voor autorisaties?

Gerelateerde patronen

- Identity management (IdM): gaat dieper in op het beheer van identiteiten
- Access Management (AM): gaat dieper in op de toekenning van toegang tot objecten
- Single Sign-On (SSO): gaat in op gemeenschappelijk gebruik van authenticatiemiddelen en - diensten binnen een organisatie
- Federated Identity Management: gaat in op het gebruik van identiteitsgegevens en mogelijk ook authenticatiediensten van andere organisaties, binnen een vertrouwenskader (federatie).

Standaarden en Links

- RBAC: (http://www.nist.gov/rbac/)
- SAML: (http://www.oasis-open.org/)
- XACML: (http://www.oasis-open.org/)
- OAuth: Open Authorization is een open standard voor autorisatie. (RFC 5849: the OAuth 1.0 Protocol)
- LDAP (RFC 4510: Lightweight Directory Access Protocol)

Omdat organisaties en partners elkaar niet kunnen voorschrijven welke producten en leveranciers moeten worden gebruikt en met welke partijen ze mogen samenwerken, wordt de toegepaste *Federatieve* Authenticatie bij voorkeur volledig gebaseerd op z.g. *Open Standaarden*. De belangrijkste standaarden die in dit verband moeten worden geadopteerd zijn:

- **SAML**: Security Assertion Markup Language. De OASIS standaard voor uitwisseling van authenticatie en autorisatiegegevens tussen verschillende zones.
- **XACML**: eXtensible Access Control Markup Language. Een access control policy taal, die geïmplementeerd is in XML en een procesmodel. Dit model beschrijft hoe met policies om moet worden gegaan en geeft structuur aan Access management met onderstaande begrippen:

XACML functie	Toelichting
PIP: Policy Information Point	Bevat alle identiteitsinformatie voor toegang tot IT-systemen zowel *persoonsgebonden* als *functioneel*. Vanuit verschillende directories vindt *provisioning* plaats naar het PIP, dat vervolgens relevante account- en persoonsinformatie *real-time* kan doorgeven aan authenticatieservices, zoals Kerberos.
PAP: Policy Administration Point	Administreert beleidsregels zoals wachtwoord policy, de authenticatiemethode voor toegang tot specifieke objecten (resources), een kenmerk die een subject (gebruiker) moet hebben voor autorisatie tot een object etc.
PDP: Policy Decision Point	Neemt real-time *besluiten* op basis van resource-, identiteit- en policy- informatie. De PDP maakt daarbij gebruik van de Identity Repository (PIP) en de Policy Repository.
PEP: Policy Enforcement Point	Dwingt real-time in de infrastructuur af dat de juiste policy wordt nageleefd. Dat kan betekenen dat voor een bepaalde URL de gebruiker zich moet authenticeren door middel van één of twee factor authenticatie (Wachtwoord of Token met PIN etc.)

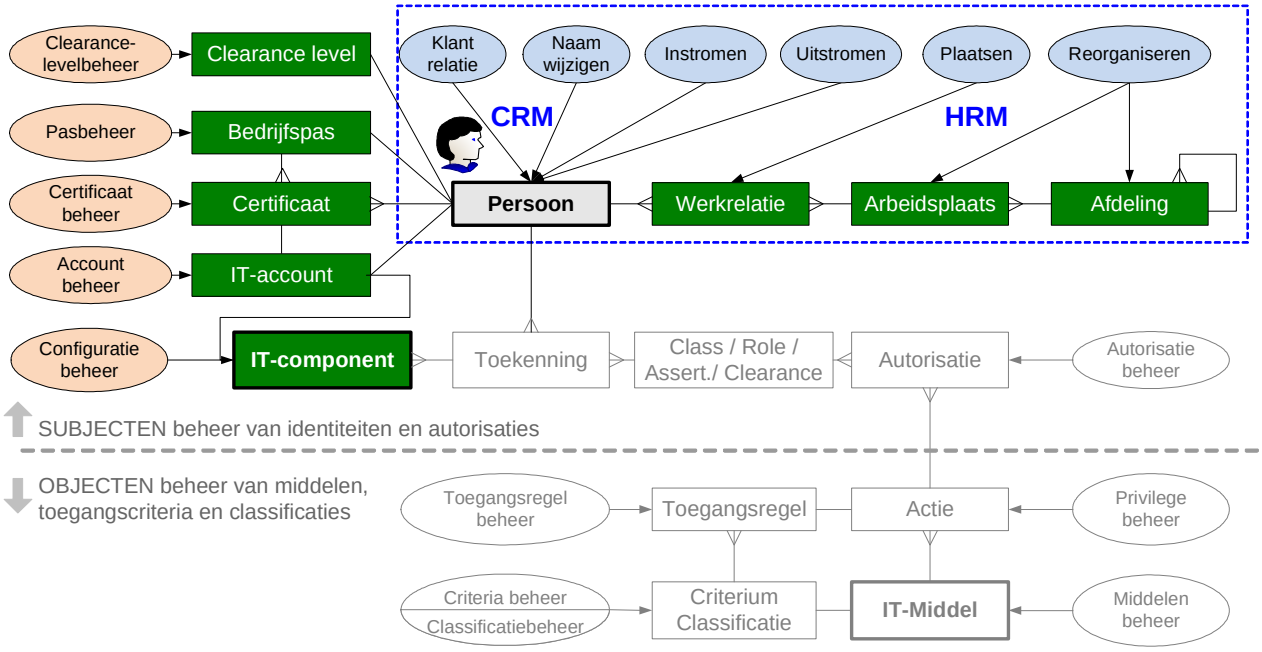
15. Identitymanagement (IdM)

Criteria

Integriteit, Vertrouwelijkheid

Context

Organisaties registreren personen om daarmee de toegang en het gebruik van objecten (gebouwen, ruimten, gegevens, diensten, systemen, etc.) te regelen. Daarbij wordt onderscheid gemaakt naar medewerkers (zowel intern als extern), klanten, (zaken)partners en personen in andere rollen. Niet alleen personen, maar ook systemen, services en processen moeten toegang kunnen hebben tot objecten. In zakelijke context behoren personen en systemen in het algemeen bij een organisatie en organisatiedeel, extern of intern. Deze actoren, in de gedaante van personen, systemen en organisaties worden aangeduid als *subjecten*.



Beheerprocessen Identity Management

Probleem

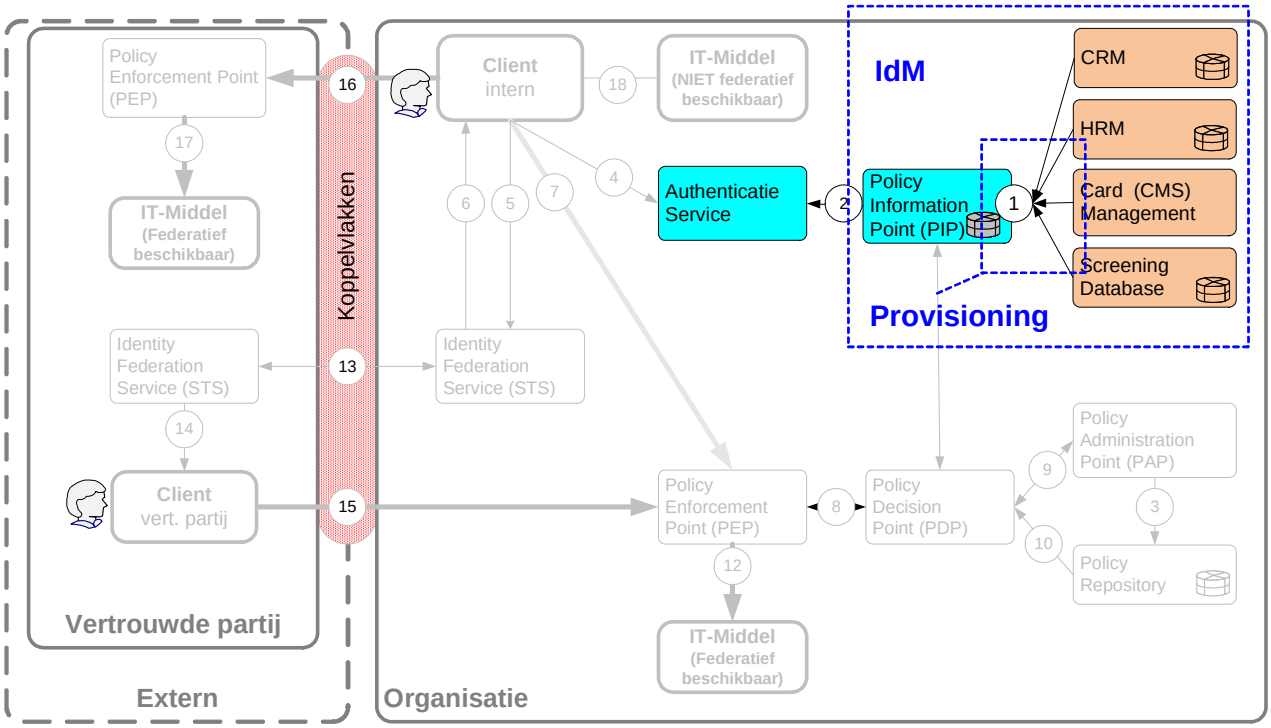
De geschetste problemen uit het themapatroon hieronder toegelicht:

1. **De identiteit van een subject is niet uniek.**
   Subjecten kunnen op veel plaatsen verschillend worden geregistreerd. Geautomatiseerd koppelen of relateren van gegevens over dezelfde persoon is moeilijk of zelfs onmogelijk. Wijzigingen in (stam)gegevens kunnen daardoor niet snel en betrouwbaar in alle gekoppelde systemen worden doorgevoerd. Gevolg is dat nieuwe medewerkers niet direct aan de slag kunnen en rechten niet worden ingetrokken bij functiewijzigingen of bij het verlaten van de organisatie.
2. **Registratieprocessen zijn niet volledig.**
   Gevolg daarvan is dat bijvoorbeeld tijdelijke krachten minder nauwkeurig worden geregistreerd, terwijl juist deze groep medewerkers een hoge mutatiegraad kent.
3. **Samenhang van registraties ontbreekt.**
   Registratieprocessen zijn verdeeld over verschillende afdelingen en hebben verschillende kwaliteitseisen. Uitzendkrachten kunnen bijvoorbeeld via afdeling Inkoop worden geregistreerd.
4. **De kwaliteit van identiteitsgegevens is ontoereikend.** De gegevens van subjecten zijn niet actueel of onvolledig.

Oplossing

Het implementeren van processen en hulpmiddelen om subjecten eenduidig te registreren en identificeren en ervoor zorg te dragen dat relevante gegevens binnen de gehele organisatie beschikbaar zijn. Dit geheel van processen en hulpmiddelen wordt aangeduid als *Identity Management* (IdM). Dit omvat het managen van de gehele levenscyclus (lifecycle) van een identiteit.

Identity management is gepositioneerd in onderstaand deel van de IAM architectuur en gebruikt de HRM database als “authentieke bron” en “basisregistratie”. Via een berichtenmakelaar (hier niet getekend) worden de persoonlijke gegevens met alle relevante attributen aangeleverd (1) aan een geconsolideerde database: het IdM systeem. Het IdM systeem treedt voor de functie Access Management op als het z.g. *Policy Information Point* (PIP). Het PIP geeft alle relevante subject gerelateerde informatie door aan het *Policy Decision Point* (PDP), om toegang te laten verlenen. Deze configuratie kan ook eenvoudiger worden opgezet met behulp van een z.g. *virtuele directory*.

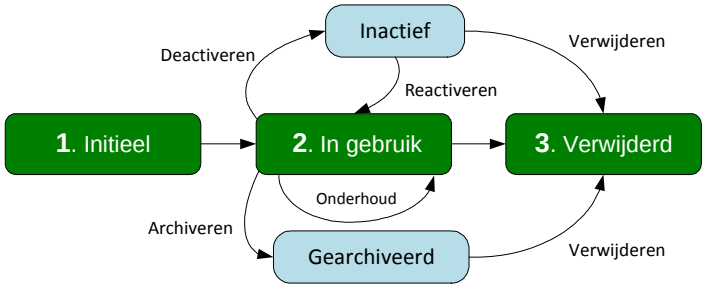


Positionering van Identity Management in de IAM architectuur

Vanuit de verschillende directories van het IdM systeem vindt *provisioning* (1) plaats naar het PIP. Via interface (2) kan vervolgens (real-time) account/persoonsinformatie aan de centrale Authenticatie Service, b.v. Kerberos, ter beschikking gesteld. Provisioning is een relatief *langzaam* uitgifteproces, maar wel snel genoeg om b.v. de *uitzendkracht* dezelfde dag nog toegang te kunnen geven. Bij het IT-account worden vanuit IdM ook attributen voor authenticatie aangegeven zoals een password of een Public Key Certificaat dat behoort bij het account. Provisioning blijft nodig gedurende de hele levenscyclus van een IT-account voor een subject.

Voor identiteiten is de volgende levenscyclus van toepassing:

1. **Initieel:** er zijn gegevens over een subject bekend, maar er is nog niet aan de voorwaarden voldaan om een identiteit in het IdM systeem vast te leggen.



Levenscyclus van identiteiten

2. **In gebruik:** de identiteit is geregistreerd en voldoende volledig om gebruikt te kunnen worden. In dit stadium van de levenscyclus wordt de identiteit gebruikt en onderhouden, zonder dat dit tot overgang naar een ander stadium leidt. Vanuit dit stadium kan de identiteit worden gedeactiveerd (bijv. voor een werknemer die ontslag neemt of een klant die een contract opzegt), of gearchiveerd.
   - **Inactief:** de identiteit is niet beschikbaar voor normaal gebruik, maar kan wel weer actief worden gemaakt.
   - **Gearchiveerd:** de identiteit is niet langer beschikbaar voor gebruik en mag niet opnieuw worden geactiveerd. Wel worden de gegevens bewaard voor eventuele controles.
3. **Verwijderd:** de gegevens zijn uit archieven verwijderd en zijn daarna niet meer beschikbaar.

Afwegingen

Uit onderzoek blijkt dat medewerkers al snel kunnen beschikken over een groot aantal attributen. De databases van het IdM- en IAM systeem moeten in staat zijn om deze aantallen te ondersteunen. Overwogen kan worden om attributen die slechts voor één afnemend systeem van belang zijn, in dat systeem zelf te onderhouden. Die overweging geldt met name voor kritische systemen met een hoog afbreukrisico voor de organisatie. Dit zijn systemen die in de zone ‘kluis’ staan.

Bij traditioneel beheer van identiteiten worden identiteitsgegevens veelal verbonden met een kunstmatig unieke identificatie binnen een organisatie, bijvoorbeeld een personeelsnummer of accountnaam. Dit wordt dan opgevat als “de” identiteit van het subject. Nadeel van dergelijke identifiers is, dat ze buiten de context van de organisatie geen betekenis meer hebben en in een federatieve context onbruikbaar zijn. Door de identiteit te communiceren in de vorm van een set attributen over een subject, is het mogelijk dat partijen federatie gegevens over identiteiten kunnen combineren en matchen. Dit maakt het mogelijk, meer functionaliteit te bieden. Het heeft ook implicaties voor de privacy. Ook bestaat het gevaar dat onterechte matches worden gemaakt. Dergelijke methoden, getypeerd als “Identity 2.0”, worden gebruikt door internet dienstverleners als Google en Amazon.

Implicaties

Invoering van IdM heeft voor de organisatie en gebruikte techniek relatief veel implicaties:

- Activiteiten voor het beheer van identiteitsgegevens worden verplaatst van de doelsystemen naar IdM beheeractiviteiten.
- De doelsystemen worden afhankelijk van het IdM-systeem en indirect van de authentieke bronnen.
- De authentieke bronnen moeten juist, volledig en actueel zijn.
- Alle applicaties en systemen binnen de organisatie, althans die applicaties en systemen die binnen de scope van het IdM vallen, moeten worden aangepast, zodat ze niet meer gebruik maken van een eigen identiteitenregistratie maar van het IdM-systeem.
- Applicaties en systemen die gebruik maken van IdM, moeten de koppelvlakstandaarden van het IdM ondersteunen. Omgekeerd moet het IdM-systeem zo worden opgezet, dat het alle koppelvlakstandaarden van applicaties en systemen kan ondersteunen.
- Voorafgaand aan de uitrol van een IdM, moet een *naamgevingconventie* beschikbaar zijn, geldig voor het hele bereik van het IdM-systeem. Uitzonderingen op de naamgevingconventie kunnen leiden tot ongewenste effecten in de IT-voorzieningen en toegangssystemen.
- In grootschalige IdM-omgevingen is het mogelijk dat verschillende attributen of sets van attributen gebruikt kunnen worden om dezelfde persoon te identificeren. Een gebruiker kan bijvoorbeeld een gebruikersnaam én een *Distinguished Name* van een digitaal certificaat hebben.
- Omdat doelsystemen via IdM afhankelijk zijn van actuele gegevens uit de authentieke bronsystemen, moeten de wijzigingen in de authentieke bronsystemen tijdig worden doorgegeven aan de doelsystemen. Dit wordt aangeduid met *synchronisatie*. Het mechanisme voor synchronisatie moet voldoen aan de eisen die de doelsystemen stellen aan de actualiteit van de gegevens. Dit heeft gevolgen voor de initiële opvoer binnen de authentieke bronsystemen, maar ook bij een tussentijdse verwijdering met spoedeisend karakter (bijvoorbeeld als gevolg van een ontslag op staande voet).
- In veel gevallen moeten verschillende *doelgroepen* worden geregistreerd. Voor elk van de doelgroepen moet een authentieke bron beschikbaar zijn om de kwaliteit van de gegevens te borgen. Het is niet aanvaardbaar dat personen “zo maar” worden opgevoerd zonder een proces om de actualiteit en kwaliteit van de gegevens te waarborgen (zoals bij een authentieke bron).
- Een IdM-systeem is een IT-voorziening die zelf ook moet worden onderhouden. Om continuïteit te waarborgen zal het IdM-systeem zelf vaak niet zijn aangesloten als doelsysteem.
- *Functionele identiteiten* (b.v. IT-voorzieningen als identiteit) hebben een afwijkende levenscyclus van persoonsgebonden identiteiten. Hierbij is het belangrijk dat er een eenduidige eigenaar van de functionele identiteit is, zodat de verantwoordelijkheid over handhaving en gebruik van de functionele identiteit duidelijk ligt. Dit hoeft vaak niet (meer) de originele aanvrager/eigenaar te zijn.
- Bij de registratie van *persoonsgegevens* moet rekening gehouden worden met de eisen van de WBP (Wet Bescherming Persoonsgegevens). Bij registratie van gegevens moet *doelbinding* worden vastgelegd.
- Er dienen afspraken gemaakt te worden over het *eigenaarschap* van de IdM-omgeving.

Gerelateerde patronen

- Themapatroon: IAM - Identity & Access Management.
- Federated Identity Management.
- AM - Access Management.
- PKI - Public Key Infrastructure.

Standaarden

- Directory – gegevensstructuur en protocollen: X.500. LDAP (gebaseerd op X.500 maar vereenvoudigd, vormt de basis voor een groot aantal producten).
- Directory-toegang: X.500 DAP, LDAP.
- Public Key certificaten: X.509.
- Bevestiging en authenticatie van identiteitsgegevens en attributen: SAML.
- Uitwisseling van gegevens over toegangsverlening en model voor toegangsverlening: XACML.

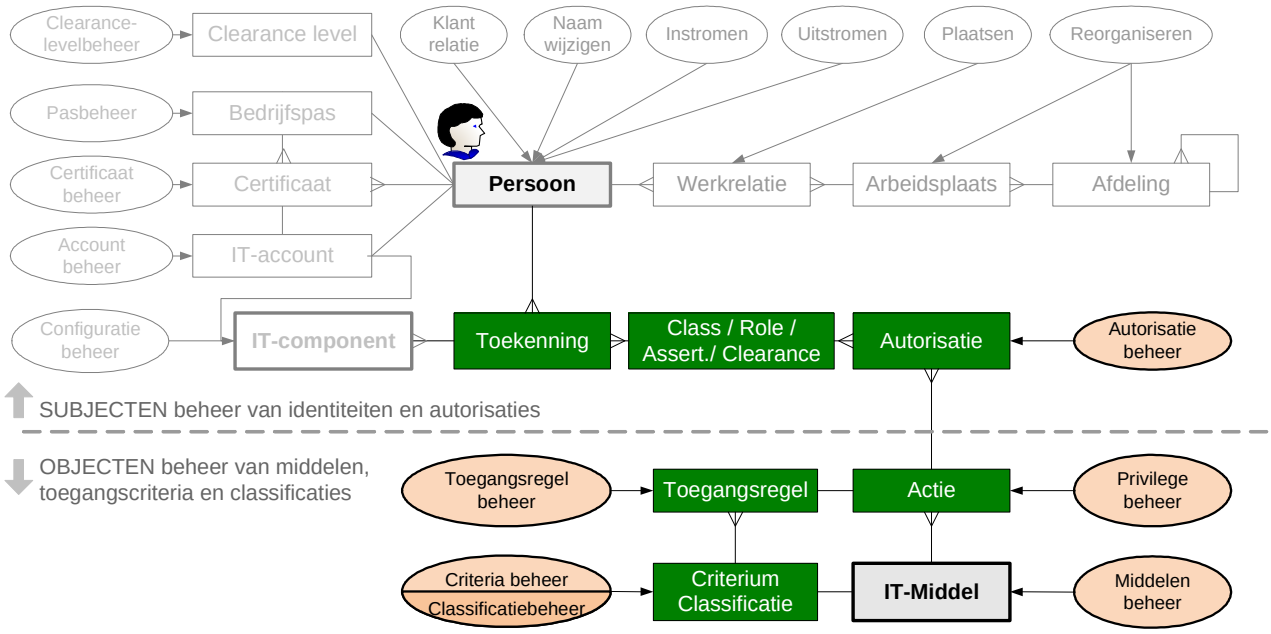
16. Access Management (AM)

Criteria

Vertrouwelijkheid, Integriteit, Controleerbaarheid

Context

Binnen iedere organisatie moet de toegang tot informatie beperkt worden tot personen of systemen die geautoriseerd zijn om de informatie in te zien of te kunnen wijzigen. Daarbij wordt veelal onderscheid gemaakt naar medewerkers (zowel intern als extern), klanten, (zaken)partners en individuen in andere rollen. Onderstaande figuur schetst de omgeving waarin toegang verleend wordt tot het IT-middel.



Processen voor verlenen van toegang

Probleem

De geschetste problemen uit het themapatroon worden hieronder toegelicht:

1. **Need to know dilemma.** Vaak wordt gebruik gemaakt van Role Based Access Control (hierna RBAC). Het definiëren van een rollenmodel is lastig, omdat medewerkers op basis van de toegewezen rollen enkel de toegangsrechten toegewezen dienen te krijgen die zij nodig hebben om hun taken te vervullen (Need to know). Wordt er te 'ruim' geautoriseerd, dan ontstaan er risico's van ongeoorloofde toegang, maar een te 'strikt' ingeregeld rollenmodel zorgt voor een 'explosie' van rollen waardoor een onwerkbare situatie ontstaat.
2. **Het definiëren van toegangsrechten is een moeizaam en langdurig proces.** Organisaties zijn bovendien geen 'vaste structuren'. Reorganisaties volgen elkaar vaak sneller op dan de doorlooptijd van het samenstellen en doorvoeren van een bedrijfs-rollenmodel. RBAC implementaties worden veelal ervaren als 'in beton' gegoten structuren van toegangsrechten die te wensen overlaat aan flexibiliteit. Dit probleem en het 'need to know' dilemma hebben tot gevolg:
   - Het IT-landschap wordt maar gedeeltelijk (rol-) gemodelleerd.
   - Rollenmodellen lopen achter bij de werkelijke situatie.
   - Organisaties onderscheiden (te) veel rollen; soms meer rollen dan medewerkers!

   Deze effecten veroorzaken *inefficiënt toegangsbeheer* of zelfs het 'vastlopen' van IAM-projecten.
3. **Samenhang ontbreekt** in registraties van identiteiten en hun toegangsrechten.
4. **Management heeft geen overzicht** en inzicht in actuele toegangsrechten van medewerkers.
5. **Management is niet adequaat** om toegangsrechten op maat te verlenen of in te trekken.
6. **Procedures en/of technieken ontbreken** om vast te stellen tot welke gegevens subjecten zich toegang hebben verschaft en in hoeverre dit in strijd is met bedrijfsregels (beleid).
7. **Het aantal wijzigingen is te groot** voor handmatige invoering van identiteiten en toegangsrechten van subjecten op elk individueel systeem (IT-middel).
8. **Toegangsrechten worden niet ingetrokken** wanneer medewerkers deze voor hun werk niet meer nodig hebben, of wanneer ze de organisatie verlaten.

Oplossing

Voor de geschetste problemen 1 t/m 8 zijn verschillende oplossingen mogelijk die een systematische aanpak opleveren. Niet alle problemen zijn met techniek op te lossen zoals **1, 2, 5** en **8**, maar kunnen qua impact worden gereduceerd door faciliterende technische maatregelen.

Een systematische aanpak vraagt per informatiesysteem een methode, waarmee bepaald wordt hoe de toegangsrechten verdeeld worden over de betrokkenen. De bekendste methoden zijn: DAC, RBAC en MAC. Voor autorisatieprofielen worden op de *gegevenslaag* deze drie methoden gebruikt, waarbij in de praktijk mengvormen voorkomen in één en dezelfde onderliggende infrastructuur.

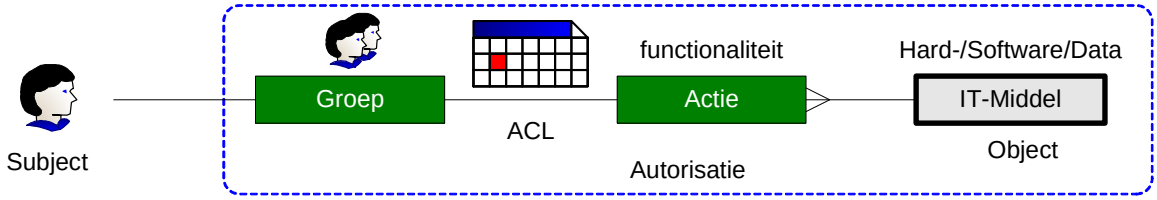
1. *Directe* koppeling van subjecten aan acties op objecten (DAC).
2. Aan de hand van *rollen.* Identiteiten vervullen één of meerdere rollen in een organisatie. Bij elke rol hoort een set toegangsrechten (RBAC).
3. Op basis van *classificatie* van gegevens (MAC). Subjecten krijgen een *clearance*-label toegekend, oftewel een formeel vertrouwensniveau (geheim, zeer geheim of confidentieel). Gegevens zijn in een organisatie die MAC gebruikt op dezelfde wijze geclassificeerd en gelabeld.

Op de *technologielaag* ontwikkelt zich een nieuwe methode: ABAC. Aanvullend op Access Control wordt Access Governance (AG) toegepast, waarmee achteraf kan worden bepaald welk subject toegang heeft gehad tot welke objecten. De volgende technologie methoden worden toegepast:

1. Aan de hand van *regels* (bedrijfsregels, bijv. grenswaarden: max. transactie 20k Euro voor rol R);
2. Aan de hand van *beweringen* (*assertions)* over attributen van een subject wordt een certificaat, verstrekt door een vertrouwde derde partij) via Attribute/Assertion Based Access Control (ABAC)
3. Op basis van de *context* (bijvoorbeeld: subject is geauthenticeerd met 2-factor authenticatie; gebruiker werkt remote, de gebruiker die de transactie heeft ingevoerd, mag hem niet goedkeuren);
4. Op basis van de *content* (bijv: een gebruiker mag alleen klanten van de eigen vestiging behandelen)

Methode 1: DAC: *Discretionary Access Control*:

Iedere applicatie, bestand of dataset heeft een eigenaar. Ieder te beveiligen object heeft zijn eigen repository. De data-eigenaar vult de repository voor zijn object met de toegangsrechten van de geautoriseerde subjecten. Bij een functieverandering verwijdert of wijzigt de eigenaar de rechten van het subject. DAC wordt geïmplementeerd via Access Control Lists (ACL), vaak afgebeeld in applicatie matrices. Toegang tot objecten is *gekoppeld aan de identiteit* van een subject. Er is dus een directe toegangsrelatie van subject naar object.



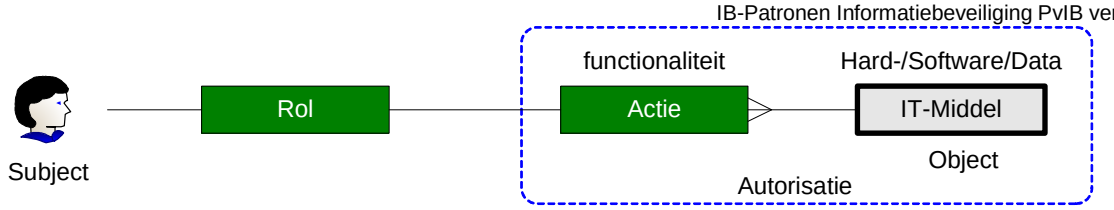
DAC: toegang gekoppeld aan identeiten

DAC wordt beheersbaar door subjecten in te delen in klassen (class) of kringen; (b.v. owner, group, system, world). De toegangscontrole in Unix, VMS en PC-Windows werkt op deze basis. Permissies worden verleend als: *No access*, *Read*, *Write*, *Change* en *Full Access*. In dit model wordt bij een verandering van de functie van de betrokkene de rechten van de persoon (of systeem) in de repository rechtstreeks gewijzigd.

Methode 2: RBAC: *Role Base Access Control*:

Toegang wordt centraal geregeld, aan de hand van vastgestelde regels, die aangeven hoe subjecten en objecten interacteren. Toegang tot objecten wordt verleend op basis van de *rol die* een subject heeft binnen een organisatie. Omdat er geen directe koppeling is tussen subject en object, wordt RBAC ook wel *Non-discretionary* Access Control genoemd.

Hieronder is het RBAC principe geschetst. Een *rol* is een afspiegeling van de taken van een subject op een bepaald moment en is daarmee een afspiegeling van de autorisaties die iemand heeft. Een rol is applicatieoverstijgend en bestaat zelfstandig. Een subject vervult één of meerdere rollen in een organisatie. Vanuit een specifieke rol in het bedrijfsproces krijgt hij toegang tot IT-functies, uitgevoerd door IT-middelen. Rollen zijn bedoeld om toegewezen te worden aan *meerdere* subjecten.

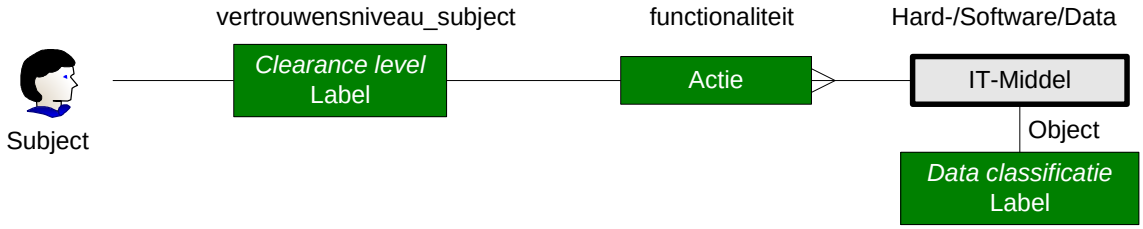


RBAC: toegang gekoppeld aan rollen

Het vaststellen van autorisaties van een rol binnen RBAC kan in twee richtingen: *bottom-up* en *top-down*. De bottom-up methode gebruikt bestaande autorisaties en groepeert deze tot rollen. Dit wordt bij voorkeur geautomatiseerd uitgevoerd en wordt *role-mining* genoemd. De top-down aanpak gaat uit van de bedrijfsprocessen. Vanuit een bedrijfsproces wordt afgeleid welke autorisaties minimaal nodig zijn om een bepaalde taak uit te voeren. Beide methoden hebben specifieke voor- en nadelen. Role-mining is relatief onnauwkeurig en vergt voor controle op de juistheid van de verkregen rollen alsnog een zekere 'top-down' aanpak. De top-down methode kan in de praktijk van grote organisaties een zodanig lange doorlooptijd hebben, dat het verkregen rollenmodel al weer achter loopt op de realiteit van snel veranderende organisaties. Beperk daarom het aantal rollen tot wat absoluut noodzakelijk is.

Methode 3: MAC: *Mandatory Access Control*:

Centraal wordt geregeld, dat subjecten toegang hebben tot gegevens met een classificatie (label) van maximaal het subjectgebonden 'vertrouwensniveau' (clearinglevel). Het label is een *attribuut* dat behoort tot het subject. Elk afzonderlijk dataobject heeft een attribuut. De gezamenlijke repository van de *toegangsregels* wordt beheerd door de verschillende eigenaren van IT-middelen én datasets.



MAC: toegang gekoppeld aan labels

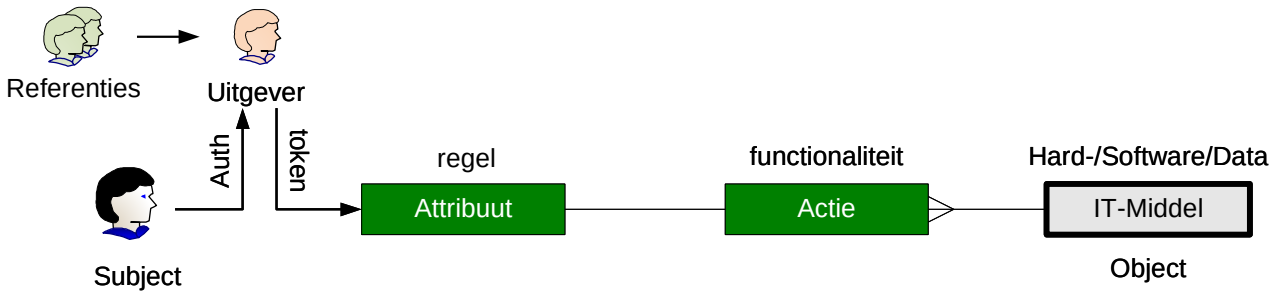
MAC verleent het subject toegang tot objecten op basis van Clarence level *labels,* die worden vergeleken met overeenkomstige classificatie labels van de subjecten.

MAC verleent toegang tot geclassificeerde data, tot maximaal het vertrouwensniveau wat aan het subject is toegekend. Zowel het subject als object bezit labels, die wanneer ze voldoen aan de bedrijfsregels, toegang geven tot IT-middelen en gegevens. MAC is bedoeld voor het verwerken van geclassificeerde gegevens en kan op verschillende manieren worden ingevuld, b.v. met RBAC, maar ook met ABAC.

Implementatie ABAC: *Attribute/Assertion Based Access Control*:

Deze vorm van Access Control is een techniek om DAC, RBAC of MAC te kunnen implementeren.
In ABAC worden toegangsrechten geassocieerd met een set van *regels*, die zijn uitgedrukt in meetbare parameters of *attributen*; die vervolgens worden toegekend aan subjecten die kunnen bewijzen dat zij voldoen aan de regels. ABAC, geeft dus toegang tot IT-diensten op basis van een bewering over de *eigenschappen* (attributen) van de dienstaanvrager (subject). De attributen kunnen allerlei formaten of gedaantes hebben: groepen, rollen, clearance levels, context etc.

ABAC past in een omgeving, waar de eigenaar van het object de identiteit van het subject niet exact kent, zoals het internet of een gefedereerde omgeving. Bepaalde kenmerken worden gebruikt om te bepalen of iemand toegang krijgt zonder de identiteit eerst vast te stellen. Die kenmerken kunnen geborgd zijn in certificaten of tokens uitgegeven door een derde partij.



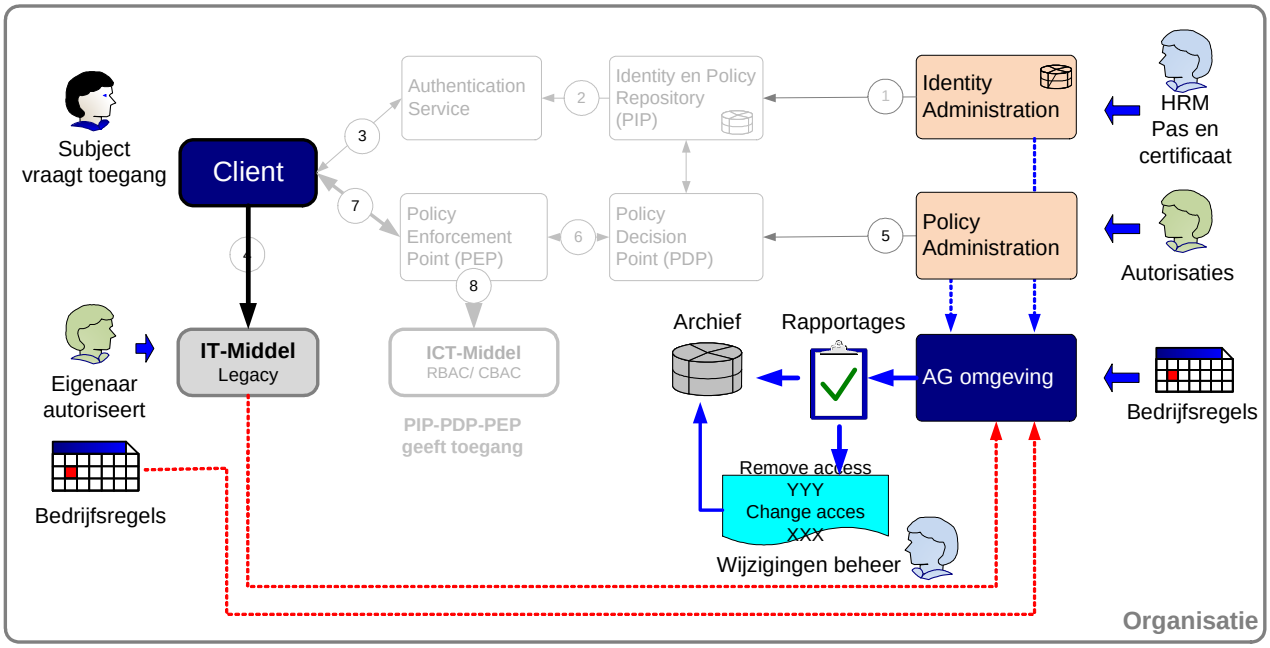
ABAC: toegang gekoppeld aan attributen

Implementatie AG: *Access Governance*:

Access Governance, hierna afgekort met AG, is geen methode van Access Control, maar een *aanvulling* op DAC, RBAC, MAC of implementaties van ABAC en stelt het management in staat om de reeds toegekende rechten geautomatiseerd en *detectief* te beheersen.

In snel veranderende organisaties, die toegang verlenen op basis van DAC, of die de vereiste autorisatieregels niet voldoende fijnmazig kunnen implementeren in RBAC of A/CBAC, kan *Access Governance* (AG) worden toegepast.

Dit is een systeem, dat in plaats van de toegang *proactief* te regelen op basis van Need-to-know, *reactief* bepaalt of subjecten op basis van *verleende* autorisaties toegang hebben gehad tot IT-services, waar ze gelet op verleende autorisaties en bedrijfsregels toegang toe zouden mogen hebben. AG is dus controle *achteraf*.



AG: toegang gecontroleerd op basis van bedrijfsregels

De meerwaarde van AG is vooral de *menselijke* tussenkomst. Als bij AG vals alarm geslagen wordt, dan kan dat via een handmatige nacontrole of in overleg met de gebruiker recht gezet worden. Access Control is echter absoluut en onjuiste afkeuring leidt tot onnodige hinder.
AG controleert toegang aan de hand van *bedrijfsregels*. Dit zijn meetbare parameters, afgeleid van autorisatiematrices, de inrichting van IT-systemen en de beheerprocessen voor logische toegang.

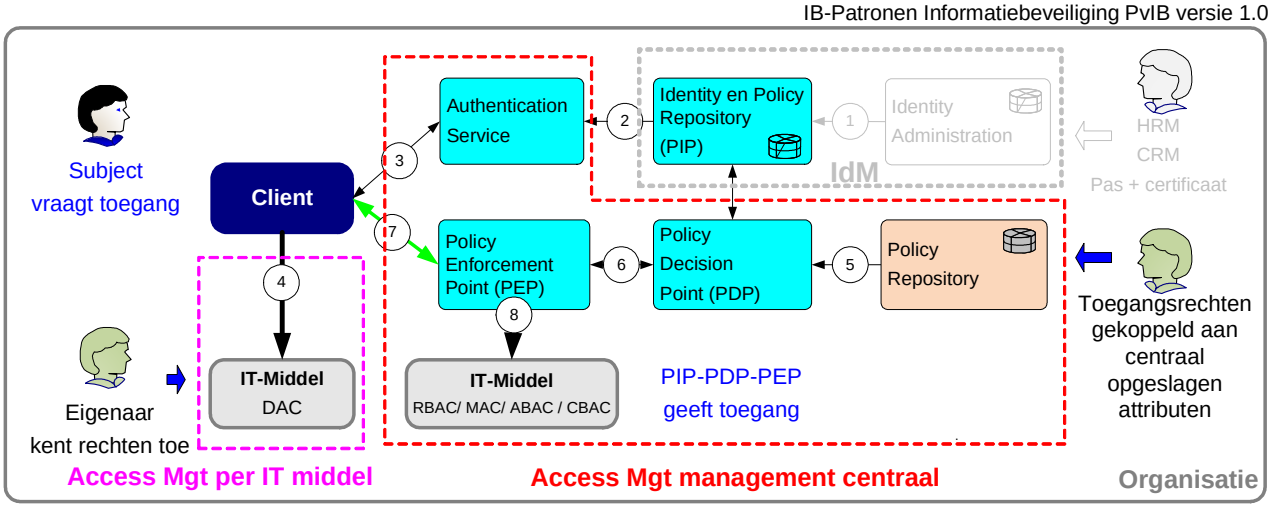
We onderscheiden twee soorten bedrijfsregels:
1) Generieke Bedrijf Regels (GBR's)
Generieke bedrijfsregels omvatten de toetsingscriteria die zijn afgeleid vanuit het generieke informatiebeveiligingsbeleid van de organisatie. Deze regels zijn van toepassing op meer dan één specifiek IT-systeem. Voorbeeld van een GBR: "Accounts zijn herleidbaar tot een natuurlijk persoon".

2) Specifieke Bedrijf Regels (SBR's)
Per IT-systeem worden bedrijfsregels gedefinieerd die specifiek voor het betreffende systeem van toepassing zijn. De regels worden opgesteld vanuit autorisatiematrices (indien aanwezig) en stellen eisen t.a.v. van het beheersen van functiescheidingen en van het afschermen van kritieke functies. Voorbeeld van een SBR: "Een gebruiker met autorisatie PQR mag geen toegang worden verleend tot een systeem waarvoor autorisatie XYZ nodig is".
AG kan voor het oplossen van probleem 5 en 6 worden gecombineerd met RBAC of CBAC.

Architectuur

Onderstaande figuur schetst de bouwblokken van een architectuur voor verschillende vormen van Access management. Links een per IT-middel (DAC) en rechts een centraal geregelde methode van Access Management.

In mengvormen van DAC en MAC wordt IdM vaak ook buiten het IT-middel geregeld, al dan niet gebruik makend van een Authentication Service zoals Kerberos.

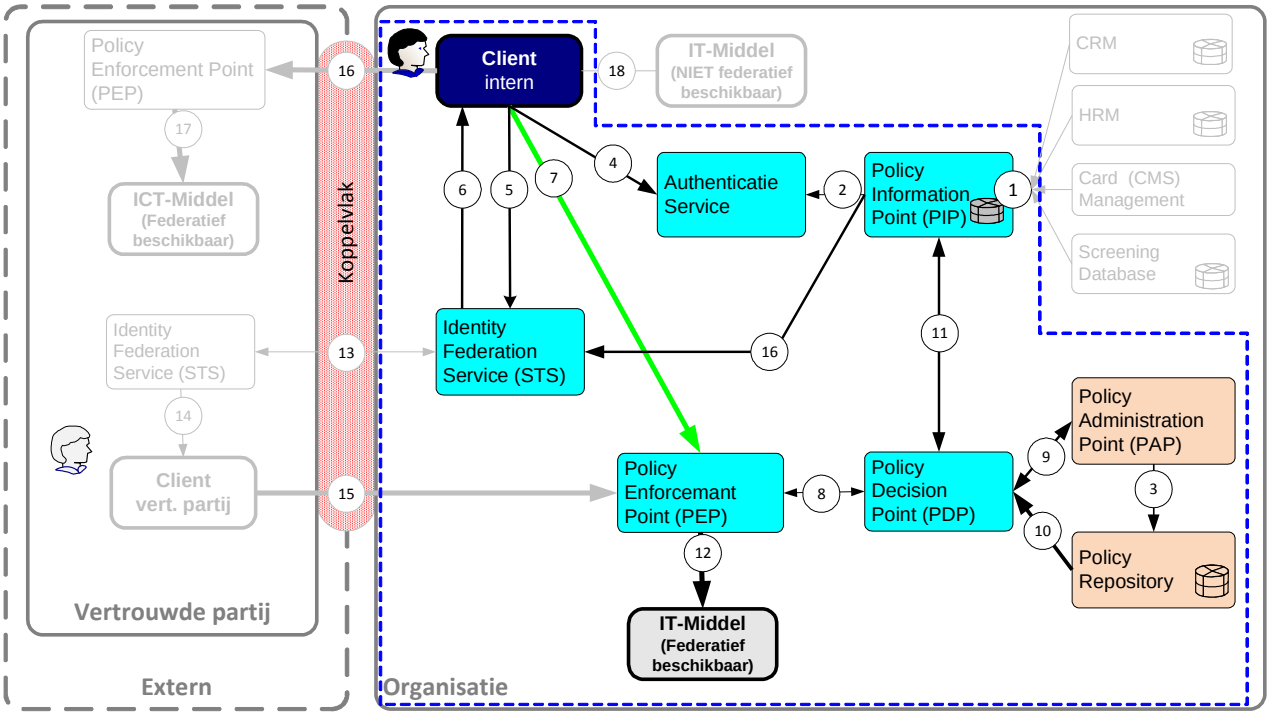


Architectuur voor verschillende methoden van acces management

Architectuur voor intern geregelde toegang tot IT-middelen

Deze figuur schetst de generieke opzet voor AM op basis van RBAC of CBAC. Deze opzet is tevens geschikt voor web-based toegang en kan worden uitgebreid met toegang tot systemen van een externe vertrouwde partij (zie patroon Federated Identity & Access Management).

In het Policy Administration Point vindt het beheer van de autorisaties plaats. Het gaat hier om beheer van z.g. access-policies, of anders gezegd: de *Toegangsregels* en *Criteria*. Die policies bestaan uit wachtwoordconventies, authenticatie methode voor specifieke resources en kenmerken die een gebruiker moet hebben voor autorisatie tot een resource. De Criteria en Toegangsregels waaronder een bepaalde toegang kan worden verleend wordt uitgedrukt in XACML statements en worden opgeslagen in een daarvoor geschikte Policy Repository.



Architectuur voor intern geregelde acces management

De toegang wordt verleend in de volgende stappen:

- De Authenticatie Service verzorgt de authenticatie van de medewerker in het Intranet en treedt tevens op als Kerberos server.
- De gebruiker logt via de Authenticatie Service in op zijn IT-account met behulp van een wachtwoord (of bedrijfspas + Pincode). Dit authenticatieproces heet PKInit. Het resultaat is een Kerberos ticket op de client van de medewerker (pijl 4).
- Als een gebruiker een middel (resource) wil gebruiken dat vraagt om een SAML-token, dan kan de gebruiker het benodigde SAML-token verkrijgen bij de Identity Federation Service. Deze Identity Federation Service treedt in dat geval op als Security Token Service en voert een protocolconversie van Kerberos naar SAML uit (pijlen 5 en 6).

- Voor het plaatsen van additionele informatie over de medewerker in het SAML-token kan de Identity Federation Service via LDAP informatie ophalen uit het Policy Information Point (pijl 16).
- Het verzoek om toegang van de gebruiker komt binnen bij het Policy Enforcement Point (PEP) (pijl 7).
- Het PEP bevraagt het Policy Decision Point (PDP) of de desbetreffende gebruiker toegang kan krijgen tot het gevraagde IT-Middel (pijl 8).
- Het PDP raadpleegt het PIP en het Policy Administration Point (PAP) en ontvangt de relevante toegangsregels uit de Policy Repository (pijlen 9,10 en 11).
- Als het PEP van de PDP verneemt dat de gebruiker toegang tot het IT-middel mag krijgen, dan wordt die verleend (pijl 12).

Afwegingen

Bepalende factoren bij de keuze van de Access management methodes zijn de omvang van de organisatie en het belang dat gehecht wordt aan de granulariteit van de autorisaties van subjecten. De tabel geeft aan welke van AM-problemen (1 t/m 8) kunnen worden opgelost door de verschillende methoden van toegang. Wat opvalt is de relatief slechte score van DAC en RBAC, wat overigens wel de meest toegepaste methoden zijn.

ABAC is een veelbelovende implementatievorm van DAC, RBAC of MAC, maar de sortering van ondersteunende tools daarvoor is nog beperkt. MAC vereist dat IT-componenten labeling van gegevens ondersteunen, voor zowel input, verwerking als output van gegevens. Voorts moeten aan gebruikers van geclassificeerde gegevens via MAC systemen vertrouwensniveaus worden toegekend. AG is geen Access Control, maar een veelbelovende methode om via ‘intelligence’ achteraf te kunnen bepalen wie toegang heeft gehad tot welke resources. Ondersteunende tools daarvoor zijn beperkt leverbaar.

Nr	Welk probleem kan worden opgelost met AM-methode:	DAC	RBAC	MAC	ABAC	AG
1	Need to know dilemma van een strikt ingeregeld rollenmodel	√	-	nvt	nvt	nvt
2	Definiëren toegangsrechten is een moeizaam en langdurig proces	-	-	√	√	nvt
3	Samenhang van registraties voor IdM en AM ontbreekt	-	√	√	√	nvt
4	Management heeft geen overzicht in verstrekte toegangsrechten	√	√	√	√	√
5	Management is niet adequaat voor verlenen/ intrekken van rechten	-	-	√	√	√
6	Ongewenste toegang tot gegevens wordt niet opgemerkt	-	-	√	-	√
7	Aantal wijzigingen te groot voor handmatig aanbrengen	-	√	√	√	√
8	Toegangsrechten worden niet tijdig ingetrokken	-	√	√	√	√

DAC geeft de eigenaar van het object rechtstreeks invloed op wie toegangsrechten krijgt tot de applicatie. Dit is voor systemen met gevoelige informatie een pluspunt. Een arbeidsintensieve methode, waarvan de beheerinspanning exponentieel toeneemt bij het groeien van het aantal objecten en subjecten. Problemen 4 t/m 8 kunnen worden opgelost in combinatie met AG.

RBAC: Een doelmatig ingericht RBAC-systeem vereenvoudigt het toekennen en intrekken van autorisaties aanzienlijk. Voorwaarde van succes met RBAC is beperking van het aantal rollen. Richtgetal: 100 rollen voor organisaties van 5000 medewerkers. Soms moeten daarvoor compromissen gesloten worden, die tegen het ‘need-to-know’ principe ingaan. Een nadeel van RBAC is het arbeidsintensieve proces voor het bepalen van rollen. Dit kan worden versneld door *rolemining* toe te passen. Een ander nadeel is dat vooral oudere systemen geen RBAC ondersteunen, waardoor er procedures nodig zijn voor uitzonderingen.

MAC biedt oplossingen voor alle generieke Access management problemen, maar wordt vanwege de vergaande consequenties voor organisatie en techniek slechts beperkt toegepast. Security Enhanced Linux (SE-Linux) is speciaal ontwikkeld voor MAC en biedt goede kansen voor de toekomstige implementaties. De aanpassingen die in de Linux-kernel nodig zijn om SE-Linux te kunnen draaien, zijn in de bekende distributies geïmplementeerd.

ABAC is een technologie gebaseerd op SAML om DAC, RBAC of MAC mee te kunnen *implementeren*. Het is ontwikkeld voor een omgeving, waar de eigenaar van het object de identiteit van het subject niet (exact) kent en is bedoeld voor webservices en internet toepassingen. ABAC is door toepassing van niet-bedrijfsgebonden attributen conventies tevens geschikt voor federatieve toepassingen. Voor ABAC geldt ook een beperkte ondersteuning van bestaande en oudere IT-platformen.

AG is geen Access management, maar een *aanvulling* daarop. Het is een relatief nieuwe aanpak en technologie. AG is ontwikkeld om *alle* gangbare Access Control methoden eenvoudig te kunnen monitoren, gericht op het oplossen van problemen 4 t/m 8. Alvorens vanuit een bestaande situatie met DAC te kiezen voor RBAC, dient aanvulling met AG serieus te worden overwogen.

Gerelateerde patronen

Thema Identity & Access Management, Identity Management en Federated IdM & AM

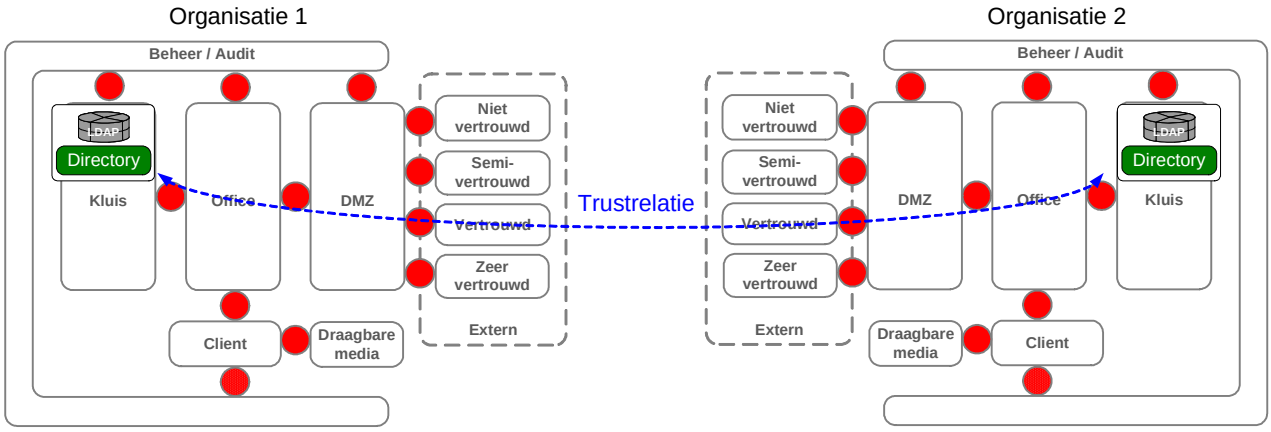
17. Federatie van Identity Management

Criteria

Vertrouwelijkheid, Integriteit

Context

Organisaties gaan steeds meer samenwerken en willen daarbij externe of interne gebruikers toegang bieden tot IT-middelen. Dit gebeurt al dan niet in combinatie met SSO (Single Sign-On). Ondersteuning van gezamenlijk identiteitengebruik wordt geregeld met *Federated Identity Management*.



Organisaties die identiteiten uitwisselen

Succesvolle implementatie van *federatie* van identiteiten biedt organisaties kansen, maar ook bedreigingen. De kansen zijn:

a) Mogelijkheden voor nieuwe efficiënte vormen van bedrijfsvoering
b) Verhogen van gebruikerstevredenheid en imago
c) Terugdringen van kosten en risico's
d) Integratie met toepassingen van partnerorganisaties

Wanneer de verschillen in volwassenheid van IT-beheer en IT-voorzieningen echter groot zijn, dan dreigt het tegengestelde resultaat van kans 1, 2 en 3 te gebeuren.

Probleem

Problemen verbonden aan het wederzijds kunnen benaderen van gegevens van partners onderling, zijn te relateren aan de volgende thema's:

1. **Samenwerking**. Om elkaars identiteiten te kunnen gebruiken moeten strategische keuzes worden gemaakt. Gebruiken we identiteitsgegevens *van partners* of bieden we partner(s) juist *onze* identiteitsgegevens aan?
2. **Vertrouwen**. Hoe kunnen organisaties identiteitsinformatie uitwisselen met partners, om real-time sessies en transacties betrouwbaar te laten verlopen, met behoud van hun eigen *beveiligingsniveau*?
3. **Fusie**. Het samenvoegen van grootschalige infrastructuren en informatiesystemen van verschillende organisaties blijkt in de praktijk *extreem complex*. Oorzaak is dat organisaties in de informatieverwerking en de keuzes van standaarden autonoom zijn gegroeid tot het moment dat besloten wordt om te fuseren. Knelpunten zijn verschillen in toegepaste standaarden, formulering van attributen etc.
4. **SaaS**. Voor gebruikers van organisaties die "Software as a Service" afnemen is het niet aanvaardbaar dat ze voor *elke nieuwe service een ander gebruikersaccount* nodig hebben. (koppeling van SaaS leverancier met IAM processen van de klant is noodzakelijk).

Oplossing

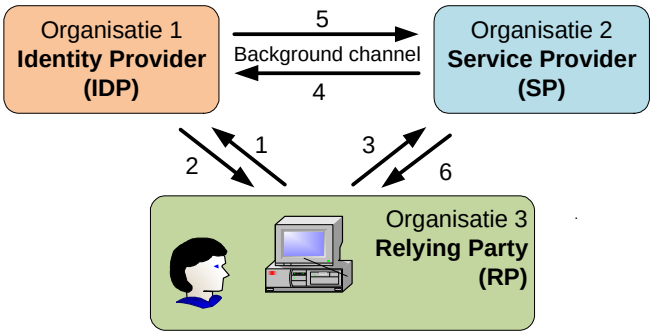
Samenwerken met identiteiten dwingt organisaties tot de volgende strategische keuzes:

1. Identiteiten te ***centraliseren*** in één centrale IdM store voor alle samenwerkende organisaties óf
2. Identiteiten ***uit te wisselen***, met behoud van de eigen IdM.

Het principe voor centraliseren van identiteiten tussen organisaties is geschetst in onderstaande figuur. Minimaal zijn er twee organisaties (of onderdelen van organisaties) betrokken in een federatie.

Eén van de organisaties heeft de rol van Identity Provider (IDP), waarmee dit de federatievariant is met één centrale IdM, uitgevoerd door de IDP. In dit voorbeeld is dat organisatie 1.

De IDP geniet van de andere organisaties RP (Relying Party's) het vertrouwen voor adequaat identiteitenbeheer. Organisatie 2 vervult hier enkel de rol van Service Provider (SP) voor de gebruiker(s) van beide organisaties, bijvoorbeeld voor een SaaS applicatie, maar die rol had net zo goed tevens door organisatie 1 vervuld kunnen worden. In een federatieve 'wolk' kan immers elke organisatie fungeren als service provider. Organisatie 3 is een RP, die enkel identiteiten afneemt van de IDP en IT-services van de SP.



Federatie met centrale IdM in de vorm van een IDP

De toegang tot services verloopt bij federatie steeds in de volgende 6 stappen:

1. Gebruiker (subject) authenticeert zich bij de identity provider.
2. IDP geeft een 'identity-assertion' bericht (een soort ticket) terug aan de gebruiker.
3. Gebruiker vraagt op basis van de uitgegeven identity-assertion de SP om content.
4. SP vraagt IDP om identiteitsgegevens op basis van de assertion.
5. IDP geeft de SP de identiteitsgegevens.
6. SP controleert of de identiteit geautoriseerd is en geeft de gebruiker toegang tot resources.

In plaats van de communicatie (4) en (5) via het z.g. *background channel,* te laten lopen, kan deze communicatie ook indirect via de gebruiker (RP). Voordeel hiervan is *reductie van complexiteit* omdat er dan geen extra communicatiekanaal nodig is. Om de identiteits/autorisatie gegevens in die opzet te beschermen, wordt encryptie of elektronische handtekeningen toegepast zoals gebeurt bij SAML en Kerberos.

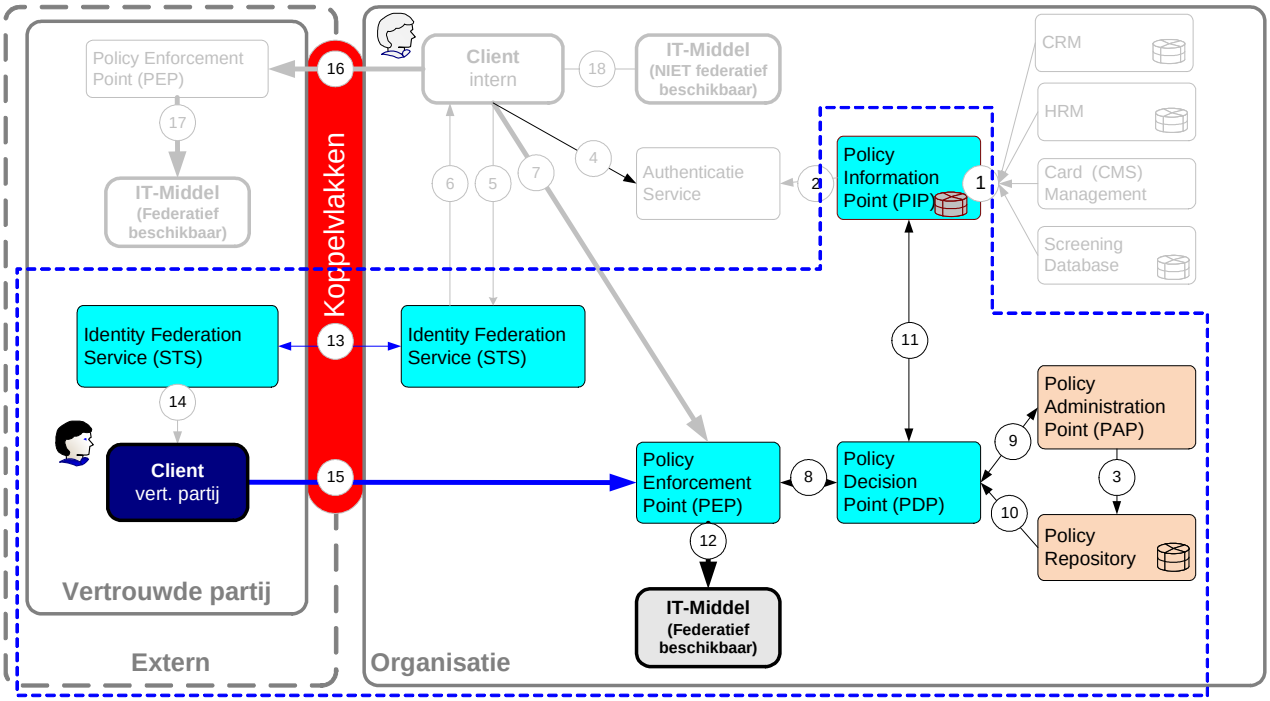
Federatie met uitwisseling van identiteiten en behoud van eigen IdM.

Onderstaande figuur schetst een eenvoudige architectuur, waarin medewerkers van een vertrouwde *partnerorganisatie* (federatieve) toegang kunnen krijgen tot een IT-middel van de eigen organisatie. Er is hier geen sprake van een seperate IDP en SP. Dit is de federatievariant, waarbij de organisaties identiteiten met elkaar uitwisselen. De organisaties zijn hier wederzijds zowel IDP als SP.

Om dit te bewerkstelligen, wordt er eerst een *System To System* (STS) vertrouwensrelatie (trust) gedefinieerd tussen de Identity Federation Service van de Organisatie en de Identity Federation Service van de partner.

In dat kader kunnen bijvoorbeeld afspraken gemaakt worden over (de betrouwbaarheid van) de te hanteren authenticatiemiddelen. De te hanteren betrouwbaarheidsniveaus zijn afhankelijk van de aard van de ontsloten dienst. De trust kan bijvoorbeeld worden gelegd door het Public Key Certificaat van de Identity Provider van de vertrouwde partij als vertrouwde bron op te nemen in de Federation Service van de eigen organisatie (pijl 13).

De medewerker van de vertrouwde partij authenticeert zich bij zijn eigen authenticatie service met zijn eigen authenticatiemiddel (niet afgebeeld). Voor de authenticatie kan gebruik gemaakt worden van standaard authenticatiemiddelen zoals voor de overheid bijvoorbeeld DigiD en eHerkenning.

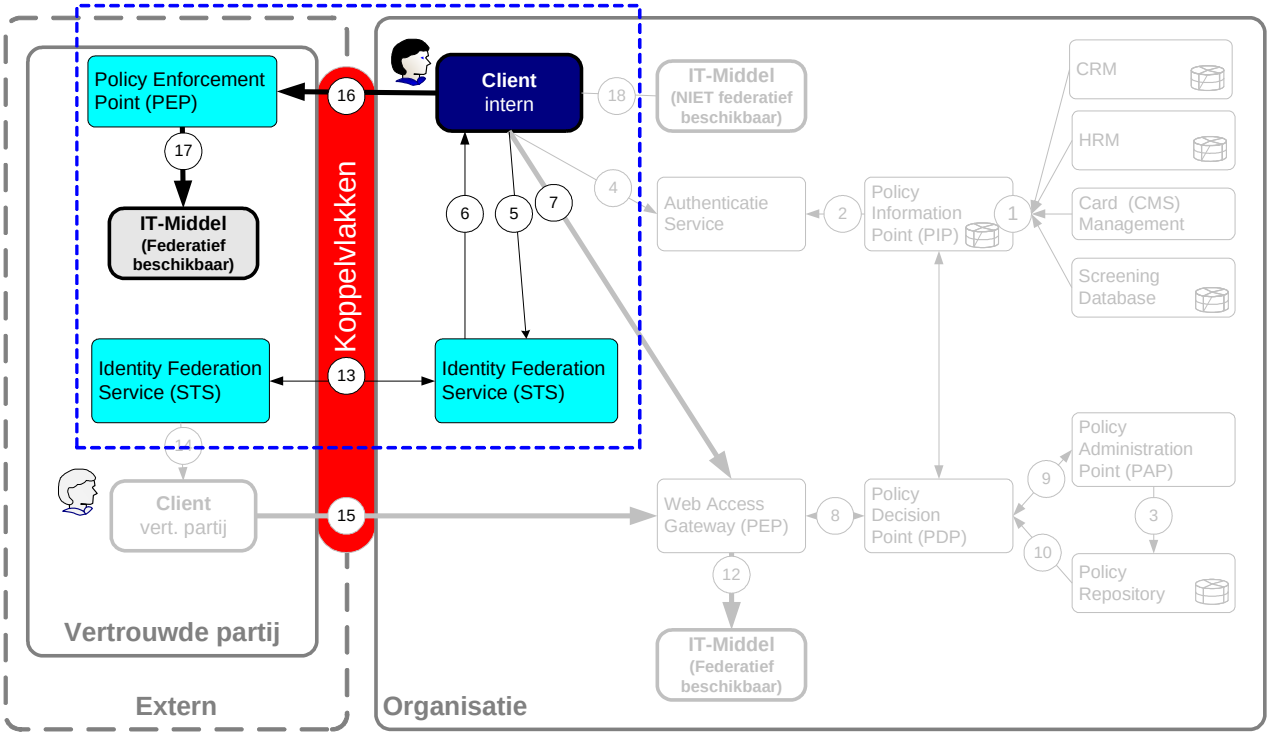


Federatieve toegang van de partner tot resources van de eigen organisatie

Op het moment dat de medewerker van de vertrouwde partij een IT-middel van de Organisatie wil gebruiken, genereert de Identity Federation Service van de vertrouwde partij een SAML-token waarmee de gebruiker toegang kan krijgen tot het middel van de partnerorganisatie. (pijl 14 en 15). Het Policy Enforcement Point vraagt vervolgens aan het Policy Decision Point of de toegang mag worden verleend (pijlen 8 t/m 11) en verleent vervolgens toegang (pijl12).

Federatieve toegang van eigen organisatie tot resources van een vertrouwde partner.

Ook hier wordt er eerst een vertrouwensrelatie (“Trust”) gedefinieerd tussen de Identity Federation Service van de organisatie en de Identity Federation Service van de vertrouwde partner. Deze trust wordt gelegd door het Public Key Certificaat van de Identity Provider van de Organisatie als vertrouwde bron op te nemen in de Federation Service van de vertrouwde partij (pijl 13).



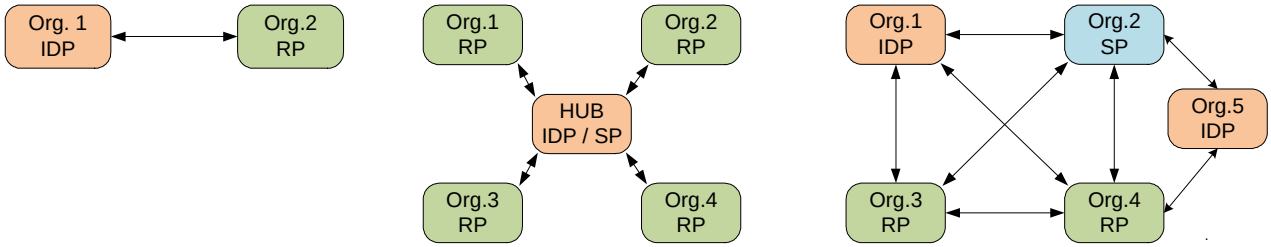
Federatieve toegang eigen organisatie tot de vertrouwde partner

De (geauthenticeerde) medewerker van de organisatie vraagt bij de Identity Federation Service een ("SAML") token aan voor het benaderen van IT-middel (pijlen 5 en 6). Met dit token verleent de organisatie haar medewerkers toegang tot IT-middelen van de vertrouwde partij (pijlen 16 en 17).

Basistopologiën voor federatie

Onderstaande figuur schetst drie basistopologieën voor federatie van identiteiten, ieder met zijn eigen karakteristieken en beperkingen.

1. In een Point-to-point topologie wisselen twee of meer organisaties identity assertions direct uit. Het aantal vertrouwensdomeinen (trust domains T) neemt echter snel toe: T = n * (n-1)/2, waarbij *n* het aantal trust domains is. Het opzetten en beheren van een trustdomain is kostbaar, zodat dit alleen een acceptabele oplossing is voor kleine aantallen deelnemende organisaties.
2. In een HUB-topologie fungeert de IDP als sterpunt. Organisaties (Relying Party's) communiceren altijd via de hub. Voordeel van deze oplossing is de *eenvoud*. Belangrijke nadelen zijn dat slechts één organisatie Identity informatie in beheer heeft en de kwetsbaarheid voor de uitval van de centrale hub (single point of failure).
3. Een Netwerktopologie maakt federatie mogelijk voor grote aantallen organisaties. De federatieve configuratie kan meerdere hubs bevatten. Voordelen zijn dat organisaties hun identity informatie zelf veilig kunnen stellen en dat niet alle netwerkcommunicatie direct hoeft te verlopen. Er kunnen in het netwerk een aantal supernodes zijn ingericht om het aantal interconnecties en te beheren trustrelaties te beperken. Nadeel van deze topologie is complexiteit en formele afstemming van Id's in het kader van de Wet Bescherming Persoonsgegevens (WBP).



Point to point topologie | Hub topologie | Netwerk topologie

Basistopologieën voor federatie met centrale IdM

Afwegingen

Organisaties die identiteiten willen delen moeten de volgende vragen meenemen in hun afweging:

- Naleving: Welke wet- en regelgeving is voor wie van toepassing? Welke aansprakelijkheid is van toepassing in het geval van beveiligingsincidenten? Welke privacy regels zijn van toepassing?
- Organisatiestructuur: Op welke wijze wordt IT bestuurd in de organisatie waarmee samengewerkt moet worden? Centraal- of decentraal? Wat is het niveau van autonomie tussen de verschillende eenheden van het betreffende concern waarmee identiteiten gedeeld worden? Welke rol spelen functionele, regionale of politieke verschillen tussen de aangesloten organisaties?
- Eigenaarschap en beheer van Id-gegevens: Wie is de bewerker van Id-gegevens en waar wordt beheer van Id- gegevens belegd?
- Bestaande applicaties: Er bestaan verschillende standaarden voor federatie van identiteiten. Sommige standaarden werken samen, anderen niet. Moeten applicaties en infrastructuur worden aangepast?
- Volwassenheid van partners: De volwassenheid van organisaties op de relevante gebieden heeft een grote impact op de resultaten die bereikt kunnen worden t.a.v. van federatie van identiteiten. Wat is de volwassenheid van de procesvoering? Voorbeelden daarvan zijn: Is risicomanagement ingevoerd? Hoe zit het met de naleving van IB-beleid? Hoe volwassen zijn de IT voorzieningen?
- Ontvlechting: Organisaties die (overwegen te) fuseren moeten strategisch vooruitkijken naar een mogelijke *ontvlechting* van complexe IdM en AM infrastructuur oplossingen.

Voorbeelden

Een aantal voorbeelden van Federatieve IdM diensten zijn:

- DigiD, de dienst voor IdM voor identificatie van de Nederlandse burger voor de e-Overheid.
- eHerkenning, de dienst voor identificatie van personen in de relatie tussen de e-Overheid en organisaties.
- EduRoam: internationaal werkende dienst voor Federated identity management binnen het hoger onderwijs.

Implicaties

De volgende algemene architectuurprincipes zijn van invloed op het ontwerp en de acceptatie van federatie implementaties:

- Mate van autonomie: Organisaties die niet afhankelijk willen zijn van andere organisaties zullen bij voorkeur niet een partner als identityprovider willen laten fungeren.
- Technische volwassenheid: Organisaties die beproefde technologie eisen voor hun bedrijfsvoering, zullen de relatieve onvolwassenheid van federatie maar moeizaam kunnen accepteren. Technieken voor provisioning en uitwisseling van attributen bij federatie van identiteiten zijn nog volop in ontwikkeling.
- Eigenaarschap, uitvoering, besturing en outsourcing: Federatie werkt als outsourcing. Federatie impliceert het opgeven van een zeker niveau van autonomie op besturing van identiteitenbeheer. Dit houdt in, dat je nog steeds zelf identiteitenbeheer uitvoert, maar afspraken maakt over toegang, waarbij je besluit om gebruikers van partnerorganisaties *niet* in je eigen identiteitenbeheer op te nemen!
- Doorbelasting: Federatie van identiteiten kan het terugverdienen van IdM voorzieningen versnellen. Voor interne doorbelasting van IdM kan nu tevens een extern rekenmodel worden benut. Dit kan zowel positief als negatief uitvallen, afhankelijk van de afspraken die gemaakt zijn met de partners.

Gerelateerde patronen

Identity Management

Standaarden

- SAML 2.0 is verreweg de meest breed gedragen Federated IdM-standaard, gelet op leveranciersproducten, ondersteuning van providers en eisen van gebruikers. Voor de helft van de implementaties worden Open Source producten toegepast.
- XACML: eXtensible Access Control Markup Language. Dit is een *taal* voor het uitdrukken van regels voor toegangsverlening. Het definieert de gebruikte begrippen en bevat modellen en een beschrijving van architectuurcomponenten, waarop de modellen in het thema Logische Toegang van dit document zijn gebaseerd.

18. Single Sign-On (SSO)

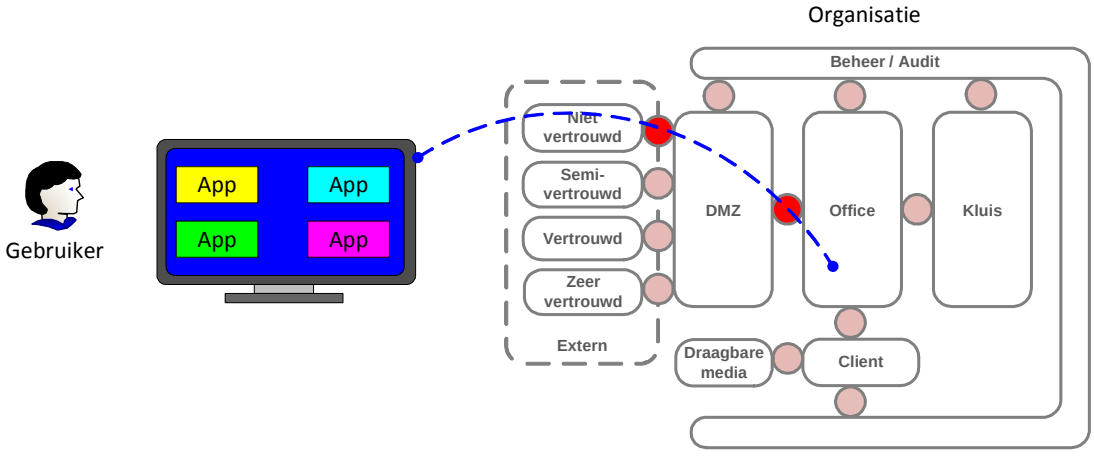
Criteria

Vertrouwelijkheid

Context

Bedrijfsprocessen worden door een toenemend aantal IT-systemen ondersteund. Ook het aantal diensten dat via het Internet wordt aangeboden krijgt een steeds grotere omvang. Bij veel van dergelijke IT-systemen en diensten moet zekerheid bestaan over de identiteit van de gebruiker en wordt geëist dat de gebruiker zich authenticeert. Het aantal momenten dat een gebruiker zich moet authenticeren neemt daarmee sterk toe:

- Binnen organisaties, waar medewerkers een scala aan bestaande systemen moeten bedienen, komt het voor dat ze soms wel 10 keer of vaker op een dag moeten aanloggen, waarbij tevens verschillende gebruikersnamen en wachtwoorden ingevoerd moeten worden.
- Bij initiële gebruikerstests van mijn.overheid.nl kwam vaak naar voren dat gebruikers niet gemakkelijk konden schakelen tussen aangeboden overheidsproducten en –diensten van de aangesloten organisaties en telkens opnieuw moesten inloggen.



Single Sign-On

Probleem

1. **Meerdere keren inloggen** voor verschillende diensten bij één en dezelfde organisatie.
2. **Opschrijven wachtwoorden**
3. **Beveiligingsincidenten,** door verwarring wachtwoordgebruik: verschillende ww conventies etc.

Oplossing

Voor probleem 1: Door te zorgen dat met één keer inloggen een reeks van diensten beschikbaar komt, is voor gebruikers een van de grootste ergernissen en drempels weggenomen. Dit ‘eenmalig aanmelden’ voor toegang tot meerdere systemen of diensten heet in vaktermen single sign-on (SSO).

Als de gebruiker vervolgens uitlogt op één van deze systemen of diensten, dan is zijn sessie bij zowel deze als bij de overige beëindigd (single sign-off).

Voor probleem 2: Met behulp van *federatie* van identiteitsinformatie wordt de ‘noodzaak’ van het noteren van wachtwoorden of pincodes binnen organisaties voorkomen.

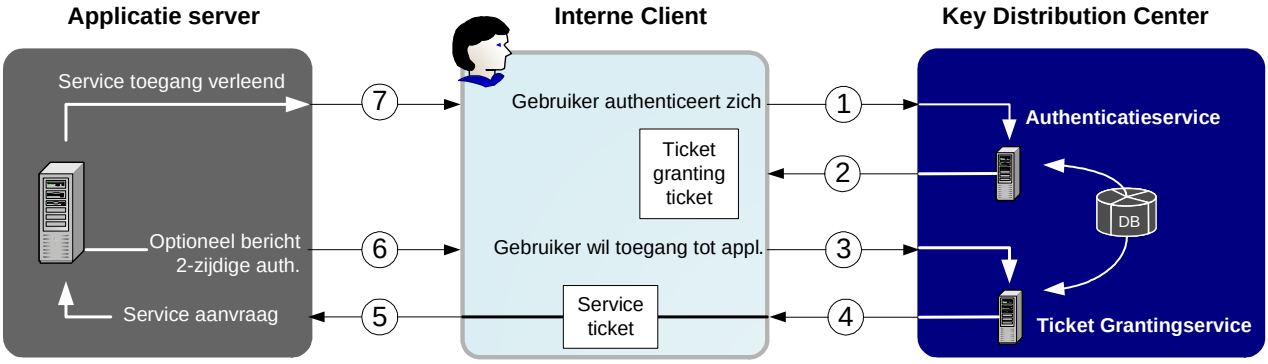
Voor probleem 3: Bij SSO is sprake van het ‘externaliseren’ van de authenticatie. Dat betekent dat de authenticatie door centrale componenten *buiten* de applicatie wordt afgehandeld. Deze centrale componenten kunnen binnen de voor die applicatie verantwoordelijke organisatie gelokaliseerd zijn of daarbuiten bij een identity provider. Op deze wijze kunnen verschillen in conventies en syntax van wachtwoorden voor BackOffice systemen aan de gebruikerskant worden vermeden.

Bij de onderstaande oplossingen wordt onderscheid gemaakt tussen SSO voor interne gebruikers binnen een organisatie, ‘interne SSO’, en SSO voor gebruikers die toegang willen tot diensten van een of meerdere externe organisaties, ‘externe SSO’.

Interne SSO met Kerberos

Een veel toegepaste en betrouwbare techniek voor interne SSO is Kerberos. Kerberos levert authenticatie (oorspronkelijk) op basis van symmetrische encryptie. SSO wordt gerealiseerd door het toepassen van zogenaamde tickets (= een set vercijferde gegevens). Een gebruiker authenticeert zich één maal, bijvoorbeeld met een wachtwoord en krijgt daarvoor een *Ticket granting ticket* met een bepaalde geldigheidsduur. Op basis van dit granting ticket, kunnen zonder tussenkomst van de gebruiker *Servicetickets* worden toegekend, waarmee automatisch op applicatie servers kan worden ingelogd. Hiermee is SSO gerealiseerd totdat het Ticket granting ticket verlopen is (bijvoorbeeld na 8 uur). Autorisatie, ofwel “wat mag de gebruiker op die server of binnen die applicatie?”, is geen onderdeel van het Kerberos protocol.

De centrale component in een Kerberos omgeving is het Key Distribution Center (KDC) waarin de Authenticatie Server de authenticatie van de client verzorgt en de Ticket Granting Server de tickets levert voor authenticatie van de client aan de applicatie servers. Sleutels, zoals voor de beveiliging met symmetrische encryptie van de berichtenuitwisseling, zijn in de Database opgeslagen.



Interne SSO met Kerberos

Na inloggen door de gebruiker met bijvoorbeeld gebruikersnaam/wachtwoord op de client worden de volgende stappen (op hoofdlijnen) doorlopen:

1. De client vraagt een *Ticket granting ticket* aan bij de authenticatieservice.
2. De authenticatieservice identificeert de gebruiker en stuurt een *Ticket granting ticket* (de master ticket) naar de client waar het tijdelijk (afhankelijk van de geldigheidsduur maar uiterlijk totdat de gebruiker uitlogt) wordt opgeslagen.
3. Zodra een client toegang wil tot een bepaalde applicatieservice, wordt hiervoor een *Service ticket* aangevraagd. Omdat hiervoor het opgeslagen ticket granting ticket gebruikt kan worden hoeft de gebruiker zich niet opnieuw te authenticeren, waarmee SSO is gerealiseerd.
4. De *ticket granting server* stuurt een ticket om toegang te krijgen tot de applicatie server.
5. De client stuurt de *Serviceticket* naar de *applicatie server* om toegang te krijgen.
6. Optioneel bericht voor authenticatie van de applicatie server door de client (wederzijdse authenticatie).
7. Gebruiker krijgt toegang tot de gevraagde applicatieservice.

Voor de eerste twee berichten wordt de hash van het gebruikerswachtwoord als encryptiesleutel gebruikt, die ook bekend moet zijn bij het KDC en op basis waarvan de authenticatie van de gebruiker plaatsvindt. Daarna wordt een sessiesleutel toegepast voor de beveiliging van de berichten.

Dit mechanisme biedt alleen SSO voor services met hetzelfde beveiligingsniveau. Als gebruikers inloggen op services met een hoger beveiligingsniveau, dan moeten zij hiervoor apart inloggen, of inloggen met een authenticatiemiddel dat voor de verschillende niveaus geschikt is. Als het beveiligingsbeleid verbiedt dat een gebruiker tegelijk op verschillende niveaus is ingelogd, dan zijn er aparte Kerberos sessies nodig.

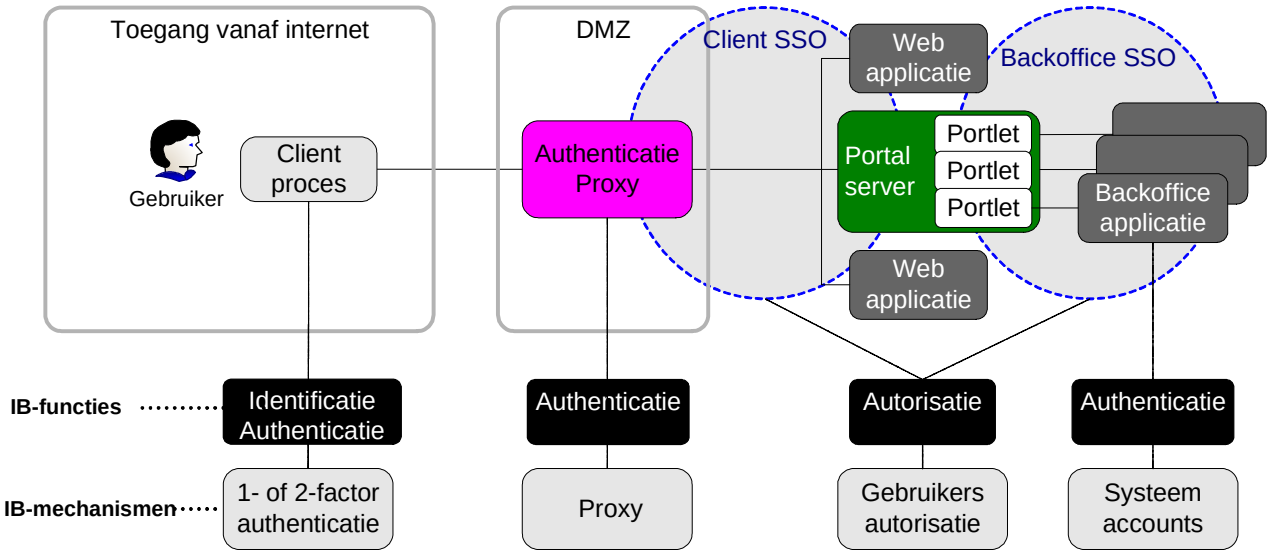
Applicaties kunnen Kerberos integreren via de standaard GSS-API. Deze techniek wordt door MS-*Directory Services* vaak toegepast voor het authenticatiedeel.

Een client kan ook toegang krijgen tot applicaties die onder een *ander KDC regiem* vallen, wanneer die KDC en het eigen KDC een vertrouwensrelatie hebben en onderling een symmetrische sleutel hebben afgesproken. De betreffende client vraagt dan bij zijn eigen KDC een *authenticatie service* aan voor een ticket granting ticket van de andere KDC. Hiervoor wordt de onderlinge KDC sleutel gebruikt. Daarna verloopt het proces op dezelfde manier als bij toegang tot de eigen applicaties, maar nu binnen het andere regiem. Op deze wijze kan een netwerk van KDC’s gecreëerd worden.

Externe SSO

Portaal met SSO-federatie

Met single sign-on functionaliteit tussen client en webapplicatie loggen gebruikers éénmalig in bij een webapplicatie en kunnen vervolgens het portaal benaderen en alle webapplicaties, die behoren tot de groep Client SSO. Het maakt hierbij niet uit of de portaalapplicatie dan wel één van webapplicaties of de authenticerende applicatie is. De BackOffice applicaties zijn vervolgens te benaderen door op het portaal één keer in te loggen.



Portaal met SSO federatie

Wat is er voor nodig?

Voor het inloggen op het portaal is authenticatie vereist, bijvoorbeeld met DigiD voor mijn.overheid.nl. Als aangesloten organisatie die toegang verleent via het portaal dient men zich aan te sluiten bij de SSO-federatie. Dit kan met ieder systeem. De federatie verzorgt vervolgens de gezamenlijke authenticatie.

Authenticatie

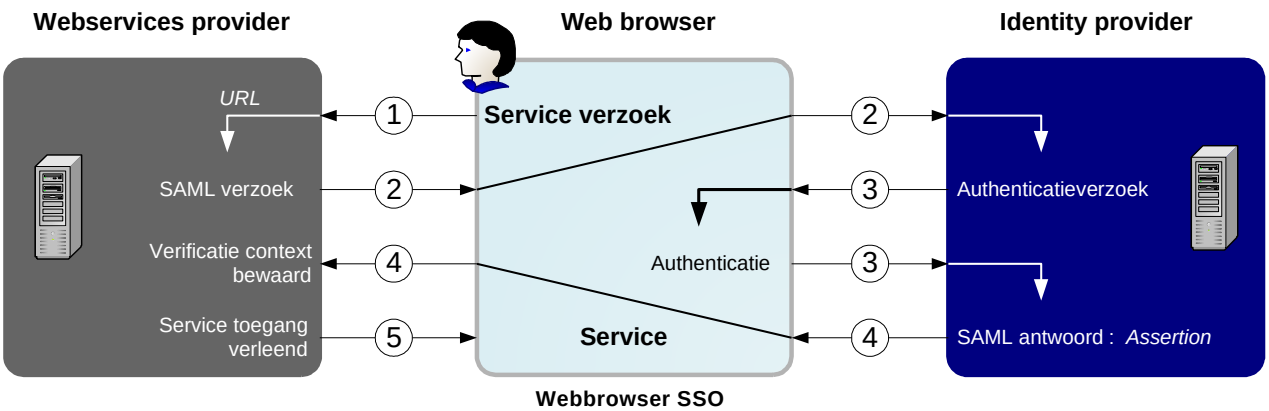
Een gebruiker logt in en authenticeert zich. Zijn gegevens worden door de server van de federatie gecontroleerd en bijgehouden. Deze authenticatie vindt bijvoorbeeld plaats op basisniveau, dat wil zeggen ‘gebruikersnaam en wachtwoord’. Organisaties bepalen zelf welk niveau authenticatie vereist is. Als het authenticatieniveau hoger is dan waarmee de gebruiker is ingelogd, ontvangt deze gebruiker een melding met het verzoek op een hoger niveau in te loggen (bijvoorbeeld met SMS-authenticatie) en wordt in de federatie het hogere inlogniveau geregistreerd.

SSO-federatie

De single sign-on federatie is de gemeenschappelijke factor – de zogenaamde ‘Federatie component’ die de sessies beheert en vaststelt of een partij een sessie kan overnemen.

Webbrowser SSO

Een provider van webservices kan de SSO authenticatie overlaten aan een derde partij, een identity provider, onder voorwaarde dat daarmee een vertrouwensrelatie bestaat. De webservice provider (“relying party”) vertrouwt de identity provider. Dit is vooral aantrekkelijk voor de eindgebruiker wanneer die al bij die vertrouwde identity provider is geregistreerd. Een dergelijke oplossing waarbij vanuit een webbrowser toegang gevraagd wordt tot de webservices van de provider is geschetst in onderstaande figuur.



Webbrowser SSO

1. De gebruiker wil toegang tot een webservice van de provider en voert daartoe de URL van de webservice in de webbrowser in. De browser moet daarbij aangeven welke identity provider gebruikt moet worden.
2. Als de gebruiker nog niet al van een andere service gebruik maakt (er is nog geen geldige context van die gebruiker aanwezig) dan dient deze eerst geauthenticeerd te worden. De webservice provider stuurt hiervoor een SAML verzoek naar de webbrowser die geherrouteerd wordt naar de identity provider.
3. De identity provider vraagt de gebruiker zich te authenticeren.
4. Na geldige authenticatie genereert de identity provider een SAML antwoord (de z.g. *Assertion* van de identiteit) en stuurt dat naar de webbrowser die het weer doorstuurt naar de URL van de webservice. De webservice provider verifieert het SAML antwoord (op basis van de public key van de identity provider) en maakt een geldige context voor die gebruiker aan.
5. De webservices provider verleent de gebruiker toegang en herrouteert de webbrowser naar de desbetreffende service.

Als de gebruiker vervolgens een andere service wil toepassen, dan hoeft niet opnieuw te worden ingelogd (single sign-on) omdat er al een geldige context aanwezig is. In het voorbeeld wordt na het verzoek (1) direct de service (5) geleverd. De context wordt ongeldig zodra wordt uitgelogd en de gebruiker krijgt geen toegang meer tot de services (single sign-off) totdat er opnieuw wordt geauthenticeerd.

Afwegingen

- Het gebruik van SSO leidt tot een stapeling van risico's: als het password van de gebruiker in verkeerde handen komt, dan vallen alle rechten die de gebruiker zijn toegekend in verkeerde handen. Dit staat tegenover de risicoverlaging van het opschrijven van wachtwoorden.
- Bij single sign-on moet overwogen worden of één sign-on afdoende is voor alle achterliggende toepassingen.
- SSO wordt gekenmerkt door "eilanden rond grote softwareleveranciers". Binnen één technologie voor applicatieservices (Microsoft, Oracle, Tivoli, CA) is er veel mogelijk, maar bruggen tussen deze werelden en de mogelijkheden voor het aansluiten van 'als standalone' ontwikkelde applicaties zijn vaak onvolwassen. Voor de bruggen tussen de werelden bestaan ontwikkelingen zoals SAML. Voor de standalone applicaties is men afhankelijk van de ontwikkelaar.

Voorbeelden

- Mijn.overheid.nl
- Google.nl, maar ook concurrenten als Amazon en Microsoft Live ID

Implicaties

Single sign-on impliceert standaardisatie van de interfaces naar de achterliggende systemen. Vooral wanneer applicaties draaien op verschillende soorten *applicatieplatformen*, (bijvoorbeeld Microsoft, Oracle, Tivoli en IBM-applicaties) is het realiseren van betrouwbare single sign-on niet eenvoudig.

Met single sign-on krijgt een gebruiker met slechts één gebruikersnaam/wachtwoordcombinatie toegang tot meerdere informatiebronnen. De impact van compromittering van de credentials wordt daarmee evenredig groter wat al snel een reden kan zijn om sterke authenticatie (met token en/of biometrie) toe te passen.

Bij SSO oplossing is sprake van externalisering van authenticatie, dat wil zeggen dat het door een centrale voorziening wordt uitgevoerd in plaats van door elke applicatie afzonderlijk. Om SSO geen single-point-of-failure te laten zijn, dient deze voorziening dubbel te worden uitgevoerd.

Gerelateerde patronen

- Themapatroon Identity & Access Management
- Federated Identity & Access Management

Standaarden

- DigiD API
- SAML 2.0
- Kerberos Network Authentication Service (RFC 4120,), Kerberos GSS-API (RFC 4121)
- Open ID

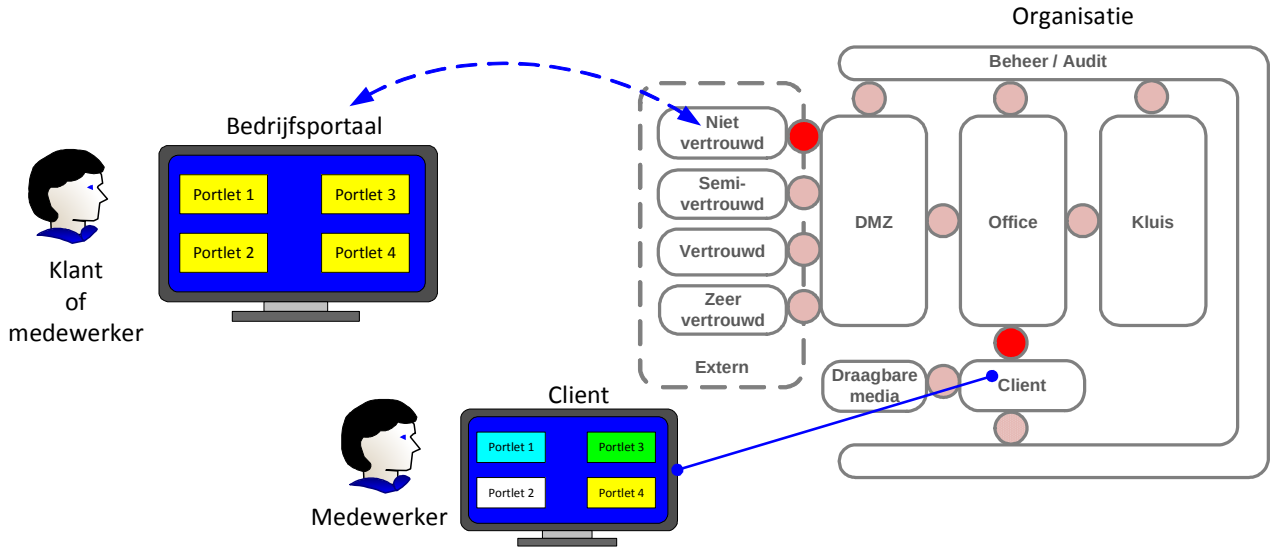
19. Portaal – toegangserver

Criteria

Integriteit, Vertrouwelijkheid

Context

Een *portaal* of portal is een webapplicatie, die eindgebruikers via internet of bedrijfsnetwerken toegang geeft tot zowel toepassingen als gegevens. Er zijn grote organisaties die hun gehele IT-omgeving voor medewerkers ontsluiten via een portaal op het internet! Interne netwerken (LAN) zijn dan 'verleden tijd'. Hieronder een voorbeeld van een klant en medewerker die informatie zoeken op een bedrijfsportaal. Een portaal kan afhankelijk van de toepassing informatie ophalen vanuit verscheidene bronnen. Het portaal kan daarbij de gegevens samenstellen, veredelen (aggregeren) en ze op hetzelfde moment presenteren aan klanten, partners of medewerkers van een organisatie. Een portaal kan informatie uit verschillende databases en applicaties voor een gebruiker toegankelijk maken via vooraf gedefinieerde *portlets*; die in combinatie met elkaar het 'portaal' vormen, afhankelijk van de behoefte en bevoegdheden van de gebruiker. Behalve zoekfuncties bieden portalen toegang tot e-mail, nieuws en prijsinformatie en ontspanning. Voor organisaties bieden portalen een goede mogelijkheid om klanten een consistente 'look and feel' te geven voor de toegang tot applicaties, die voorheen ieder hun eigen toegangsprocedures en 'gezicht' hadden naar eindgebruikers. Een graag geziene functionaliteit van portalen is dat keuzemogelijkheden worden beperkt tot uitsluitend datgene waarvoor gebruikers bevoegd zijn en dat men daarvoor maar één keer hoeft aan te loggen; het z.g. Single Sign-On (zie hiervoor verder het patroon SSO).



Informatievoorziening via een bedrijfsportaal

Probleem

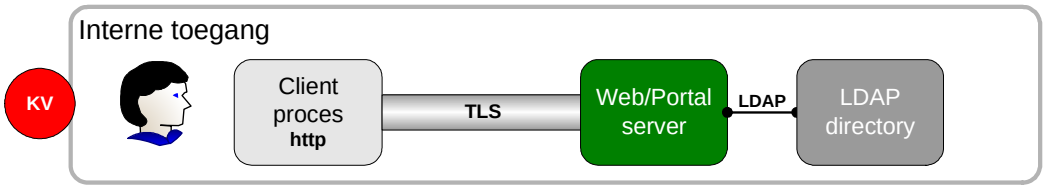
1. **Gevoelig voor inbreuk.** Voor de klant of eindgebruiker fungeert een bedrijfsportaal als de 'voorkant' van de informatieketen, al dan niet toegankelijk via het internet. Hoewel portalen publiek vrij toegankelijke informatie kunnen verschaffen, zal gevoelige informatie pas verstrekt worden na *authenticatie* van de gebruiker. Probleem daarbij is dat Internet netwerk- en berichtenverkeer door de georganiseerde misdaad gemakkelijk op afstand kan worden ingezien, worden gekopieerd of gewijzigd.
2. **Concessies op beveiliging voor laagdrempeligheid.** Een belangrijke eis voor een portaal is een *laagdrempelige* gebruikersinterface, maar vanwege die eis worden er vaak *concessies* gedaan op beveiligingsmaatregelen, waardoor het portaal in de keten een evident kwetsbare schakel vormt voor misbruik en digitale sabotage.
3. **Beperking J2EE Platform beveiliging**. J2EE is ontworpen voor *administratieve* systemen en kan niet in alle gevallen voorkomen dat malicious portlet code het portaal beschadigt of dat gevoelige data ongeautoriseerd kan worden gelezen via een call vanuit andere interne portlets.

Oplossing

De set van benodigde maatregelen voor beveiliging van portalen is samengevat afhankelijk van:

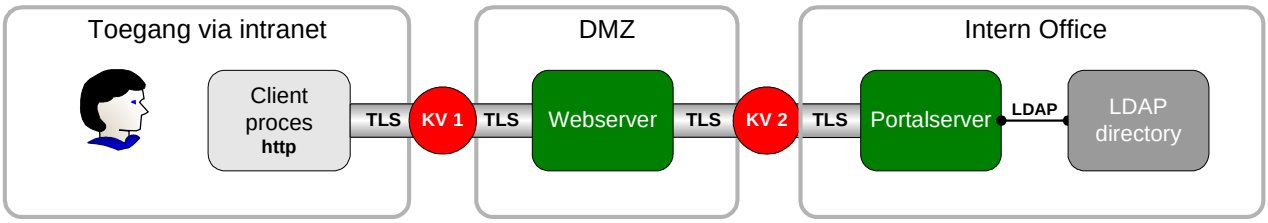
1. **Toegangsketen**: wordt toegang verleend vanuit een intern netwerk, een vertrouwd of semi-vertrouwd intranet of vanuit een niet vertrouwd netwerk zoals het internet.
2. **De aard van acties** die gebruikers van het portaal (klant, partner of medewerker) moeten kunnen doen. Betreft de actie bepaalde publieke informatie raadplegen, vertrouwelijke informatie raadplegen of moeten gebruikers ook transacties kunnen uitvoeren?
3. **Portaal architectuur.** Leveranciersafhankelijke architectuurkeuzes voor de mechanismen van toegang en autorisatieservices. In dit patroon beperken we ons tot generieke oplossingen.

Intern netwerk.
De eenvoudigste portaalconfiguratie is toegang vanuit een beveiligd intern netwerk (LAN). Een voorwaarde hierbij is dat er geen aanvallen te verwachten zijn vanuit dit netwerk. Zowel het portaal als de clientomgeving en de gebruikersgegevens worden beschermd door de firewall KV (Koppelvlak). De clients kunnen direct met het Portalserver communiceren, omdat ze zich in hetzelfde beschermde netwerk bevinden. In dit voorbeeld is de Applicatieserver code en de Portalserver code op dezelfde fysieke machine geïnstalleerd. Alle gebruikersgegevens, zoals autorisaties zijn opgeslagen in de LDAP directory. De netwerkverbinding wordt beveiligd met behulp van TLS-encryptie, waarbij de client zich eenzijdig authenticeert aan de Webserver.



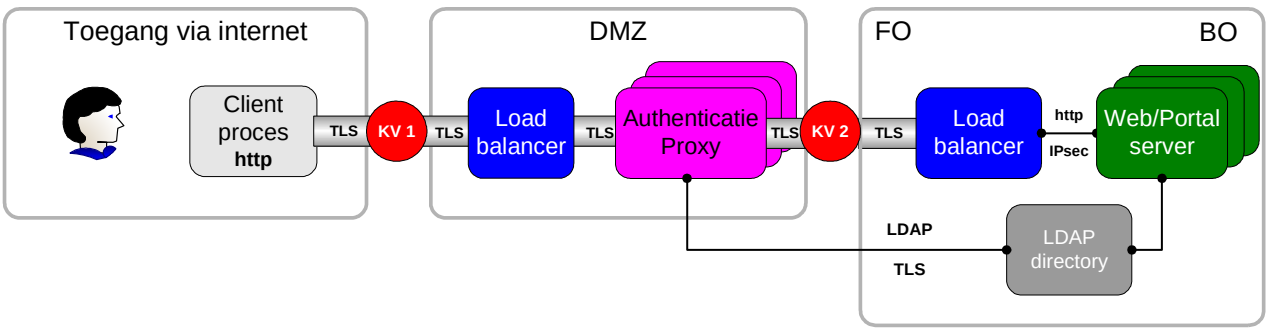
Toegang via het interne bedrijfsnetwerk (LAN)

Intranet.
Wordt toegang wordt verleend tot een portaal via een semi-vertrouwd extern netwerk, dan wordt de Client, Webserver en Portalserver met firewalls gescheiden van elkaar en van de Webserver. Er worden twee TLS verbindingen opgezet voor beveiliging van de communicatie, die de firewalls 1:1 doorlaten.



Toegang via een extern bedrijfsnetwerk voor partners of medewerkers (intranet / WAN)

Internet.
Wanneer toegang tot het portaal wordt verleend vanuit niet vertrouwde netwerken zoals het internet, dan wordt een afzonderlijke authenticatie component toegepast waarmee de gebruiker zich authenticeert. Vervolgens wordt toegang verleend naar de Web/portalserver. Hiervoor wordt een Authenticatie proxy gebruikt, ook wel Reverse proxy genoemd. De LDAP directory verstrekt gebruikersgegevens aan de proxy, de Web/Portal server en de andere systemen in de Front- en BackOffice. Load balancers worden gebruikt voor het verdelen van de gegevensstromen over de verschillende systemen.



Toegang via publieke netwerken (internet)

Per functieblok is in onderstaande tabel aangegeven welke IB-functies werkzaam zijn in bovenstaande portal ketens. De koppelvlakken zijn standaard koppelvlakken, zoals beschreven in aangegeven patronen. Dat geldt ook voor de LDAP directory en het clientproces.

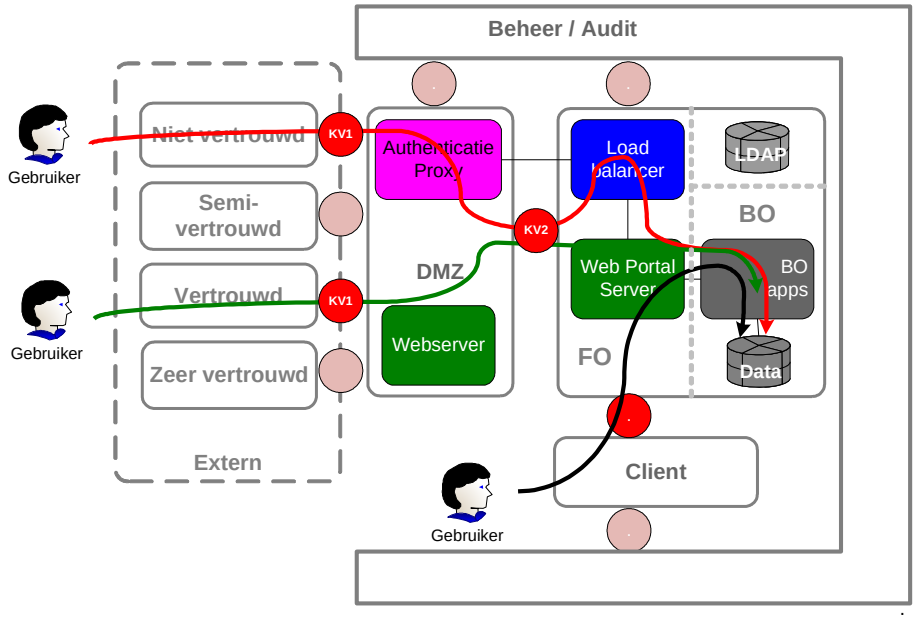
Functieblok	Continuïteit	Zonering	Identificatie Authenticatie	Autorisatie	Vaststellen gebeurtenissen	Controleren Alarmering	Systeem integriteit
Client proces	nvt	Beginpunt SSL tunnel	Username / ww 2-factor (extern)	nvt	nvt	nvt	Handhaven van IB-functies
	zie verder beschouwingsmodel: **Client**						
Koppelvlak 1	Intern-portaal via LAN: zie Patroon **Interne koppelvlakken**; koppelvak 2 en 9 Extern- portaal via Intranet: zie beschouwingsmodel: **Kanaal Vertrouwd** koppelvak V Extern **-**portaal via Internet: zie beschouwingsmodel: **Kanaal Niet vertrouwd** koppelvlak Ou en Oi						
Load balancer	-Dubbele units -Dubbele PSU	nvt	nvt	nvt	-Vollopen queue -IB-events	Drempelwaarde systeem - resources	-Hardening -Syst.patches
Authent. proxy	Dubbele units	Ongebruikte poorten uitgeschakeld of verwijderd	-Pincode opstart -Systeem ww	Systeem-autorisaties	-Syslog -IB-events	Drempelwaarde systeem - resources	-Hardening -Code scan/hash -OS-patches -Vulnerabilityscan
Koppelvlak 2	zie Patroon **Interne koppelvlakken**; koppelvak 2, 6 en 9						
Web-/ Portalserver	-Dubbele units -Dubbele PSU	- Sandboxing	Ww gescheiden van toepassing gegevens opgeslagen	Temp-bestanden alleen voor systeembeheer toegankelijk	-Bewaartermijn -Vollopen media -Rollback	Vollopen queues en media	Foutloos berichten verkeer en opslag RAID
LDAP directory	zie Patronen: **IAM Identity Management** en **Access Management**						

IB functie

IB mechanismen

Maatregelen per functieblok voor portaalketens

In onderstaande figuur zijn drie generieke portal configuraties afgebeeld in de context van één bedrijfsnetwerk. Afhankelijk van het aantal externe gebruikers, kan een extra loadbalancer worden ingezet om de verkeersbelasting over de verschillende authenticatieproxies of webservers in de DMZ te kunnen verdelen.



Drie toegangswegen tot een bedrijfsportaal

Toegang tot gevoelige gegevens

Autorisatie is gebaseerd op authenticatie. Om zeker te zijn dat uitsluitend geautoriseerde gebruikers toegang verleend wordt tot het portaal, moet worden vastgesteld wie de persoon is. Authenticatie is daarom de eerste stap die moet worden uitgevoerd bij iedere aanvraag op de portalserver.

Portal Access Control (PAC) definieert een set van gevoelige activiteiten die een eindgebruiker mag uitvoeren in zijn eigen gedefinieerde portaalomgeving. Deze set van activiteiten is gedefinieerd via de aan de gebruiker verleende autorisaties. Dit kan worden geregeld op basis van rollen, waarbij een set van autorisaties wordt gekoppeld aan een bepaalde rol in de organisatie.

Beveiliging gevoelige handelingen
Gebruikers interacteren met het portaal op allerlei manieren, variërend van het simpel browsen door informatieve pagina's tot complexe handelingen zoals uitvoeren van software-updates, het aanpassen van portlets en bedrijfstransacties. Toegang van bijna elke soort van acties moet worden beperkt tot een groep van geautoriseerde gebruikers. Daarom zijn alle gevoelige handelingen beveiligd door het Portal Acces Control component, vergelijkbaar met Access Control voor elke standaard applicatie.

Portlet beveiliging
Portlets, of portal-applets zijn visuele, dynamische componenten die deel uitmaken van een webpagina van een web-portal. Normaal wanneer een gebruiker vraagt om een gepersonaliseerde webpagina, worden er meerdere portlets aangeroepen die samen de webpagina opbouwen. Een voorbeeld is een nieuwsportaal, dat in enkele pagina's actueel financieel nieuws geeft, beursnieuws en de meest recente informatie over voorraden geeft die van belang zijn voor de eindgebruiker. Elke component beschikt daarbij over zijn eigen portlet. Portlets zijn gebaseerd op API's, zoals gebruikersprofielen. Wegens het ontbreken van specifieke technische standaarden, leveren portalserver-leveranciers eigen API's voor lokale portal componenten, die een uniforme beveiliging van lokale portlets ingewikkeld maakt.

Een oplossing is de toepassing van Java Virtual Machine (JVM) code, dat draait op de portal/webserver. De Java code volgens de J2EE specificatie, maakt gebruik van de LDAP gebruikersdatabase voor toegang tot de portlets. J2EE Platform beveiliging is echter ontworpen voor administratieve systemen en kan niet in alle gevallen voorkomen dat malicious portlet code het portaal beschadigt of dat gevoelige data ongeautoriseerd kan worden gelezen via een call vanuit andere interne portlets. Daarom moeten portlet-ontwikkelaars aanvullende maatregelen nemen in de vorm van *geprogrammeerde controles* om gevoelige data te beschermen en de betrouwbaarheid van het portaal als geheel te waarborgen.

Verificatie veilige verbinding
Portlets die een beveiligde verbinding vereisen, moeten de garantie krijgen dat de gegevens die ze versturen vertrouwelijk worden behandeld. Als het portaal TLS ondersteunt, dan kunnen portlets een TLS connectie opzetten via een "*start transaction*" link. Echter, het portlet moet wel controleren of de verbinding nog steeds veilig is, wat kan worden gedaan met de '*request.is.Secure()'* methode. Als een portlet request niet via een beveiligde verbinding de portal bereikt, mag het portlet geen vertrouwelijke data versturen naar de aanvrager.

Voorkomen van Cross Site Scripting aanvallen
Omdat portlets rechtstreeks toegang hebben tot de 'markup stream' van de portal/web applicatie, worden ze blootgesteld aan Cross Site Scripting aanvallen net als alle andere webtoepassingen. Daarom is de portlet ontwikkelaar verantwoordelijk voor de juiste codering van alle gegevens voorafgaand aan de 'markup stream'. Dit wordt meestal gedaan met behulp van een *JSTL out tag* vanuit JSP of met behulp van leverancier specifieke commando's voor web applicaties.

Om het risico van schade door aanvallen te verminderen, kan de portal engine zodanig worden geconfigureerd, dat het een aantal basis filteringen uitvoert op de portlet input. De karakters 'kleiner dan' en 'groter dan' worden geconverteerd tot de corresponderende HTML escape sequences. Met deze maatregel worden echter maar een beperkt aantal potentiële kwetsbaarheden opgelost.
Soortgelijke problemen ontstaan ook wanneer een portlet markup van een andere server aggregeert.

WSRP beveiliging
Portalen kunnen Web Services for Remote Portlets (WSRP) protocol ondersteunen. Dit zijn z.g. remote portlets, die gebruikt kunnen worden als lokale portlets onder bepaalde restricties. WSRP wordt gebruikt, wanneer het portaal van een 'klant' (consumer) een verbinding legt met een portal van een 'leverancier' (supplier). Standaard worden WSRP verbindingen niet beveiligd. Er worden geen betrouwbare identiteiten uitgewisseld tussen de klant-leveranciers portalen. Daarom kan een portlet niet terugvallen op de betrouwbare gebruikersgegevens of referenties.

Gepropageerde gebruiker metadata kan worden gebruikt om een *gepersonaliseerde* 'user experience' in te stellen, bijvoorbeeld door informatie over en weer te sturen op basis van de locatie (postcode) in het gebruikersprofiel-window. Echter, deze informatie moet meer als 'hint' worden opgevat voor de identiteit van de gebruiker dan als geverifieerde gebruikers identiteit.

Webserver leveranciers ondersteunen voor deze toepassingen WSRP verbindingen die TLS ondersteunen, zodat man-in-the-middle aanvallen kunnen worden voorkomen.

Afwegingen

Portals, in de vorm van webapplicaties, zijn voor hun type beveiligingsmaatregelen in belangrijke mate afhankelijk van de web-technologie die binnen een organisatie gebruikt wordt en de architectuur die fabrikanten van web- en portal-technologie toepassen. Universele standaarden voor de mechanismen binnen een portaal zijn er nog niet, wat impliceert dat beveiliging van dit type webapplicatie voorlopig nog maatwerk is en dat we moeten kiezen uit wat de fabrikant ons biedt. Als gekozen wordt om zich te beperken tot *marktleiders* van web- en portal technologie, dan zijn er voldoende mechanismen leverbaar om portalen te kunnen beschermen.

Voorbeelden

Bedrijfsportalen van banken, verzekeringsmaatschappijen, reisbureaus en luchthavens.

Implicaties

Koppel portaalbeveiliging aan de binnen een organisatie gebruikte technologie voor webservices.

Train applicatiebouwers op ‘secure programming’ en software testmethodieken, zie [4]. Zorg dat de mechanismen van applicatiecontroles worden gebruikt zoals invoer- en uitvoercontroles.

Controleer portalen en de onderliggende code periodiek op kwetsbaarheden voor inbreuk en ongewenste mobiele code.

Gerelateerde patronen

- Koppelvlak niet vertrouwde derden, semi-vertrouwde derden en interne koppelvlakken
- IAM
- Encryptie

20. Vertrouwd Toegangspad (VTP)

Criteria

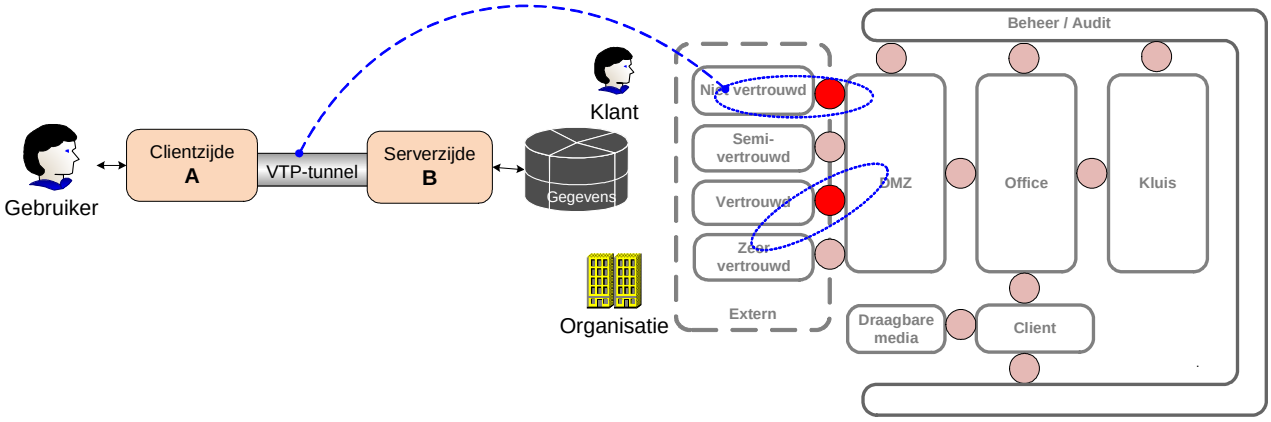
Vertrouwelijkheid, Integriteit

Context

Definitie: Er is sprake van een vertrouwd toegangspad (VTP), wanneer een applicatieproces A vanaf de clientzijde veilig kan communiceren met applicatieproces B aan de serverzijde via een voor invloeden van buitenaf beschermd kanaal dat twee of meer koppelvlakken bevat.

Vertrouwde toegangspaden (VTP) zijn cruciaal voor betrouwbaar datatransport via niet vertrouwde omgevingen zoals het Internet of in situaties waar verschillende datastromen elkaar kunnen beïnvloeden. Onderstaande figuur schetst een dergelijke omgeving. Behalve voor een veilige verbinding naar de buitenwereld vindt het VTP ook zijn toepassingsgebied binnen een organisatie. Voorbeelden zijn de kanalen waarlangs persoons- of financiële gegevens worden verstuurd via een *Intranet*. Een ander toepassingsgebied is communicatie voor het beheer van systemen. Een VTP is zowel voor datatransport naar niet vertrouwde als vertrouwde derden gewenst. Medewerkers die thuis- of vanuit niet-bedrijfslocaties werken, maken altijd contact met bedrijfssystemen via een VTP.

De identificatie van de gebruiker aan het clientproces en de autorisaties van de gebruiker voor proces A en B en de toegangsrechten van de gebruiker tot gegevens zijn hier buiten beschouwing gelaten!



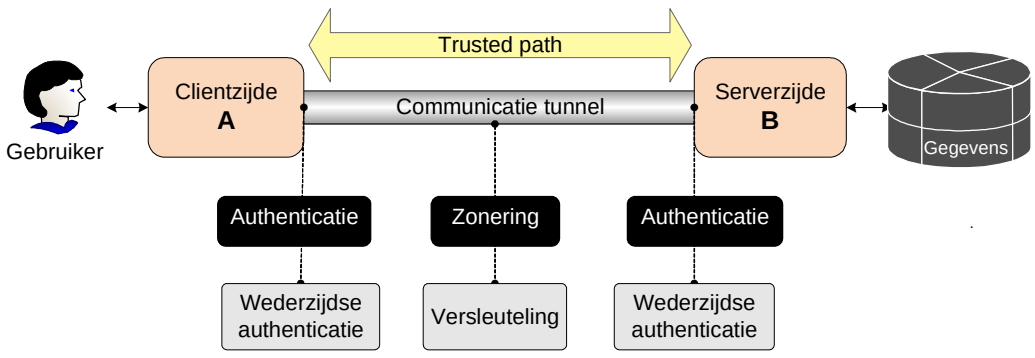
Vertrouwd toegangspad naar een organisatie

Probleem

Als clientproces A via een open verbinding wil communiceren met applicatieproces B, dan kan de communicatie door afluistering negatief kan worden beïnvloed. In die situatie zijn er geen garanties te geven voor de vertrouwelijkheid en integriteit van de gecommuniceerde gegevens.

Oplossing

Door toepassing van de IB-functies: Zonering en (wederzijdse) authenticatie tussen de client en applicatieprocessen aan het begin en eindpunt van het pad. Kort samengevat is een VTP een veilige point-to-point verbinding en wordt in de vakliteratuur ook wel ‘trusted path’ genoemd.



Opbouw van een VTP.

Bovenstaande figuur schetst een eindgebruiker, die via een vertrouwd toegangspad gegevens benadert of uitwisselt. De bescherming die een vertrouwd toegangspad biedt, fungeert als een *tunnel* voor de communicatie tussen twee processen of systemen en moet daarom 'transparant' zijn voor de protocollen die er door heen gaan. Eerst authenticeren clientproces A en applicatieproces B zich aan elkaar, waarna een versleutelde verbinding wordt opgezet voor het transport van de informatie.

De figuur schetst de beveiligingsfuncties die een VTP minimaal moet bevatten om te kunnen functioneren: wederzijdse authenticatie aan de eindpunten van het pad en scheiding van de buitenwereld over de gehele lengte van het pad. Een veel gebruikt mechanisme daarvoor is versleuteling, maar er kunnen ook andere mechanismen worden toegepast, zoals een Closed Usergroup mechanisme van een netwerkaanbieder, gekoppeld aan de zekerheid dat beveiligingsmaatregelen door de leverancier worden nageleefd via TPM (Third Party Mededeling).

Een vertrouwd toegangspad kan in zijn geheel worden verzorgd met standaard protocollen op systeemniveau of op applicatieniveau. Een vertrouwd toegangspad verloopt meestal via een traject met verschillende nodes. Elke node heeft een specifieke functie in de communicatieketen, maar voegt in het geval van een VTP aan de gegevens niets toe. Een VTP kan bijvoorbeeld door een grensbescherming lopen, met behoud van de vertrouwelijkheid.

	IB-Functies				
Functieblok	Zonering	Authenticatie	Vastleggen gebeurtenissen	Controleren Alarmeren	Systeem integriteit
Clientzijde	- Data encryptie - Sessie encryptie - Netwerk encryptie - Lijn encryptie	- wederzijdse authenticatie - 1, 2 of 3-factor - context based aanmelden	- Beheerhandelingen - Verbindingen	- Handhaven IB-functies - Afwijkingen op beleid	- Hardening - Applicatie patch
Toegangspad	- shttp - https - TLS tunnel - IPSec tunnel - Proprietary tunnel - Closed Usergroup	nvt	nvt	nvt	Infrastructuur firmwarepatches
Serverzijde	- Data encryptie - Sessie encryptie - Netwerk encryptie - Lijn encryptie	- wederzijdse authenticatie - 1, 2 of 3-factor - context based controleren	- Beheerhandelingen - Verbindingen	- Handhaven IB-functies - Afwijkingen op beleid	- Hardening - Applicatie patch

IB mechanismen

Overzicht gebruikte IB-mechanismen voor een VTP.

Afwegingen

In deze uitleg worden alleen de IB-functies beschouwd die een bijdrage leveren aan het vertrouwde pad tussen het klantproces A en het applicatieproces B.

Voorbeelden

- Telebankieren
- Telewerken

Zowel voor het bankieren via het internet als voor telewerken via internet, is een veilige verbinding vanaf de klant naar de betreffende organisatie een eerste vereiste. In beide situaties wordt een VTP opgezet tussen het clientproces van de klant en het ontvangende applicatieproces van een organisatie. De mechanismen voor wederzijdse authenticatie verschillen van organisatie tot organisatie, maar meestal wordt 2-factor authenticatie toegepast op basis van tokens.

Implicaties

Het kunnen opzetten van een VTP vereist, dat aan beide uiteinden van het pad dezelfde standaarden worden gehanteerd voor communicatieprotocollen, doorvoersnelheden en het minimum beveiligingsniveau

Gerelateerde patronen

- Koppelvlakken
- Generieke netwerkconfiguratie
- Draadloze netwerken

21. Thema encryptie

Leeswijzer
Dit is een themapatroon, dat voor de algemene probleemstelling van vertrouwelijk opslaan en uitwisselen van gegevens een oplossing biedt. Onderliggende patronen bieden oplossingen voor specifieke soorten van versleuteling.

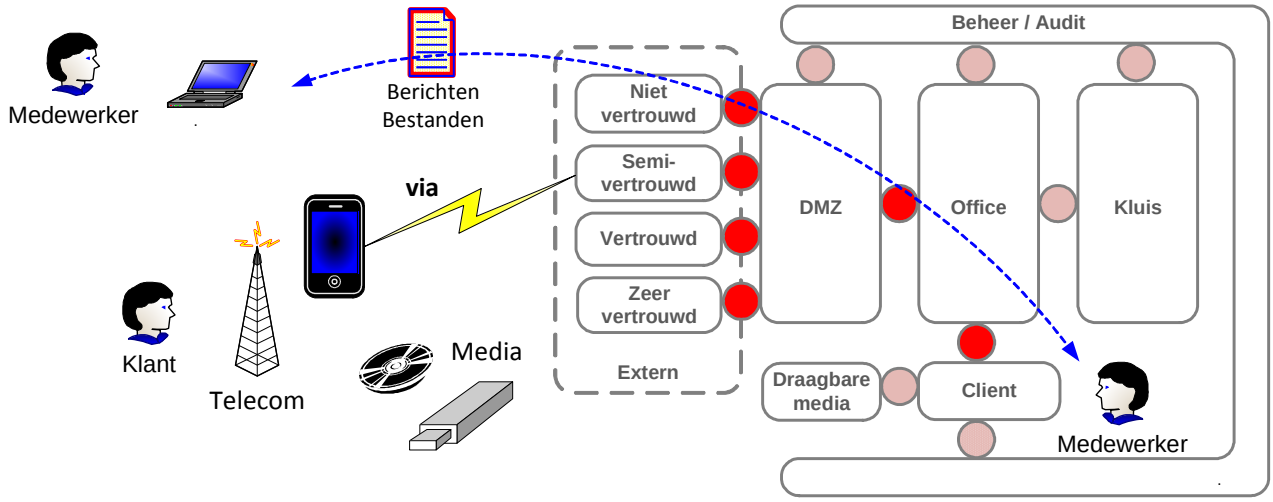
Criteria

Vertrouwelijkheid en Integriteit

Context

De op papier gebaseerde uitwisseling van formele documenten wordt steeds meer vervangen door elektronische berichtenuitwisseling. Veel communicatie over en weer vindt plaats met behulp van elektronische middelen. De communicatie tussen zender en ontvanger vindt daarbij plaats via netwerken, waarvan de vertrouwelijkheid niet altijd gegarandeerd is.

Organisaties hebben behoefte aan vertrouwde en integere uitwisseling van berichten en het vertrouwd kunnen opslaan van bestanden binnen en buiten de organisatie, tussen de daarvoor geautoriseerde personen en systemen. Voorbeelden daarvan zijn uitwisseling van wachtwoorden en pincodes tijdens financiële transacties, draagbare opslagmedia zoals USB sticks, gebruik draadloze verbindingen enz.



Omgeving waarin gegevens elektronisch wordt uitgewisseld

Probleem

Elke vorm van uitwisseling en opslaan van gegevens kent zijn eigen risico's t.a.v. vertrouwelijkheid en integriteit.

1. **Gegevens tijdens verwerking in tijdelijke opslag:** het gaat hier om gegevens in het werkgeheugen van systemen en risico's van "lekkage" van de ene gegevensstroom naar de andere, of het gebruik van in bewerking zijnde gegevens door onbevoegden. Het probleem daarbij is dat besturingssystemen zelden zijn ingericht op 'gelaagde beveiliging' en dat er geen beheer wordt uitgevoerd op tijdelijke opslag van geheimen zoals wachtwoorden. Oplossingen voor dit type beheer zijn in de patronen van het thema Encryptie niet uitgewerkt.
2. **Gegevens op transport:** het gaat hier enerzijds over elektronische berichten of bestanden, die verstuurd worden via vaste of draadloze netwerken en risico's impliceren van afluisteren, wijziging en misbruik door onbevoegden. Anderzijds gaat het over transport van bestanden via draagbare media of mobiele clients. Deze impliceren risico's van verlies, diefstal, misbruik en wijziging door onbevoegden.
3. **Gegevens in langdurige opslag:** het gaat hier over berichten of bestanden die opgeslagen worden binnen de vertrouwde infrastructuur van een organisatie. Hier speelt afhankelijk van de classificatie van de gegevens het risico van ongeautoriseerd gebruik van gegevens, b.v. door beheerders.

Oplossing

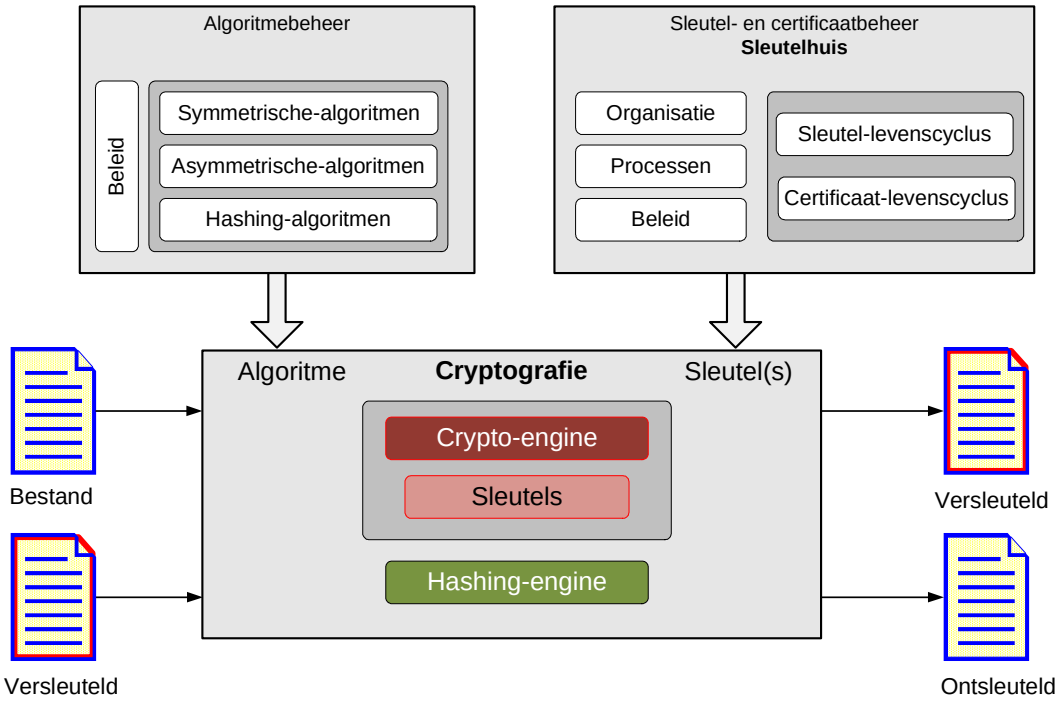
Per levenscyclus van gegevens zijn onderstaande generieke oplossingen ontwikkeld, waarbij de vertrouwelijkheid van de getransporteerde of opgeslagen gegevens wordt gewaarborgd door het principe van versleuteling (encryptie) van gegevens door een zender en de ontsleuteling daarvan door een

geautoriseerd ontvanger. De te beschermen gegevens (cijfers, tekst, figuren) worden daarbij omgezet in niet interpreteerbare tekst of beelden. Aan de ontvangstkant vindt een omgekeerde bewerking plaats. Encryptie bestaat uit twee basiselementen:

- Algoritme: de formule op basis waarvan de gegevens worden versleuteld en ontsleuteld.
- Sleutel: de geheime component waarmee het algoritme versleutelt en ontsleutelt.

Encryptie kent drie hoofdgroepen:

1. Symmetrisch: Alle informatie wordt versleuteld en ontsleuteld met één geheime sleutel (zie patroon Symmetrische encryptie)
2. Asymmetrisch: Informatie wordt versleuteld met een *sleutelpaar*, bestaande uit een *private* en *publieke* sleutel. Voor verzending *versleutelt* de zender met de publieke sleutel van de ontvanger. De ontvanger *ontsleutelt* met zijn private sleutel, die wiskundig verbonden is met het paar van de zender. Elk sleutelpaar heeft een publieke en een private sleutel. (zie patroon PKI).
3. Hash: Informatie wordt één-weg verwerkt met een hashing algoritme tot een uniek controlegetal. Een bepaalde tekst levert via dat algoritme altijd hetzelfde getal op, zodat zonder overdracht van sleutels met het algoritme bepaald kan worden dat de tekst ongewijzigd is. Hashing wordt ook wel *one way encryption* (éénwegversleuteling) genoemd, en het controlegetal de hash of het synoniem daarvoor: de *digest*.



Basisfuncties en componenten van Encryptie

Bovenstaande figuur geeft aan uit welke basisfuncties en componenten encryptie is opgebouwd. Het beheer van algoritmen, sleutels en certificaten en sleuteldistributie neemt daarbij een belangrijke plaats in (zie patronen Symmetrische encryptie, PKI en Sleutelhuis). De Crypto-engine voert op basis van een algoritme de versleuteling (of ontsleuteling) uit bij symmetrische en asymmetrische encryptie. De Hashing-engine voert op basis van een hashing algoritme een z.g. éénwegversleuteling uit, die aan de ontvangstkant vergeleken wordt met het controlegetal van de verzonden data. De integriteit van data op transport is aangetoond wanneer aan de zend- en ontvangkant de controlegetallen aan elkaar gelijk zijn.

Toepassingen in verschillende context

Gegevens in tijdelijke opslag: Gevoelige gegevens zoals wachtwoorden en pincodes worden op *systeem- of applicatieniveau* versleuteld en de waarden daarvan zijn uitsluitend leesbaar voor bevoegde processen. Deze functies moeten specifiek op applicatie- en systeemniveau zijn ingebouwd.

Gegevens op transport: Dit is de grootste risicogroep en betreft versleuteling van netwerkverkeer: *Public Key Infrastructure* (PKI); een infrastructurele totaaloplossing op basis van certificaten uitgegeven door een derde vertrouwde partij. (zie patroon PKI)

Versleuteling op *applicatieniveau*: Hierbij wordt versleuteling door twee met elkaar communicerende systemen end-to-end uitgevoerd. Alleen het dataveld van een pakket wordt hierbij versleuteld. Een bekende vorm van encryptie op applicatieniveau is de *secure-http* techniek, die gebruikt wordt voor versleuteling van http (*hypertext transfer protocol*) berichten.

Versleuteling op *sessieniveau*: zoals Transport Layer Security (TLS). Deze techniek wordt gebruikt in combinatie met applicatieprotocollen, zoals http(s), ftp(s), imap(s), pop(s) en smtp(s), herkenbaar aan het (s)-je. Als TLS is toegepast bij (http), dan wordt per sessie de webcommunicatie versleuteld (https) en zie je in de statusbalk van de browser het bekende slotje.

Versleuteling op *netwerkniveau*: zoals IPSec. Op basis van dit protocol worden versleutelde communicatietunnels gelegd tussen netwerkeindpunten, waarmee veilige communicatie mogelijk is. Met deze tunnels kunnen Virtual Private Networks (VPN's) worden gebouwd. Draadloze netwerken worden versleuteld met eigen protocollen als WPA (Wi-Fi Protected Access).

Versleuteling op *datalinkniveau*. Hierbij wordt op het 'laagste niveau' van het netwerk versleuteling uitgevoerd tussen twee netwerk knooppunten. Alle data die wordt uitgewisseld, dus ook protocolinformatie is daarbij versleuteld.

Informatie op transport

Gegevens in langdurige opslag: Dit betreft versleuteling van informatie op vaste en mobiele gegevensdragers:

- Versleuteling van *mobiele geheugenmedia*, zoals Harddisks van laptops, USB-stick, CDROM, Tape of insteek-memorymodules en in toenemende mate geheugens van PDA's en Smartphones.
- Versleuteling van *vaste geheugenmedia*, zoals harddisk arrays van databases, tape en optische media.

Afwegingen

De vraag is op welk niveau encryptie moet plaatsvinden; op applicatie-, middleware of hardwareniveau? Behalve voor zeer vertrouwelijke gegevens moet worden voorkomen dat versleuteling op meerdere niveaus gelijktijdig plaatsvindt. Elk niveau heeft zijn eigen specifieke voor- en nadelen. Criteria zijn: Flexibiliteit en Performance. Op applicatieniveau is end-to-end encryptie relatief eenvoudig realiseerbaar. Hardware-encryptie biedt duidelijke performance voordelen

Implicaties

- Toepassen van encryptie in bedrijfsprocessen vereist classificatie van informatie. Besluitvorming over welke informatie in welke situatie (bewerking, transport, opslag) dient te worden versleuteld.
- Toepassing van PKI vereist uitgifte, beheer- en periodieke vernieuwing van certificaten.
- Sleutels en certificaten hebben een eigen levenscyclus. Adequaat sleutelbeheer is randvoorwaardelijk voor encryptie. Daarvoor is het *Sleutelhuis* de oplossing.
- Acceleratie is nodig omdat cryptografische bewerkingen rekenintensief zijn en relatief veel processorcapaciteit vergen. Waar mogelijk wordt dit rekenwerk door speciale hardware gedaan.
- Lange termijn versleutelde opslag vereist ook lange termijn sleutelbeheer.

Gerelateerde patronen

- Symmetrische Encryptie, zoomt in op het mechanisme Symmetrische encryptie, het toepassingsgebied daarvan en sleutelbeheer en distributie.
- Public Key Infrastructure (PKI), waarin o.a. het doel en toepassingsgebied van Asymmetrische encryptie wordt uitgelegd en de uitgifte en beheer van certificaten.
- Sleutelhuis, dat het beheer van cryptografische sleutels regelt.

22. Symmetrische encryptie

Criteria

Vertrouwelijkheid en Integriteit

Context

De focus ligt bij dit patroon op methoden voor de versleuteling van de *gegevens*. Voor authenticatie en het veilig uitwisselen van sleutels wordt gebruik gemaakt van PKI op basis van asymmetrische encryptie.

Berichten en bestanden worden op verschillende manieren via de niet vertrouwde “buitenwereld” uitgewisseld:

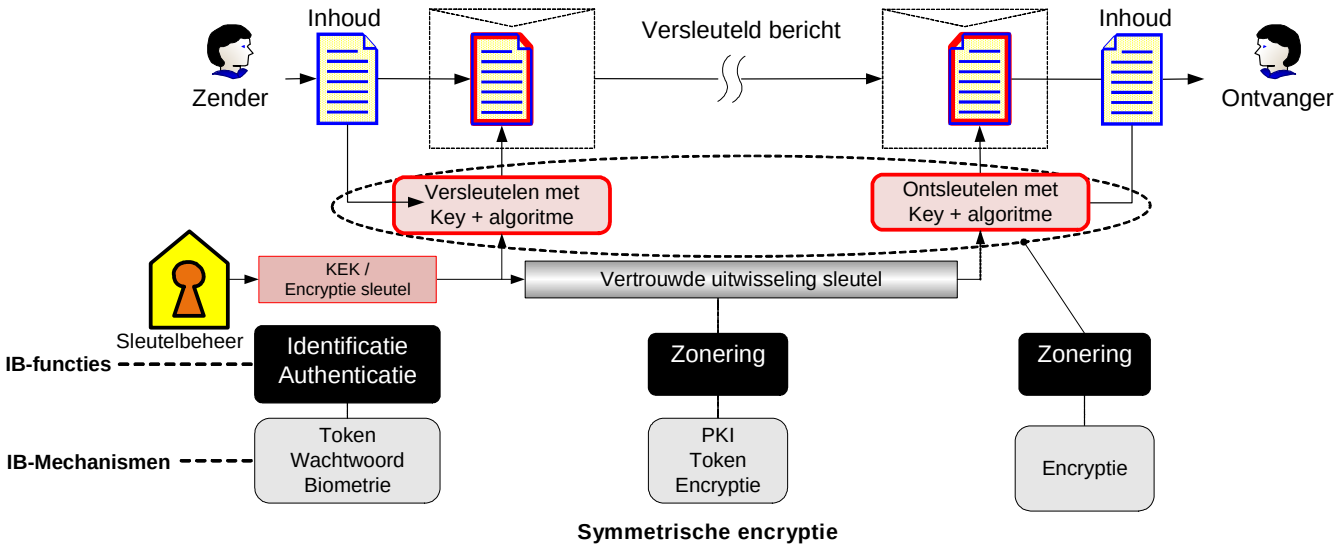
- Eindgebruikers versturen berichten via e-mail over het Internet.
- Eindgebruikers plaatsen bestanden op draagbare media (USB-stick, CD-ROM, DVD, SD kaarten etc.) die ze meenemen naar het externe domein.
- Berichten worden via openbare netwerken naar een semi-vertrouwde of niet vertrouwde client verstuurd, bijvoorbeeld voor telewerken of mobiel werken.
- Bij gebruik van draadloze verbindingen binnen de omgeving van de organisatie, waarvan te verwachten is dat ze buiten het gebouw te ontvangen zijn (zoals Wi-Fi).
- Er worden berichten uitgewisseld via openbare netwerken tussen systemen van de organisatie op verschillende locaties of met die van vertrouwde partners.
- Berichten en bestanden worden opgeslagen op een mobiele client (laptop, PDA, smartphone) die meegenomen wordt naar het externe domein.

Probleem

1. Voor informatie in (tijdelijke) *opslag* of *transport*, ontstaan er grofweg twee soorten risico’s voor ongeautoriseerd gebruik van de informatie uit het bericht of bestand:
   a. Draagbare media of mobiele clients, waarop gevoelige informatie is opgeslagen, impliceren risico’s van verlies, diefstal en misbruik.
   b. Bij het transport van gevoelige informatie via draadloze en/of openbare netwerken bestaat het risico dat de communicatie wordt afgeluisterd en misbruikt.
2. Binnen de fysiek afgeschermde en/of beheerde infrastructuur van een organisatie zorgen maatregelen voor zonering en filtering tussen de zones voor de benodigde fysieke en logische afscherming van gevoelige informatie. Daarbuiten leveren deze maatregelen geen afscherming meer waarmee elke garantie voor de vertrouwelijkheid en integriteit van de informatie vervalt.

Oplossing

Het openbaar of voor onbevoegden toegankelijk worden van (gevoelige) informatie kan voorkomen worden door encryptie tijdens gebruik, opslag of transport van het bericht of bestand. Als oplossing wordt in dit patroon symmetrische encryptie toegepast.



Symmetrische encryptie

Bij voorkeur vindt de symmetrische encryptie transparant voor de eindgebruiker plaats.
Omdat symmetrische encryptie zich vaak afspeelt op het niveau van verbindingen, netwerken en systemen is dat ook meestal het geval. Bekende voorbeelden hiervan zijn de VPN's (Virtual Private Network), TLS (Secure Socket Layer) en Wi-Fi encryptie (WPA). Daar waar de encryptie zich op applicatieniveau afspeelt, is vaak interactie van de eindgebruiker vereist. Voorbeelden hiervan zijn e-mail encryptie en aparte software voor encryptie van bestanden om deze op draagbare media op te slaan of als bijlage met e-mail te versturen.
De encryptie is uiteindelijk zo sterk als de mate waarin de cryptografische sleutel geheim gehouden kan worden voor onbevoegden. Voor de sterkte van de encryptie spelen de volgende factoren een cruciale rol:

- Encryptiealgoritme en sleutellengte.
- Distributie van sleutels.
- Lifecyclemanagement van sleutels.

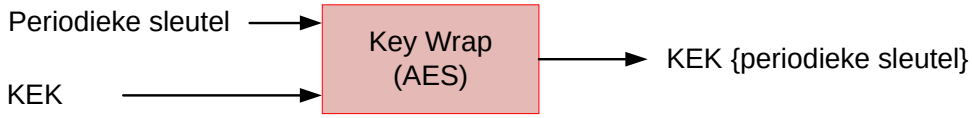
Encryptiealgoritme en sleutellengte:
Het meest robuuste en inmiddels standaard toegepaste encryptiealgoritme is AES. Daarnaast bestaan er nog meer goede algoritmen, die we in dit patroon buiten beschouwing laten. Het AES algoritme is geschikt voor de sleutellengtes van 128, 192 of 256 bits. De sleutellengte en de kwaliteit van de sleutel bepalen in belangrijke mate de tijdsduur die nodig is voor het 'kraken' van de encryptie.

Distributie van sleutels:
Voor distributie van sleutels worden vaak weer andere encryptiemechanismen ingezet met de bijbehorende sleutels. Samen met de sleutels voor distributie en beheer worden er drie soorten cryptografische sleutels onderscheiden: Key Encryption Keys (KEK), periodieke sleutels en sessiesleutels. De eigenschappen van deze sleutels zijn in onderstaande tabel samengevat.

Eigenschap	Key Encryption Key	Periodieke sleutel	Sessiesleutel
Doel	Encryptie van de periodieke of sessiesleutel	Symmetrische encryptie van de gevoelige gegevens	Symmetrische encryptie van de gevoelige gegevens
Soort	Publieke sleutel of geheime sleutel	Geheime sleutel	Geheime sleutel
Levensduur	1 jaar	Vastgestelde periode	1 sessie
Distributie	Fysiek (smartcard, CD-ROM, sleutellaadapparaat, papier) over vertrouwd pad	Beveiligd met KEK over communicatiepad zelf of over ander onvertrouwd pad	Beveiligd met KEK over communicatiepad zelf
		Fysiek over vertrouwd pad (geen KEK)	

Afhankelijk van de toepassing zijn er verschillende methoden om sleutels veilig te distribueren. Een aantal gangbare methoden worden hier aan de hand van voorbeelden toegelicht.
Distributie van de KEK: de KEK moet voorafgaand aan de ingebruikname van de encryptie over een vertrouwd pad gedistribueerd worden. De KEK wordt meestal op een fysiek medium opgeslagen, zoals een smartcard, dat bijvoorbeeld met een speciale koerier verstuurd kan worden of bij een loket afgehaald moet worden op basis van een bewijsstuk en legitimatie. Bij specifieke apparatuur wordt de asymmetrische sleutel al bij de fabriek geïnstalleerd.

Distributie van periodieke sleutels: voor beveiliging van de distributie van periodieke sleutels kan men zowel kiezen voor asymmetrische encryptie (KEK is publieke sleutel afkomstig van een PKI) als voor symmetrische encryptie (KEK is geheim). Een voorbeeld van een systeem met een geheime KEK is de AES Key Wrap methode, zie onderstaande figuur.

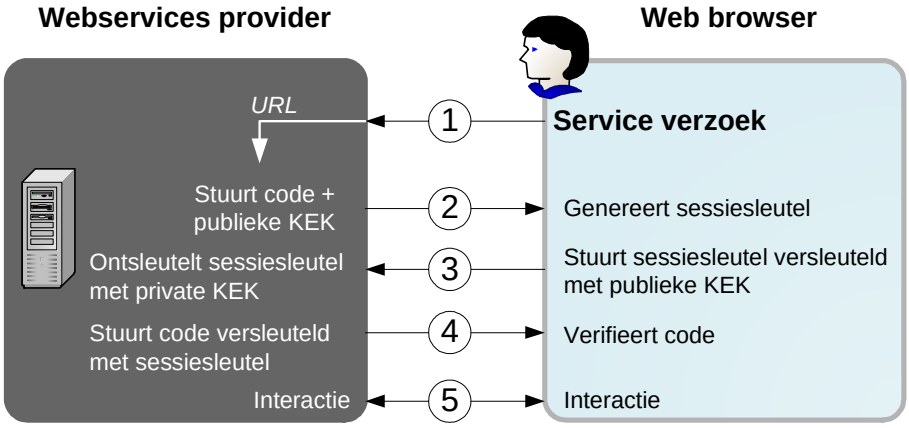


Distributie van sleutels

Symmetrische encryptie met de KEK als sleutel zorgt hier voor de beveiliging van de periodieke sleutel, zodat deze via een niet vertrouwd pad verzonden kan worden of veilig op een systeem kan worden opgeslagen. De periodieke sleutel kan weer verkregen worden met de omgekeerde bewerking (Key Unwrap) en dezelfde KEK. Een bekende toepassing is Over-The-Air-Keying (OTAK) voor encryptie van draadloze systemen voor spraak.

Distributie van periodieke sleutels met een publieke KEK verloopt bijvoorbeeld op een vergelijkbare manier als hierna beschreven wordt voor distributie van een sessiesleutel.

Distributie van een sessiesleutel: Onderstaande figuur laat zien hoe een publieke KEK (afkomstig van een PKI) wordt gebruikt bij het uitwisselen van een sessiesleutel voor het beveiligen van webverkeer (https) tussen client en server op het Internet.



Uitwisseling van sessiesleutel

De berichtuitwisseling verloopt als volgt:

1. Vanuit de client (webbrowser) wordt een serviceverzoek gedaan naar een webserver;
2. De server stuurt een willekeurige code samen met de publieke KEK van de server. De Web browser checkt de geldigheid van het certificaat van de server aan de hand van een tabel in de browser.
3. De client genereert een random sessiesleutel, versleutelt deze met de publieke KEK van de server en stuurt die terug naar de server;
4. De server ontsleutelt de sessiesleutel met behulp van de geheime private KEK van de server en stuurt de met de nieuwe sessiesleutel versleutelde code opnieuw naar de client, zodat die kan verifiëren of er nog steeds met dezelfde server gecommuniceerd wordt.
5. De sessiesleutel is nu bij beide partijen bekend en wordt vervolgens voor de symmetrische encryptie van het webverkeer gebruikt. Veilige interactie is nu gegarandeerd voor de duur van de sessie.

Omdat de KEK van alle sleutels de langste levensduur heeft, is dat ook de meest gevoelige sleutel. De KEK zelf wordt niet versleuteld en dient dus op een andere wijze fysiek en/of logisch te worden afgeschermd. Toegang tot de KEK is alleen toe te staan na identificatie en authenticatie van de beheerder dan wel de gebruiker van de KEK.

Er bestaan ook oplossingen waarbij een KEK ontbreekt. Een bekend voorbeeld is Wi-Fi encryptie in de pre-shared key (PSK) mode. Daarbij worden de (periodieke) Wi-Fi sleutels ter plaatse door een beheerder ingevoerd. De beheerder moet er voor zorgen dat de sleutels niet bekend worden.

Afwegingen

De te selecteren oplossing voor symmetrische encryptie is sterk afhankelijk van de toepassing waarvoor men de encryptie wil inzetten. Voor de beveiliging van de distributie van de encryptiesleutel heeft men de keuze tussen asymmetrische en symmetrische encryptie.

Asymmetrische encryptie van sleutels heeft de voorkeur omdat het flexibeler is. Het maakt veilige communicatie mogelijk tussen partijen die elkaar niet kennen. Een partij die versleutelde data wil ontvangen, kan zijn publieke sleutel op elke manier versturen of bekend maken, die hem past. De sleutel kan op internet op de eigen website geplaatst worden. Het gebruik van asymmetrische sleutels vraagt wel aanzienlijk meer rekenkracht dan het gebruik van symmetrische sleutels. Daarom wordt asymmetrische encryptie wel gebruikt voor het versturen van sessiesleutels, maar meestal niet voor het versleutelen van de data. Daarvoor wordt de efficiëntere Symmetrische encryptiemethode gebruikt.

Sessiesleutels hebben de voorkeur boven encryptie met periodieke sleutels, omdat het veiliger is (de sleutel wordt bij elke nieuwe sessie gewijzigd). Bij sessiesleutels wordt voor aanvang van de communicatie een sleutel uitgewisseld wat enige opstartvertraging oplevert. Bij berichtuitwisseling tussen slechts twee partijen is dit in de praktijk meestal geen probleem. Wanneer berichten naar meer dan twee partijen gestuurd worden (groepscommunicatie) kan de opstartvertraging te groot worden en hebben periodieke sleutels de voorkeur.

Wanneer berichten of bestanden naar partijen of systemen gezonden worden waarmee geen directe verbinding bestaat (store-and-forward), is men gebonden aan periodieke sleutels. Er is dan immers geen communicatiepad beschikbaar waarover een sessiesleutel kan worden uitgewisseld. Bij encryptie van opgeslagen data bestaat het risico dat er bij decryptie een fout optreedt als gevolg waarvan de data niet meer toegankelijk is. Het is daarom belangrijk er altijd voor te zorgen dat er, alvorens de data versleuteld wordt opgeslagen, back-ups gemaakt worden die binnen de eigen afgeschermde omgeving bewaard worden.

Voorbeelden

- E-mail encryptie: PGP, S/MIME
- Encryptie van webverkeer: TLS
- VPN: IPsec
- Wi-Fi encryptie: WPA, WPA2

Implicaties

Toepassing van symmetrische encryptie impliceert sleutelbeheer en sleuteldistributie. Afhankelijk van de toepassing en de omvang van het gebruik kan sleutelbeheer zeer complex zijn. Meestal betekent het dat het sleutelbeheer organisatorisch en procedureel moet worden ingericht inclusief personele inzet. Als de geselecteerde oplossing voor symmetrische encryptie zich er voor leent, kan men er voor kiezen gebruik maken van een bestaande PKI dienst (overheid of commercieel).

Gerelateerde patronen

Symmetrische encryptie heeft een relatie met de volgende patronen:

- PKI, voor het sleutelbeheer van publieke sleutels voor sleuteldistributie.
- Secure E-mail, als toepassing waarin symmetrische encryptie gebruikt wordt.

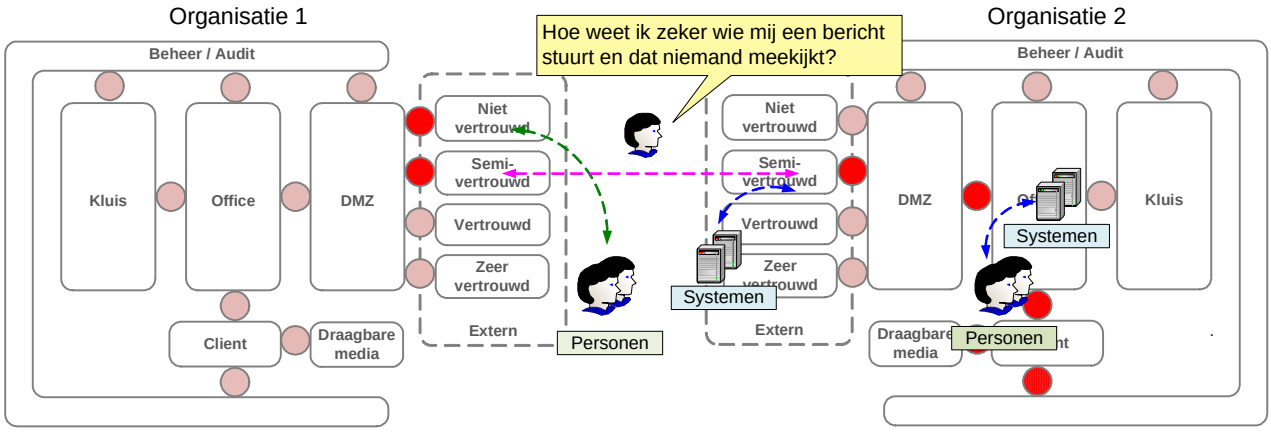
23. Public Key Infrastructure (PKI)

Criteria

Integriteit, Vertrouwelijkheid

Context

Bij elektronische communicatie rekenen de gebruikers er op dat deze dezelfde- of een hogere betrouwbaarheid biedt als hetgeen men gewend was bij postverkeer, namelijk: bezorging op het juiste adres inclusief handhaving van het briefgeheim.



Omgeving van een PKI

Probleem

De belangrijkste problemen die voor een betrouwbare elektronische communicatie opgelost moeten worden zijn:

1. **Identiteit:** Hoe kun je vaststellen met wie je communiceert en hoe weet de ontvanger zeker dat jij de verzender bent en niet iemand anders?
2. **Vertrouwelijkheid:** Hoe zorg je ervoor, dat de inhoud onleesbaar is voor derden?
3. **Integriteit:** Waarmee kan worden aangetoond dat gegevens tijdens transport (niet) zijn gewijzigd?
4. **Onweerlegbaarheid:** Waarmee wordt voorkomen dat een ontvangen bericht kan worden ontkend?
5. **Sleuteldistributie en beheer:** Bij grote aantallen gebruikers van symmetrische versleuteling neemt de beheerlast exponentieel toe. Een dilemma bij encryptie is tevens dat er eerst geheime sleutels uitgewisseld moeten worden alvorens veilige communicatie mogelijk is. De vraag die voorligt is: hoe kan in het publieke domein en bij grootschalige bedrijfstoepassingen sleuteldistributie en beheer haalbaar worden ingevuld?

Oplossing

Een Public Key Infrastructure (PKI) is een set van technische en organisatorische voorzieningen, die een oplossing biedt voor bovengenoemde probleemstelling. PKI berust op asymmetrische versleuteling en elektronische certificaten.

Bij asymmetrische versleuteling worden twee encryptiesleutels toegepast: één publieke sleutel[5] en één geheime private[6] sleutel. Deze sleutels hebben een unieke wiskundige relatie met elkaar, wat betekent dat de data die *versleuteld* is met de publieke sleutel van de zender, alleen *ontsleuteld* kan worden met de private sleutel van een ontvanger en niet met de publieke sleutel zelf! Omgekeerd wordt het versleutelen van een *Hash* met behulp van de private sleutel van de zender en ontsleuteling daarvan met de publieke sleutel van de ontvanger gebruikt bij ‘het zetten’ van een *elektronische handtekening*.

De persoon of instelling, die de aldus versleutelde data wil verzenden of ontvangen, kan zijn publieke sleutel op elke gewenste manier versturen of bekend maken, dus ook op zijn eigen website! Om publieke sleutels (en de geldigheid daarvan) voor een ieder toegankelijk en vindbaar te maken op het internet, zijn er ‘public key servers’ ingericht waarop men een publieke sleutel kan plaatsen. De sleutel kan dan gevonden worden op persoon en op e-mailadres, maar biedt geen garantie dat het e-mail adres bij de persoon of instelling hoort, die staat aangegeven op de server. Dit probleem wordt opgelost middels het

[5] Publieke sleutel: Public key

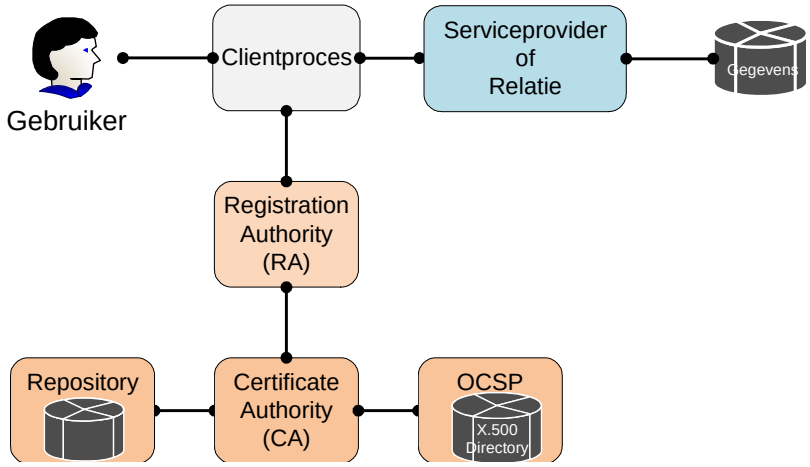
[6] Private sleutel: Private key

gebruik van certificaten. Van hetzelfde sleutelpaar wordt nu de publieke sleutel opgenomen in een zogeheten Public Key Certificaat. De uitgifte en beheer rond deze certificaten wordt op een geformaliseerde wijze uitgevoerd, zodat de status van het certificaat en de eigenaar gegarandeerd is. Daarmee kunnen de sleutels in combinatie met de betreffende certificaten gebruikt worden voor authenticatie en het versturen van geheime (sleutel-) informatie over een niet vertrouwd netwerk. Certificaten worden door een (derde) partij uitgegeven, die zowel door zender als ontvanger vertrouwd wordt; een *Certificate Service Provider* (CSP). De CSP garandeert de echtheid en de oorsprong van de certificaten en moet zelf ook aan kwaliteitseisen voldoen: ETSI of OPTA voor PKIoverheid.

Certificaten kunnen in allerlei vormen worden uitgegeven. De bijbehorende private sleutels moeten beschermd zijn tegen dupliceren en worden bij voorkeur uitgegeven en opgeslagen op afzonderlijk te beveiligen objecten als smartcards, usb-tokens, en Hardware Security Modules (HSM).

Er zijn verschillende soorten van PKI in gebruik en daaraan gekoppeld bestaan verschillende soorten van uitgifte processen van certificaten door CSP's:

1. *Binnen een organisatie*: hier worden certificaten uitgegeven door een "eigen" CSP
2. *Binnen het publieke domein*: uitgifte processen moeten hierbij voldoen aan wet- en regelgeving voor elektronische handtekeningen. In Nederland zijn normen vastgelegd voor PKIoverheid certificaten. Verschillende organisaties zijn gecertificeerd voor het uitgeven van PKIoverheid certificaten.

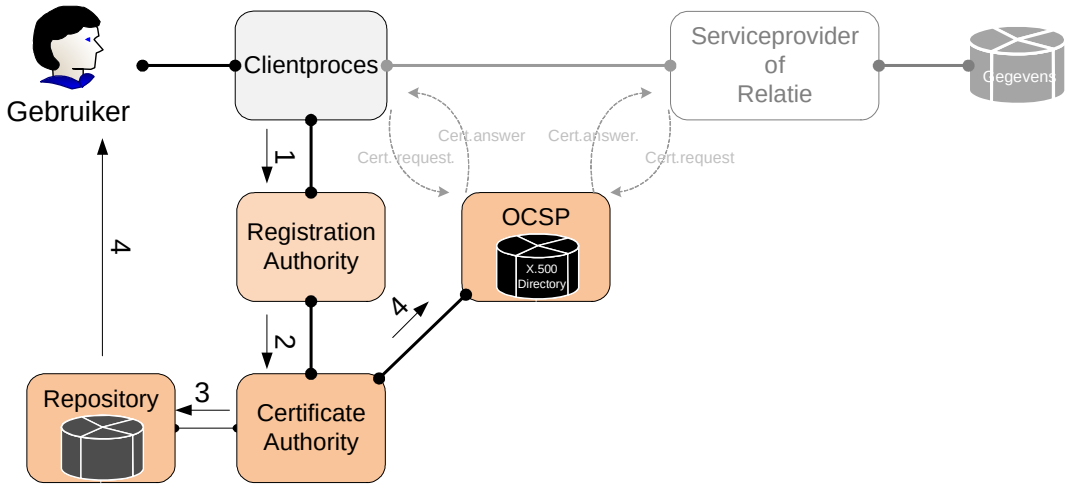


Basiselementen van een PKI

Objecten van beschouwing in een PKI zijn:

- **Gebruikers** die onderling veilige transacties willen uitvoeren. De relatie tussen de gebruikers kunnen van allerlei typen zijn (leverancier – afnemer, werkgever – werknemer, organisatie – overheid, enz.). Om dit te kunnen doen moeten de partijen vertrouwen op de *Registration Authority* (RA) en de *Certificate Authority* (CA). Deze twee organisaties behoren bij een PKI. De mate van zekerheid, dat het sleutelbeheer, de authenticatie en de vertrouwelijkheid geregeld zijn hangt rechtstreeks af van de kwaliteit van deze instellingen.
- **Registration Authority** (RA) is een instelling waar gebruikers aanvragen kunnen indienen voor het verkrijgen van een certificaat (certificate request). Voor een hoog kwaliteitsniveaucertificaat is de kwaliteit van de verificatie van de identiteit van de gebruiker belangrijk.
- **Certificate Authority** (CA) is de derde vertrouwde partij. Het is de CSP, die certificaten uitgeeft op basis van de door de CA zelf goedgekeurde certificate requests. Deze requests worden ontvangen door één of meerdere RA servers. De CA beheert de uitgegeven certificaten, publiceert ze en bewaart de certificaten in de *Certificate repository*. Tevens publiceert de CA een lijst van ingetrokken certificaten; de *Certificate Revocation List* (CRL). Op de *Online Certificate Status Protocol server* (OCSP) kan online worden bevraagd of een certificaat geldig is.
- **Sleutelpaar**. Een paar asymmetrische sleutels, waartussen een bepaalde relatie bestaat. Een sleutel is de private sleutel van de gebruiker. Deze moet de gebruiker geheim houden. De andere sleutel is de publieke sleutel van de gebruiker, deze moet juist openbaar beschikbaar zijn.
- **Certificaat**. Een elektronisch object, het bevat de identiteit van de certificaathouder, de publieke sleutel en een verwijzing naar de verantwoordelijke CA.
- **Certificaat status server.** Een server van de CA, die via het internet bereikbaar is. Deze stelt informatie over de inhoud van de CRL en over de verstrekte certificaten beschikbaar. Een eindgebruiker kan daarmee via zijn browser op Internet controleren of zijn relaties beschikken over geldige certificaten en wat de publieke sleutels daarvan zijn. Een voorbeeld is de OCSP server.

Vier stappen voor verkrijgen van PKI certificaten



Verkrijgen van Public Key Certificaten

Stap 1: Per stap worden steeds twee varianten uitgelegd: bij variant (A) genereert de houder van het certificaat de encryptiesleutels zelf, bij variant (B) doet de Certificate Authority dat.

A) De client genereert zelf het sleutelpaar. Daarna vraagt hij een certificaat aan bij de RA. De client geeft daarbij de publieke sleutel van zijn sleutelpaar mee.

B) De client vraagt een certificaat aan bij de RA zonder zelf de sleutel gegenereerd te hebben.

Stap 2: De RA doet de verificatie van de aanvrager van het certificaat. De nauwkeurigheid van de verificatie is een belangrijk kwaliteitsaspect van het certificaat. Dit kan variëren van geen verificatie tot een grondige controle van de persoonsgegevens en face-to-face of zelfs een notariële verificatie. Daarna bestelt de RA het certificaat bij de CA. Als de RA-functie geautomatiseerd verloopt[7], dan worden correct ingevulde aanvragen direct doorgestuurd naar de CA.

Stap 3: A) De CA maakt na goedkeuring het certificaat aan en zet deze in een lokale repository. De CA beoordeelt de authenticiteit van aanvragen, maakt na goedkeuring nieuwe certificaten aan en zet deze in een (lokale) repository.

B) De CA genereert een sleutelpaar en gebruikt de nieuwe publieke sleutel om een certificaat aan te maken. Deze wordt in een lokale repository gezet. De private sleutel wordt op een zodanige wijze bewaard, dat ook niemand bij de CA kennis kan nemen van de waarde van de sleutel.

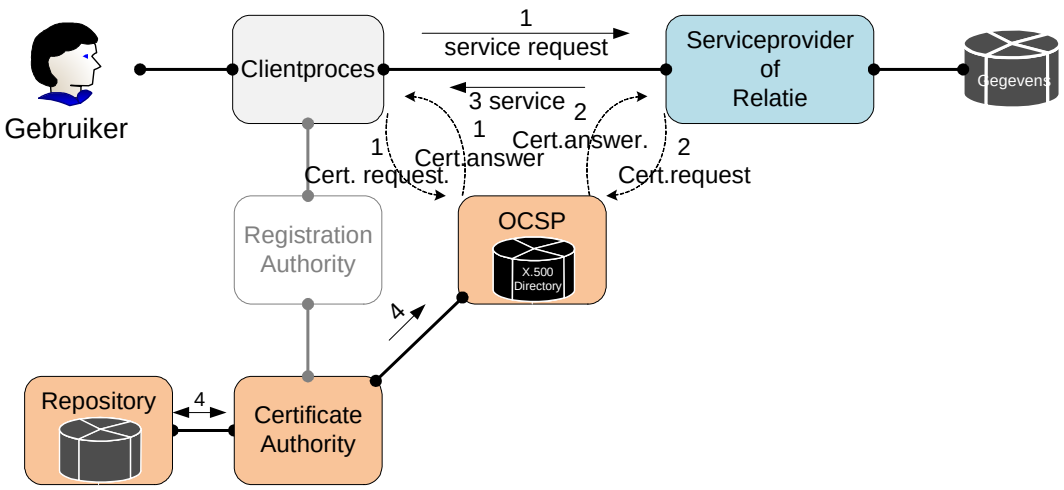
Stap 4: De CA zorgt voor de publicatie van een up-to-date Certificate Revocation List (CRL), waarop alle ingetrokken certificaten staan vermeld. De CRL wordt gepubliceerd op de OCSP server, die computers antwoord geeft over de geldigheidsstatus van een certificaat.

A) De CA stuurt een bevestiging naar de client. De client is verantwoordelijk voor de beveiligingsmaatregelen rond het gebruik van de private sleutel.

B) De Client ontvangt van de CA de private sleutel op een beveiligde wijze. De client is verantwoordelijk voor een beveiligde opslag van deze sleutel. De client is ook verantwoordelijk voor de beveiligingsmaatregelen rond het gebruik van de private sleutel.

[7] Geautomatiseerd aanvragen van certificaten kan direkt via een WEB interface met de CA

Het gebruik van PKI certificaten



Gebruik van Public Key Certificaten

Voorbeeld van het gebruik van Public Key Certificaten:

Elektronische handtekening ter authenticatie van de afzender en versleuteling van het bericht. Dit proces kan geheel geautomatiseerd worden uitgevoerd.

1) Gebruiker (Client) controleert de geldigheid van het certificaat van de relatie en haalt daar de publieke sleutel op.
2) Gebruiker stuurt een bericht naar de Relatie. Hij gebruikt zijn private sleutel voor een digitale handtekening. Hij versleutelt het bericht met behulp van de publieke sleutel van de partner.
3) Relatie gebruikt zijn private sleutel om het bericht te ontsleutelen. Relatie controleert de geldigheid van het certificaat van de Client en haalt diens publieke sleutel op via het netwerk of vanuit het certificaat van de relatie. Hij gebruikt de publieke sleutel voor de authenticatie van de afzender.

De het bericht is nu geverifieerd op *integriteit*.

Voorbeelden

Aanleveren notariële akten bij Kadaster

Implicaties

De toepassing van PKI impliceert dat zender en ontvanger beschikken over cryptografische middelen voor toepassing van sleutels, die gegenereerd zijn uit certificaten, die verbonden zijn aan één en hetzelfde rootcertificaat.
Evenals in de situatie waarbij *systemen* of organisaties als zender of ontvanger worden beschouwd, zal binnen die organisaties *functiescheiding* nodig zijn tussen degene die namens de organisatie beslissingsbevoegd is om certificaten aan te vragen, het beheer (incl. uitvoering) van het aanvraagproces van certificaten en het implementeren en *gebruiken* van certificaten.

Gerelateerde patronen

Elektronische handtekening, dat PKI gebruikt voor identificatie en authenticatie en onweerlegbaarheid van berichtuitwisseling.

Standaarden

- X.509
- RFC3647, RFC4210, RFC5280, RFC2559, RFC2585, RFC2560,
- ETSI TS 102042,
- ETSI TS 101456,
- Programma van eisen van PKIoverheid

24. Sleutelhuis

Criteria

Beschikbaarheid, Vertrouwelijkheid, Integriteit en Controleerbaarheid

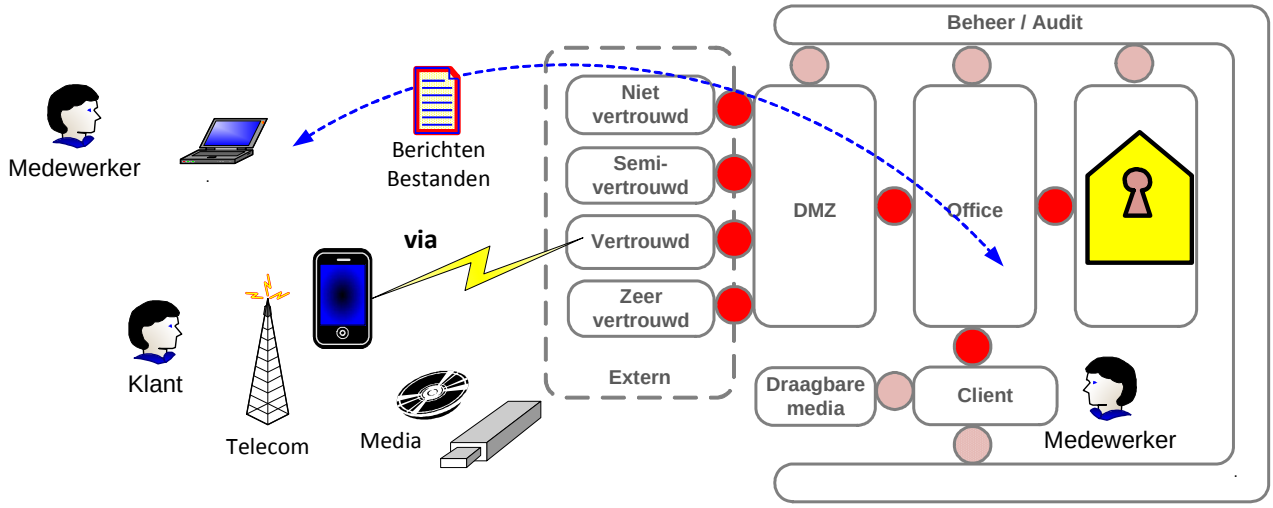
Context

Definitie. Het sleutelhuis omvat het geheel aan taken, organisatie, processen en techniek voor het beheer van cryptografische *sleutels*.

Dit patroon behandelt het sleutelhuis en een raamwerk van controleniveaus daarvoor.

Organisaties die encryptie toepassen hebben intern een sleutelhuis nodig voor de beheersing van zowel de operationele-, ontwikkeling- en beheerprocessen, vanaf het ontstaan tot en met de vernietiging van sleutels en het geheel aan sleutelmateriaal gerelateerde activiteiten. Daarin onderscheidt het zich van een Trusted Third Party (TTP), die als een derde vertrouwde partij *certificaten* uitgeeft en beheert voor verschillende organisaties die encryptie toepassen bij hun onderlinge communicatie.

De uit TTP-certificaten gegenereerde sleutels worden in het sleutelhuis van een organisatie bewaard.



Omgeving Sleutelhuis

Probleem

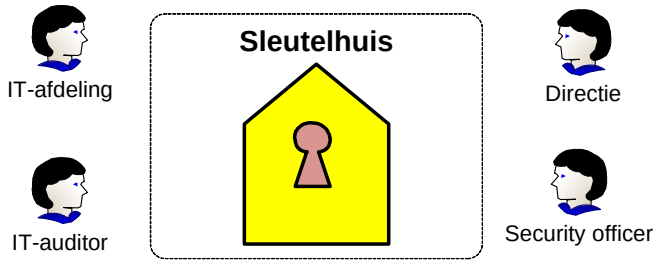
Elke organisatie die versleuteling van gegevens toepast, ervaart op een bepaald moment, dat het introduceren van encryptietechnieken betrekkelijk eenvoudig is, maar dat zonder adequaat ingericht sleutelbeheer de organisatie zeer grote risico's loopt voor ongeautoriseerde toegang of verlies van kritische gegevens.

Oplossing

Inrichting van een 'sleutelhuis', waarin een reeks gestructureerde processen voor ontwikkeling, beheer en controle en het operationele beheer van sleutels plaatsvinden

Bij de toepassing van cryptologie zijn de volgende factoren van belang:

- Versleutelde data is net zo lang toegankelijk als de beschikbaarheid van de bijbehorende sleutel;
- De versleuteling is net zo sterk als de mate van de geheimhouding van de sleutel;
- Adequaat sleutelbeheer is vereist op grond van de Wet op de inlichtingen- en veiligheidsdiensten (WIV), artikel 24:3 waarin vermeld staat dat AIVD of MIVD na een schriftelijk verzoek om toegang tot gevraagde versleutelde gegevens de toegang daartoe verleend moet worden. Verder staat in artikel 89 van de WIV vermeld dat het al dan niet opzettelijk hinderen bij het ontsleutelen van gegevens als overtreding of misdrijf strafbaar gesteld wordt.



Betrokkenen bij sleutelbeheer

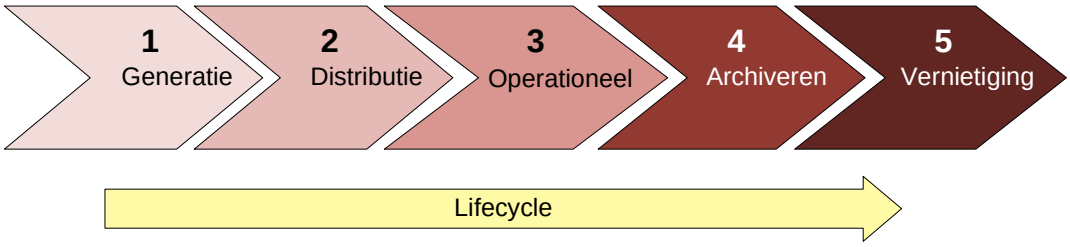
Organisatiestructuur

Het sleutelhuis is een virtueel organisatieonderdeel dat een gecontroleerde invulling geeft aan het lifecycle-management van certificaten en cryptografische sleutels. Voor het vullen van dit organisatieonderdeel wordt veelal gebruik gemaakt van medewerkers met een andere hoofdtaak. Functiescheiding is een belangrijk punt van aandacht binnen de sleutelhuisprocessen en procedures.

- De Security Officer is *eindverantwoordelijk* voor het (laten) ontwikkelen, implementeren en uitvoeren van de sleutelbeheerprocessen en procedures.
- De IT-afdeling wordt *geraadpleegd* bij de ontwikkeling van de technische werkinstructies en is verantwoordelijk voor de *uitvoering* van het technische deel van de procedures.
- De IT-auditor *toetst* periodiek de effectiviteit, efficiency en beveiliging van de uitvoering van het sleutelbeheer en rapporteert daarover aan de directie die eindverantwoordelijk is voor de informatiebeveiliging als geheel.

Lifecycle-management van sleutels

Adequaat lifecycle-management van cryptografische sleutels is randvoorwaardelijk voor toepassing van encryptie. Dat houdt in dat een sleutel de volgende fasen op gecontroleerde wijze doorloopt: generatie, distributie, operationeel, archiveren en vernietigen. Deze fasen worden die hierna beschreven.



Levenscyclus cryptografische sleutels

1. <u>Genereren van sleutels.</u>

Cryptografische sleutels kunnen symmetrisch of asymmetrisch zijn. Voor beide typen sleutels geldt dat het genereren ervan zodanig dient te gebeuren dat niet voorspelbaar is wat (het private deel van) de sleutel is. De Wet Elektronische Handtekening (WEH) stelt eisen aan de manier waarop sleutels gegenereerd worden. Er zijn verschillende aanleidingen voor genereren van nieuwe sleutels:

- **Een nieuwe toepassing** waarvoor sleutelmateriaal nodig is. Dit begint met een inventarisatie en registratie. Dit startpunt van de operationele sleutelbeheer processen legt het profiel vast van het gevraagde of aangeboden sleutelmateriaal en/of certificaten. Aan de hand van de eigenschappen en operationele eisen die voor een sleutel nodig zijn om verantwoord sleutelbeheer te kunnen voeren, worden de cryptografische eigenschappen en het eigenaarschap van het materiaal geregistreerd, de levensfases van het materiaal geïnventariseerd en vastgesteld welke sleutelbeheer procedures hiervoor noodzakelijk zijn. Alle informatie wordt vastgelegd in de Crypto Sleutelbeheer-Database, die zelf ook valt onder een regiem van geheimhouding en beschikbaarheid.
- **Aanvraag van een certificaat**. Dit begint met autorisatie van de aanvrager. De Security Officer verzamelt en *verifieert* de identiteitsgegevens van de aanvrager en *autoriseert* de aanvraag. Voor certificaataanvragen fungeert de Security Officer als interne Registration Authority (RA), dat wil zeggen identificatie, authenticatie en autorisatie van de aanvraag, het bepalen en aanvullen van de juiste inhoud en het optreden als *tussenpersoon* naar de interne of externe partij die certificaten uitgeeft: de Certificate Authority (CA).
- **Ter vervanging van sleutels waarvan de levensduur verstreken is**. Per toepassing dient in een sleutelplan te worden vastgelegd wanneer en hoe sleutels vervangen dienen te worden.
- **Vervangen van een sleutel als gevolg van een beveiligingsincident** of compromittatie van een in gebruik zijnde sleutel. Aangezien in een dergelijke situatie snel moet worden gehandeld om (verder) informatieverlies te voorkomen, moet zijn vastgelegd waar incidenten gemeld worden, wie een sleutel mag intrekken, hoe dat gecommuniceerd dient te worden, welke stappen verder moeten worden genomen en welke ingetrokken sleutels op een revocation list komen.

Cryptografische sleutels moeten veilig worden opgeslagen. Dit geldt ook voor back-ups van systemen waarin deze sleutels kunnen voorkomen. Het maken van een back-up van een sleutel is, afhankelijk van de toepassing, noodzakelijk / gewenst of juist niet toegestaan. Reden voor een back-up is het nog kunnen ontcijferen van informatie na verlies van de originele sleutel. Redenen voor het juist niet toestaan van een back-up kunnen bijvoorbeeld liggen in de eisen die de Wet Elektronische Handtekening (WEH) stelt voor authenticiteit en onweerlegbaarheid.

2. Distributie van sleutels

Dit dient op veilige wijze te gebeuren. Distributie kan fysiek of elektronisch verlopen, afhankelijk van de toepassing. Sleutels om andere sleutels te beveiligen (Key Encryption Key) en certificaten worden veelal fysiek, bijvoorbeeld op een smartcard, gedistribueerd, waarna ze onder andere voor de elektronische distributie van encryptie sleutels kunnen worden ingezet. Meer hierover staat beschreven in de patronen Symmetrische Encryptie en PKI. Alle in omloop zijnde sleutels worden op basis van een unieke identiteit geregistreerd samen met wie de ontvanger is, zodat bij compromittatie direct bekend is welke partijen geraakt zijn (in geval van asymmetrische sleutels is dat er vanzelfsprekend maar één).

3. Operationalisering van sleutels

Sleutels en certificaten hebben een aan hun gebruik aangepaste levensduur. In een sleutelplan wordt vastgelegd wanneer, welke sleutel, waar wordt toegepast. Uitzondering hierop zijn *sessiesleutels* die per sessie tussen partijen onderling worden afgesproken en alleen gedurende communicatiesessies geldig zijn.

4. Archivering van sleutels

Na de operationele fase is het van belang dat back-ups van sleutels gearchiveerd blijven, zolang de opgeslagen en nog te raadplegen berichten en bestanden nog beveiligd zijn met die sleutels en voor verificatiedoeleinden. Toegang tot het archief en het opvragen van sleutels eruit dient volgens strikte procedures te verlopen om de integriteit en vertrouwelijkheid te waarborgen.

5. Vernietiging van sleutels

Niet meer toegepaste sleutels dienen op een veilige wijze vernietigd te worden. Afhankelijk van het soort sleutel wordt voor operationele sleutels gebruik gemaakt van een hardwarematige “erase” functie of een softwarematige “wipe” functie. Het geheugen wordt hierbij zodanig overschreven dat het daarna niet mogelijk is om het sleutelmateriaal te reproduceren. Goede registratie is een voorwaarde om er voor te zorgen dat alle kopieën van sleutels vernietigd worden. Ook sleutels in back-ups en in het archief mogen niet vergeten worden om te vernietigen.

Sleutelbeheer rollen

In het sleutelhuis worden een aantal rollen onderscheiden. De rollen en de omschrijving van de bijbehorende taak staan in onderstaande tabel. Vanwege de beschikbaarheid is het wenselijk dat meerdere personen dezelfde rol kunnen vervullen en dus als back-up voor elkaar kunnen optreden. Dit is van belang om bij beveiligingsincidenten onder alle omstandigheden snel te kunnen handelen.

Ceremoniemeester

De Ceremoniemeester heeft een sturende rol in het sleutelbeheer. Initieert en/of organiseert tijdig de uitvoering van het bestaande sleutelbeheer procedures gedurende de levensfases van sleutels en certificaten. Fungeert als aanspreekpunt van het sleutelhuis, signaleert de behoefte aan nieuwe sleutelbeheer procedures en initieert de ontwikkeling hiervan.

Administratief sleutelbeheerder

De Administratief Sleutelbeheerder heeft een uitvoerende rol in de sleutelbeheer procedures:

- De rol is inventariserend, administratief en controlerend van aard.
- Doet de inventarisatie van sleutelmateriaal, de aanvragen van certificaten en werkt daarbij op basis van de sjablonen voor sleutel- en certificaatprofielen. Voert tevens een registratie uit in de Crypto Sleutelbeheer Database.
- Fungeert als geautoriseerd interface richting de CA.
- Bepaalt met behulp van het sleutelprofiel de sleutelbeheer procedures welke noodzakelijk zijn gedurende de levensfases van het sleutelmateriaal.
- Heeft een signalerende rol indien blijkt dat er aanvragen liggen voor sleutelmateriaal waar nog geen procedures voor bestaan en bepaalt de te nemen stappen.
- Beslist bij compromittatie van sleutelmateriaal en andere beveiligingsincidenten over de te volgen procedure.

Technisch Sleutelbeheerder
De Technisch Sleutelbeheerder heeft een uitvoerende rol in de sleutelbeheer procedures. Zijn/haar rol is technisch/uitvoerend van aard. Hij/zij voert de technische handeling uit op (cryptografische) systemen.

Kluisbeheerder
De Kluisbeheerder heeft toegang tot het algemene deel van de kluis en bezit een deel van de toegangsmiddelen nodig voor de toegang tot het compartiment in de kluis waarvoor Multi Party Control vereist is.

Auditor
Uitvoeren van een audit op de beveiliging van het sleutelbeheer proces.

Functiescheiding
Afhankelijk van het gewenste beveiligingsniveau kan het noodzakelijk zijn om bij de uitvoering van de procedures functiescheiding toe te passen. Dit betekent dat de rollen door verschillende personen worden uitgevoerd. In dit kader kunnen de volgende niveaus worden onderscheiden:

- **SD-SPC** Separation of Duties (= functiescheiding) – Single Party Control
  De Security Officer vervult de rol van Ceremoniemeester, Administratief Sleutelbeheerder en Kluisbeheerder. Hij/zij heeft hier het initiatief, coördineert, stuurt het proces aan en start procedures op. Een beheerder van de IT-afdeling vervult de rol van Technisch sleutelbeheerder en voert de technische werkinstructies uit.
- **SD-SPC-A** Separation of Duties – Single Party Control – Audited
  Als 1, maar nu uitgebreid met auditing. De rol van Auditor wordt ingevuld door een IT-auditor. De Administratief Sleutelbeheerder kan optreden als Auditor voor de Technisch Sleutelbeheerder.
- **SD–MPC–A** Separation of Duties – Multi Party Control – Audited
  Functiescheiding is hierbij dusdanig doorgevoerd dat geen enkel persoon een (deel van) een procedure alleen kan uitvoeren. Dit door benodigde kennis of fysieke middelen voor de gehele procedure over meerdere personen met functiescheidend tegengesteld belang te verdelen.

Het gewenste niveau van functiescheiding van de sleutelbeheer procedure wordt vastgelegd in het sleutel- of certificaatprofiel. De keuze komt tot stand op basis van een risicoanalyse. Ook kan worden opgeschaald bijvoorbeeld van SD-SPC naar SD-SPC-A bij compromittatie van een TLS certificaat.

Eigenschap	Key Encryption Key	Periodieke sleutel	Sessiesleutel
Doel	Encryptie van de periodieke of sessiesleutel	Symmetrische encryptie van de gevoelige gegevens	Symmetrische encryptie van de gevoelige gegevens
Soort	Publieke sleutel of geheime sleutel	Geheime sleutel	Geheime sleutel
Levensduur	1 jaar	Vastgestelde periode	1 sessie
Distributie	Fysiek (smartcard, CD-ROM, sleutellaadapparaat, papier) over vertrouwd pad	Beveiligd met KEK over communicatiepad zelf of over ander onvertrouwd pad	Beveiligd met KEK over communicatiepad zelf
		Fysiek over vertrouwd pad (geen KEK)	

Voorbeeld organisatie Sleutelhuis

Operationeel ontwikkelproces sleutelhuis
De Security Officer is verantwoordelijk voor de sleutelbeheer procedures en de Crypto Sleutelbeheer Database en beslist of hier onderhoud op kan plaatsvinden. Voor klein onderhoud gebeurt dit door de Security Officer zelf; groot onderhoud of functionele wijzigingen gebeuren in overleg met de IT-afdeling. Trigger voor dit proces is een eventuele constatering dat er nog ontbrekende sleutelbeheer procedures zijn. Voor de sleutelbeheer procedures vindt ontwikkeling plaats op twee niveaus:

1. Systeem onafhankelijke procedures, per type sleutel- of certificaatprofiel, voor alle fasen uit de lifecycle. Voor sommige procedures kan dit afdoende zijn voor een gecontroleerde uitvoering. Het raamwerk wordt uitgebreid indien er sprake is van een nieuw type sleutel of certificaat.
2. Technische werkinstructies, die, indien noodzakelijk, het generieke deel van de procedure uit het raamwerk aanvullen met systeem specifieke technische instructies.

Afwegingen

De inrichting van een sleutelhuis is voor een belangrijk deel afhankelijk van het beveiligingsniveau, de schaalgrootte en de verscheidenheid waarop encryptie wordt toegepast plus het belang van de ermee versleutelde gegevens. Naarmate het niveau hoger is, zullen procedures strikter zijn en de mate van functiescheiding toenemen. Een risicoanalyse kan inzicht geven in welke risico's met maatregelen, technisch, fysiek, procedureel of een combinatie, dienen te worden afgedekt. Dit wordt ook bepaald door hoe een organisatie met risico's omgaat: risicomijdend, risiconeutraal of risicodragend.
In risico afwegingen moet ook de werkbaarheid van de procedures worden meegenomen. "Onwerkbare" procedures zullen genegeerd worden en er zelfs toe leiden dat het beveiligingsniveau afneemt.

Implicaties

Het inrichten van een sleutelhuis in een organisatie kan betekenen dat huidige werknemers er nieuwe taken bij krijgen. Als deze er onvoldoende voor worden vrijgemaakt kan dat ten koste van de beveiliging gaan.

Gerelateerde patronen

- Themapatroon Encryptie
- Symmetrische encryptie: Toepassing symmetrische encryptie en sleuteldistributie
- Public Key Infrastructure: Toepassingsgebied asymmetrische encryptie en uitgifte van certificaten

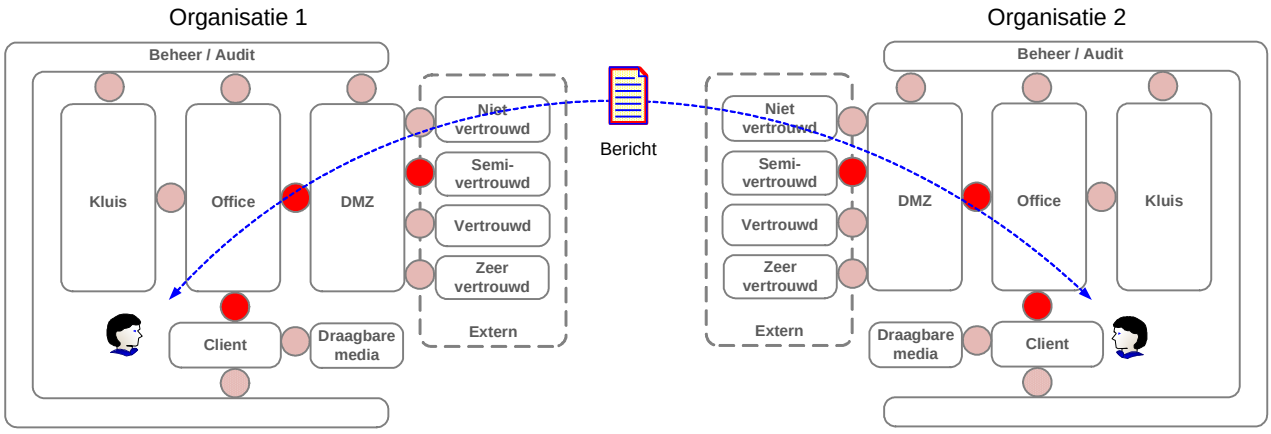
25. Elektronische handtekening

Criteria

Integriteit en Controleerbaarheid

Context

De toevoeging van een *elektronische* handtekening aan een bericht (document, e-mail, bestand), ook wel *digitale* handtekening genoemd, biedt de ontvanger de mogelijkheid om de identiteit van de ondertekenaar van het bericht te verifiëren. Tevens kan hij de integriteit (juistheid, volledigheid) van het bericht controleren (dus dat het ongewijzigd is sinds het verzonden is). Dit patroon richt zich op situaties waarbij het bericht los van enige context of andere beveiligingsmechanismen wordt beschouwd.



Omgeving waarin elektronische berichten worden uitgewisseld

Probleem

Tijdens transport en opslag, vormt het onopgemerkt wijzigen van berichten (of wijzigen door onbevoegden) een risico. De ontvanger heeft geen garantie dat het bericht integer is en dat het bericht afkomstig is van de identiteit, die als ondertekenaar bij het bericht staat vermeld (authenticiteit).

Oplossing

De elektronische handtekening geldt als bewijs van een wilsuiting wanneer het voldoet aan de eisen in de Wet Elektronische Handtekening (WEH), die inhouden:

- “Wanneer de zender een bericht voorziet van een elektronische ‘verzegeling’, waaruit de ontvanger met zekerheid kan afleiden dat het bericht ongewijzigd is en afkomstig is van de genoemde zender, dan fungeert dat ‘zegel’ als een elektronische handtekening”.
- De elektronische handtekening is inmiddels ook toepasbaar als wettig bewijs, met dezelfde juridische waarde als een gewone (fysieke) handtekening. In art.3:15a lid 4 Burgerlijk wetboek wordt de elektronische handtekening als volgt omschreven:
- “Een elektronische handtekening is een handtekening waarvan de elektronische gegevens zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel van authenticatie”.

De wet onderscheidt daarbij drie varianten, die als “zekerheidsniveau” kunnen worden gebruikt:

- Gewone elektronische handtekening.
- Geavanceerde elektronische handtekening.
- Gekwalificeerde elektronische handtekening.

Per niveau wordt daarmee bereikt:

(1) Authenticatie van elektronische gegevens
(2) Niveau (1) + Identificatie van eigenaar + Data integriteit + Onweerlegbaarheid van creatie
(3) Niveau (2) + kwalificatie van certificaat; uitgegeven door een bij de OPTA ingeschreven vertrouwde derde partij; meestal Trusted Third Party (TTP) genoemd.

Het laagste zekerheidsniveau (1) garandeert alleen de authenticiteit van het bericht. Daarvoor kan een controlegetal (hash) aan het bericht worden toegevoegd, of een pincode of wachtwoord worden gebruikt voor het bevestigen van de transactie.

Zekerheidsniveau (2) en (3) zijn qua techniek identiek en zijn beiden gebaseerd op een x.509 Public Key Infrastructure certificaat en gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen. Het verschil tussen (2) en (3) is de garantie omtrent het Public Key certificaat voor identificatie van zender en ontvanger. Onderstaande figuur schetst de processtappen voor een operationele toepassing.

In het algemeen valt het 'zetten' van de digitale handtekening uiteen in twee delen, wat leidt tot een unieke relatie tussen het bericht en de handtekening en biedt daarmee herleidbaarheid.

- Vastleggen van de unieke kenmerken van het bericht (in een 'hash').
- Verbinden van de unieke identiteit van de zender aan de hash.

De unieke identiteit van elektronische handtekeningen kan met behulp van verschillende mechanismen worden verbonden met het controlegetal, waarvan de bekendste zijn:

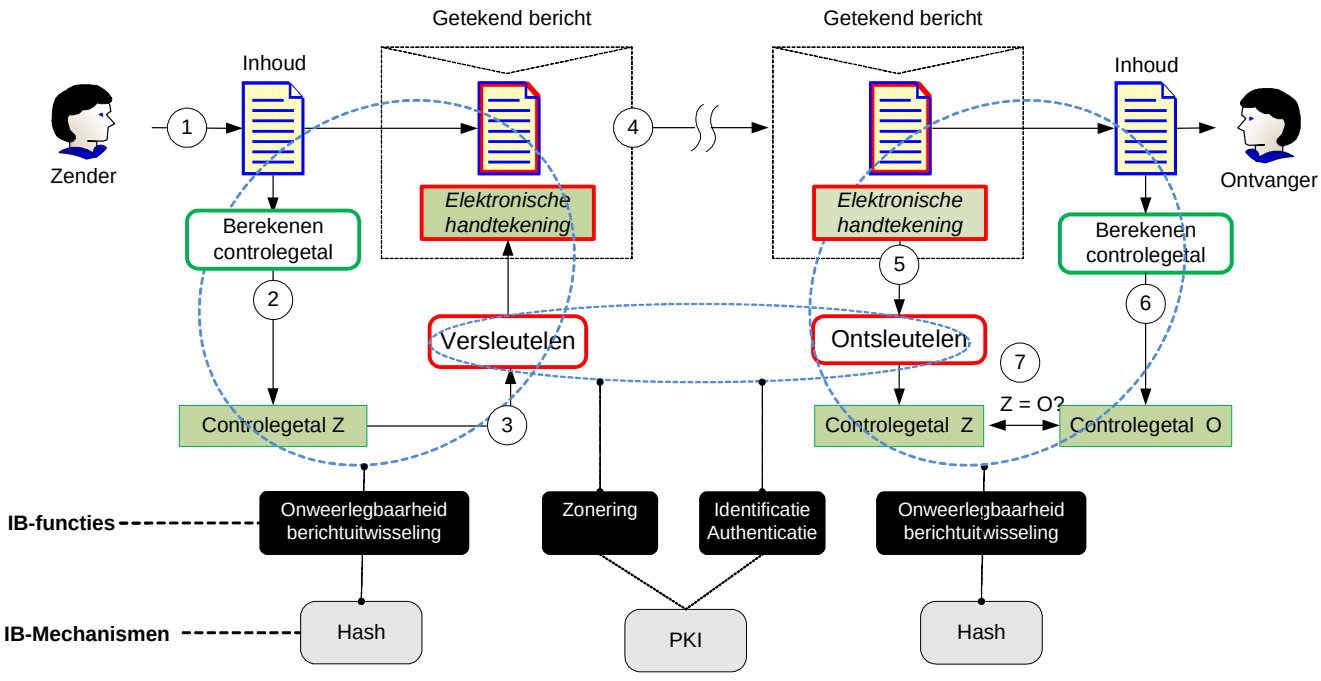
- Symmetrische cryptografische sleutels = vooraf uitgedeeld door regiepartij.
- Asymmetrische cryptografie op basis van PKI = uitgedeeld door een TTP.

De mate van zekerheid die uit de toegepaste methode voortvloeit, wordt sterk beïnvloed door de kwaliteit van de aard en toepassing van algoritmen en methoden en vooral van:

- Toevalsgetallen.
- Uniciteit en lengte van sleutels en toegangscodes.
- Sleuteluitgifte-, distributie- en bewaarprocessen en middelen.
- Kwalificatie van de certificaatuitgifte.

Onderstaande tabel geeft aan welke verbanden er bestaan tussen het zekerheidsniveau, de toegepaste sleutels en wie er door zender en ontvanger wordt vertrouwd.

Zekerheidsniveau	Sleutelmodel	Proceskwaliteit	Zender en ontvanger vertrouwen:
1: Laag, onzekere bewaartermijn	Symmetrisch	Gedeelde sleutels	Eigen organisatie of partner
2: Middel, onzekere bewaartermijn	Asymmertrisch	PKI service of private PKI	Eigen organisatie of partner
3: Hoog, gegarandeerde bewaartermijn	Asymmetrisch	PKIoverheid	Overheid of gecertificeerde partij



Bericht met elektronische handtekening

De uitgeschreven processtappen gelden voor de toepassing van PKI.

1. De zender stelt een bericht op.
2. Over de inhoud van het bericht wordt een controlegetal berekend, de z.g. Hash. Voor de berekeningsmethode van de Hash wordt een standaard algoritme gebruikt, dat door elke infrastructuur die deze standaard ondersteunt is toe te passen.
3. Het controlegetal wordt versleuteld met de private key van de zender en bij de al dan niet versleutelde

berichtinhoud gevoegd als een Elektronische handtekening. Versleutelen van de inhoud van het bericht is mogelijk. Dit maakt verder geen deel uit van het patroon voor elektronische handtekening.
4. Het bericht wordt compleet met handtekening verstuurd.
5. Van het bericht wordt de handtekening ontsleuteld met de public key van de zender, waarna het controlegetal (Z) van de zender herkenbaar wordt.
6. Van de inhoud van het bericht wordt aan de ontvangkant opnieuw een controlegetal (O) berekend.
4. Tenslotte wordt het meegestuurde controlegetal (Z) vergeleken met controlegetal (O). Wanneer deze getallen precies gelijk zijn, dan is daarmee bewezen dat:
5. De inhoud van het bericht niet is gewijzigd
6. Het bericht afkomstig is van de zender van de overeenkomende public key of gedeelde symmetrische sleutel en daarmee heeft de zender zich bij de ontvanger geauthenticeerd.

Daarmee is het bericht geverifieerd.

Afwegingen

In deze oplossing wordt vanwege de eenvoud alleen het controlegetal versleuteld, waarmee in combinatie met de private key de integriteit van het bericht én de identiteit van de zender kan worden aangetoond. Wanneer vertrouwelijkheid van het bericht ook vereist wordt, dan kan het bericht zelf ook worden versleuteld, maar dit maakt geen onderdeel uit van de elektronische handtekening.
Vanuit gebruikersperspectief spelen de vragen:

- Welke sleutel moet voor deze toepassing gebruikt worden?
- Hoe wordt vastgesteld dat de juiste data getekend wordt?
- Kan in deze omgeving de gekozen handtekening veilig geplaatst worden?

Voorbeelden

Zekerheidsniveau 1:

- Het indienen van een belastingaangifte met DigiD.
- Het gebruik van een wachtwoord om een document te ondertekenen.

Zekerheidsniveau 2 en 3:

- Uitwisselen van akten tussen Notarissen en het Kadaster.
- E-factureren.

Implicaties

- De keuze voor de elektronische handtekening impliceert, dat organisaties een keuze maken voor een bepaald niveau van beveiliging en het gewenste zekerheidsniveau voor de handtekening. Afhankelijk van dat niveau moeten de verschillende partijen beschikken over de juiste technische hulpmiddelen (cryptografie en rekencapaciteit) en organisatie-inrichting (sleutelbeheer).
- Beoogde levensduur van de bescherming. Een handtekening moet over 30 jaar nog steeds betrouwbaar zijn!
- Kosten (her-) uitgifteproces van certificaten.

Gerelateerde patronen

PKI (Public Key Infrastructure), dat als mechanisme gebruikt wordt voor identificatie en authenticatie van zender en ontvanger

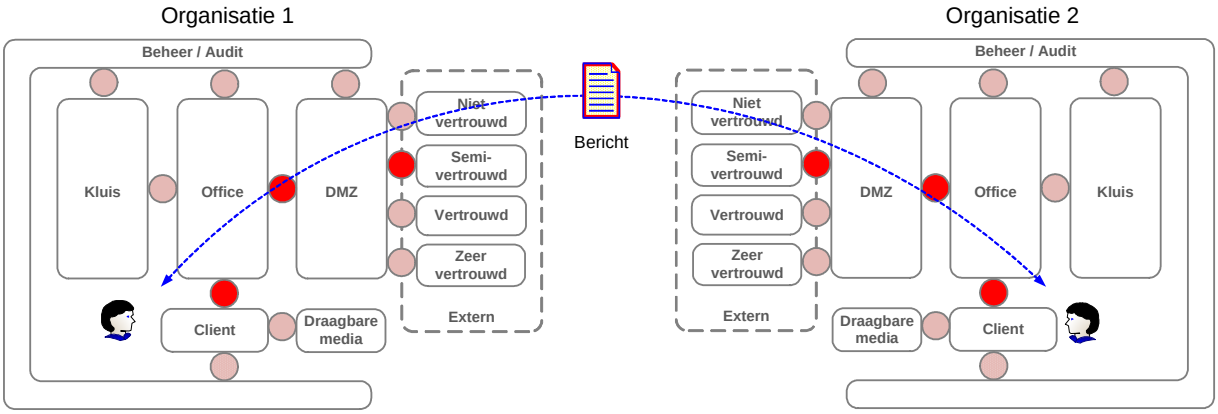
26. Secure E-mail

Criteria

Vertrouwelijkheid, Integriteit

Context

Men wisselt e-mailberichten uit tussen verschillende organisaties of natuurlijke personen. Daarbij kan niet worden uitgegaan van een vertrouwd (toegangs)pad. Toch vraagt de inhoud van het bericht om een bepaald niveau van vertrouwelijkheid. Ook wil de zender dikwijls meer zekerheid hebben over het tijdig en goed afleveren van het bericht aan de juiste ontvanger.



Uitwisseling van elektronische berichten

Probleem

Tijdens transport van de e-mail tussen de verzender en de ontvanger vormen ongewenst inzien en aanpassingen van het e-mailbericht door een buitenstaander risico's. De betrokkenen (zowel zender als ontvanger(s)) hebben geen enkele garantie dat een e-mailbericht onderweg niet wordt ingezien door andere partijen (vertrouwelijkheid). Ook is er geen garantie dat het bericht door een buitenstaander niet gewijzigd is (integriteit). Een derde probleem is dat de afzender niet eenduidig kan bewijzen dat het bericht verstuurd is en wanneer het bericht de geadresseerde heeft bereikt. De onweerlegbaarheid van de verzending en van de aankomst van het bericht en de tijdstippen daarvan is normaliter niet geregeld.

Oplossing

De oplossing is het beveiligen van het bericht voordat het de vertrouwde omgeving verlaat. Hiervoor zijn drie standaard oplossingsrichtingen bekend:

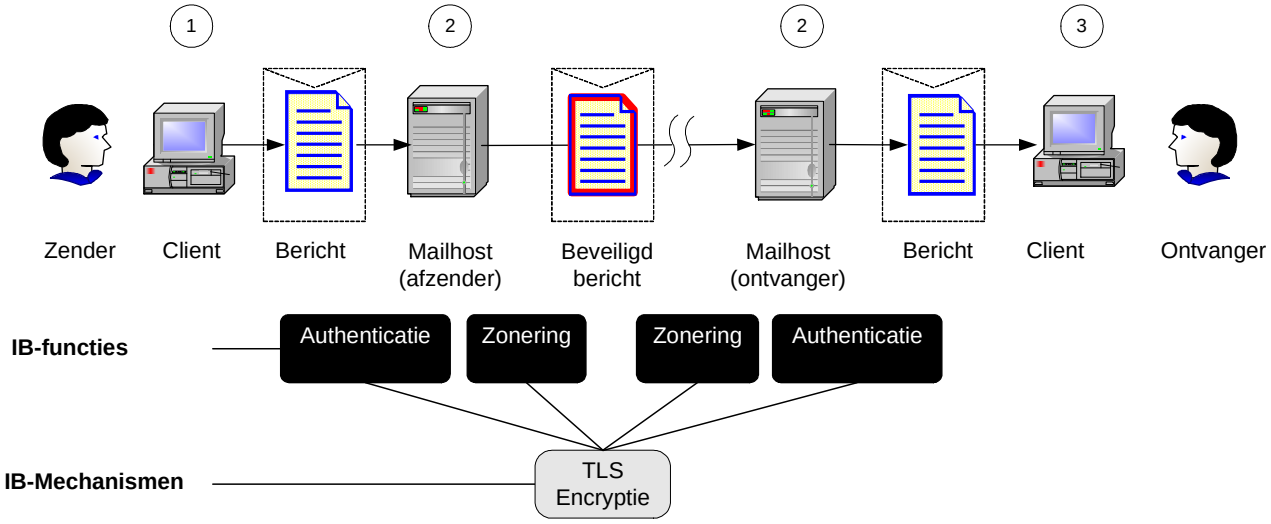
1. **Host-to-Host via het reguliere e-mailkanaal**
   Bij deze oplossing wordt een beveiligde verbinding opgezet tussen de mailservers van ketenpartners die beveiligde e-mail met elkaar willen uitwisselen. Daarvoor wordt TLS (Transport Layer Security) op de met elkaar communicerende mailservers geactiveerd, zodat een versleutelde verbinding door de mailserver kan worden opgezet met een andere host. De communicatie tussen mailserver en werkstation is echter niet versleuteld. Voor de beveiliging daarvan wordt vertrouwd op de genomen maatregelen voor beveiliging van het interne netwerk.

2. **End-to-end via het reguliere e-mailkanaal.**
   Bij deze oplossing blijft de e-mail over het hele traject tussen zender en ontvanger versleuteld. De afzender versleutelt het bericht. Het versleutelde bericht wordt naar de bestemming verstuurd. De geadresseerde ontsleutelt het bericht en heeft deze dan beschikbaar voor verwerking. Voordat men op deze manier mail kan uitwisselen met een communicatiepartner, moet er afstemming hebben plaatsgevonden over het uitwisselen van encryptiesleutels met elkaar.

3. **End-to-end via een 'secure host'.**
   De communicatie vindt plaats via een vaste vertrouwde tussenpersoon (een computer). De verbinding tussen de afzender en de host wordt beveiligd evenals de verbinding tussen de geadresseerde(n) en de host. De dienstverlener houdt meestal een administratie bij over de aankomst van het bericht en wanneer welke geadresseerde het bericht heeft opgehaald, voor de afzender is informatie over zijn berichten veelal inzichtelijk.

1. Uitwerking Host-to-Host via het reguliere e-mailkanaal

Bij deze methode wordt het bericht versleuteld in de Mailhost zoals hieronder is geschetst. Het is de eenvoudigste oplossing, die kan worden benut door op zowel de zendende als ontvangende mailhost TLS te activeren. Dit blijft meestal beperkt door 'een vinkje aan te zetten'.

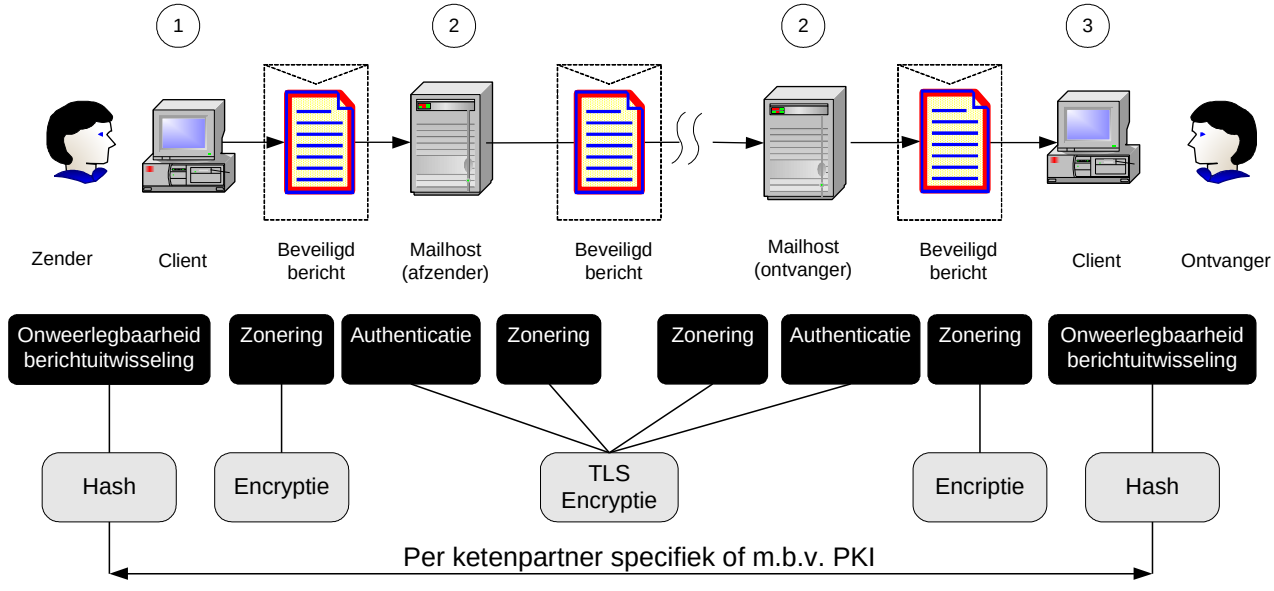


Host-to-host e-mail beveiliging met TLS

Het versturen van e-mail gaat voor de gebruiker op precies dezelfde manier als voor onversleutelde e-mail. De stappen zijn: (1) zender stelt mail op. (2) De mailhost van afzender zet een TLS-sessie op met de mailhost van de ontvanger en verstuurd een versleuteld bericht. Aan de ontvangstkant ontsleutelt de mailhost het bericht en stuurt het naar de Ontvanger (3).

3. Uitwerking End-to-End via het reguliere e-mailkanaal

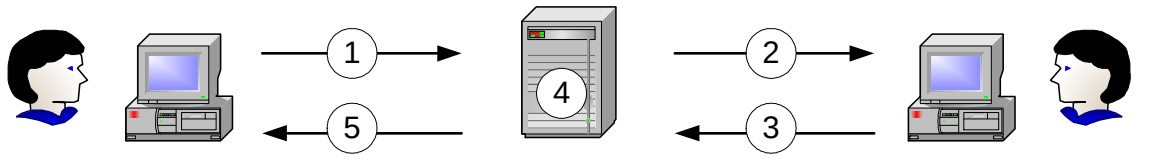
Hiervoor is een versleutelde verbinding opgezet tussen werkstations en mailhost én tussen de mailhosts onderling. Daarbij kan gebruik worden gemaakt van een Public Key Infrastructure (PKI) of van clientspecifieke oplossingen, zolang de hele keten maar is versleuteld.



End-to-end e-mail beveiliging

Het versturen van de e-mail gaat in de volgende stappen: (1) De afzender stelt met zijn standaard e-mailpakket het bericht op en selecteert de optie voor beveiligde verzending. Bij het versturen wordt het bericht voorzien van de noodzakelijke en/of gewenste bewerkingen (zoals ondertekening en/of versleuteling). (2) Het bericht wordt verwerkt op de interne e-mail server en gerouteerd naar de ontvanger. Wanneer het bericht is ontvangen op de mailserver van de ontvanger, wordt de beveiligde e-mail afgeleverd in de mailbox van de ontvanger. (3) De ontvanger opent het bericht, net als elk ander bericht, waarop het bericht wordt (al dan niet automatisch) ontsleuteld. De ontvanger ziet meestal duidelijk dat het hier gaat om een extra beveiligd bericht.

3. Uitwerking End-to-end via een externe 'secure host'.
Deze methode maakt gebruik van een serviceprovider 'in the middle'. Het zenden en ontvangen van e-mail verloopt altijd via deze serviceprovider met de volgende processtappen:



End-to-end e-mail beveiliging via een secure host

(1) De afzender zet een (beveiligde) verbinding op met de host. Hij deponeert het bericht inclusief de lijst van geadresseerden. Het bericht wordt beveiligd opgeslagen op een server van de host.
(2) De host verstuurt een attentiebericht (reguliere e-mail) aan iedere geadresseerde met daarin de informatie dat er een bericht klaar staat.
(3) De geadresseerde zet een (beveiligde) verbinding op met de host en krijgt het bericht beschikbaar voor lezen en verdere verwerking.
(4) Het hostsysteem registreert de handelingen. Hij registreert de binnenkomst van de e-mail alsook welke geadresseerde het bericht wanneer heeft opgehaald.
(5) De afzender vraagt de registratie op en ontvangt de registratie Hij weet nu wanneer welke geadresserden het bericht hebben opgehaald.

Gebruikers van deze mailservice kunnen een automatische bevestiging krijgen, of de geadresseerde het bericht heeft opgehaald en wanneer dat gebeurde. De communicatie moet lopen via een vertrouwd toegangspad naar de host. Het authenticatiemechanisme moet van een zodanig niveau zijn, dat past bij de gewenste vertrouwelijkheid van de te versturen informatie.
De host-based oplossing kan ook in eigen beheer uitgevoerd worden. Een organisatie beheert daarbij een server, waarbij de relaties van de organisatie de berichten kunnen ophalen.

Afwegingen

Voor alle methoden van beveiligde berichtenuitwisseling geldt dat de grensbeschermingen in de berichtenketen versleutelde berichten onverkort moet kunnen doorlaten. Dit heeft als consequentie dat contentscanning op malware en virussen etc. niet centraal kan worden geregeld. Dit risico moet worden afgewogen tegen de voordelen van beveiligde mail.

Per gekozen methode zijn verder de volgende punten van belang:

Via het reguliere e-mailkanaal
End-to-end. Voordeel van End-to-end is dat de mail beveiligd is tegen kwaadwillenden op het interne netwerk. Het nadeel is dat de mail versleuteld door de grensbescherming van een organisatie moet en er geen centrale screening op malware plaats kan vinden van het inkomende en het uitgaande verkeer. Controle over het hele proces inclusief het verzenden en het bereiken van de geadresseerde kan via elektronische handtekening, die uitsluitsel geeft over de authenticiteit van het ontvangen bericht.

Host-to-host. Nadeel van TLS host-to-host oplossing is dat de gebruiker er niets van merkt wanneer onverhoopt een ontvangende mailhost niet voor TLS is geconfigureerd. De gebruiker heeft vanuit zijn perspectief dus geen zekerheid over de beveiliging van het transportkanaal voor zijn bericht.

Host-Based met service provider
Voordeel van de Host-based oplossing is dat het e-mailproces volledig geregistreerd wordt. Men kan laten vastleggen door de host wanneer de mail verzonden is. Nadeel is het vertrouwen dat nodig is in de serviceprovider met bijkomende kosten voor audits etc. De kosten van de serviceprovider moeten worden afgewogen t.o.v. kosten van PKI-oplossingen.

Voorbeelden

Host-based e-mail komt voor bij verschillende banken. Banken hebben al een authenticatiemechanisme uitgerold voor hun cliënten voor elektronisch bankieren. Hetzelfde authenticatiemechanisme kan gebruikt worden voor secure e-mail.

Er zijn Amerikaanse bedrijven die diensten aanbieden voor host-based e-mail.

Implicaties

De *End-to-end* methode via het reguliere e-mail kanaal vereist, dat de zender en de ontvanger over elkaars encryptiesleutels kunnen beschikken. Dit kan op meerdere manieren gebeuren, waaronder het onderling uitwisselen van sleutels via een beveiligd kanaal. Het uitwisselen van sleutels en het beheer ervan is arbeidsintensief en kostbaar bij grote aantallen communicatiepartners. Hierbij kan gebruik gemaakt worden van een PKI-infrastructuur, waarbij de afzender een publieke sleutel van de geadresseerde ophaalt en deze gebruikt om het bericht te versleutelen. Een andere oplossing is de sleutels rechtstreeks met de geadresseerde uit te wisselen. Dit moet via een ander vertrouwd kanaal gebeuren, bijvoorbeeld fysieke post met een tamper-proof enveloppe.

De *TLS host-host* oplossing vereist dat alle mailservers die in de keten beveiligde berichten moeten uitwisselen zijn geconfigureerd voor TLS. Deze methode vereist aanvullende maatregelen om te zorgen dat gebruikers geen fouten maken met het mailen van gevoelige informatie via onbeschermd kanalen.

De *Host-Host met serviceprovider* oplossing impliceert dat de serviceprovider vertrouwd wordt. Dit gaat zowel om het vertrouwen in de kwaliteit van het bewaren van de berichten, als in de kwaliteit van de authenticatieprocedures en –hulpmiddelen. De serviceprovider rekent een bedrag per verstuurd bericht. Met de serviceprovider moeten contractuele afspraken gemaakt worden over het beveiligingsniveau en het uitvoeren van interne en externe audits.

Er moet ook een besluit genomen worden over de delen van het bericht die moet worden versleuteld: alleen de *berichtbody*, of ook de *header* met het subject.

Voor TLS moet minimaal de versie 1.2 worden gebruikt in verband met zwakheden in vorige versies. NIST heeft een standaard uitgegeven die alle beveiligingsaspecten rond dit onderwerp bespreekt.

Gerelateerde patronen

- **PKI**, te gebruiken voor het uitwisselen van encryptiesleutels en digitale ondertekening
- **Vertrouwd Toegangspad**, voor het maken van de verbinding met de host bij host-based secure e-mail.
- **Elektronische handtekening** voor ondertekening van e-mail via het reguliere kanaal
- **Logging**, vastlegging van alle relevante gebeurtenissen in het systeem.

27. Logging

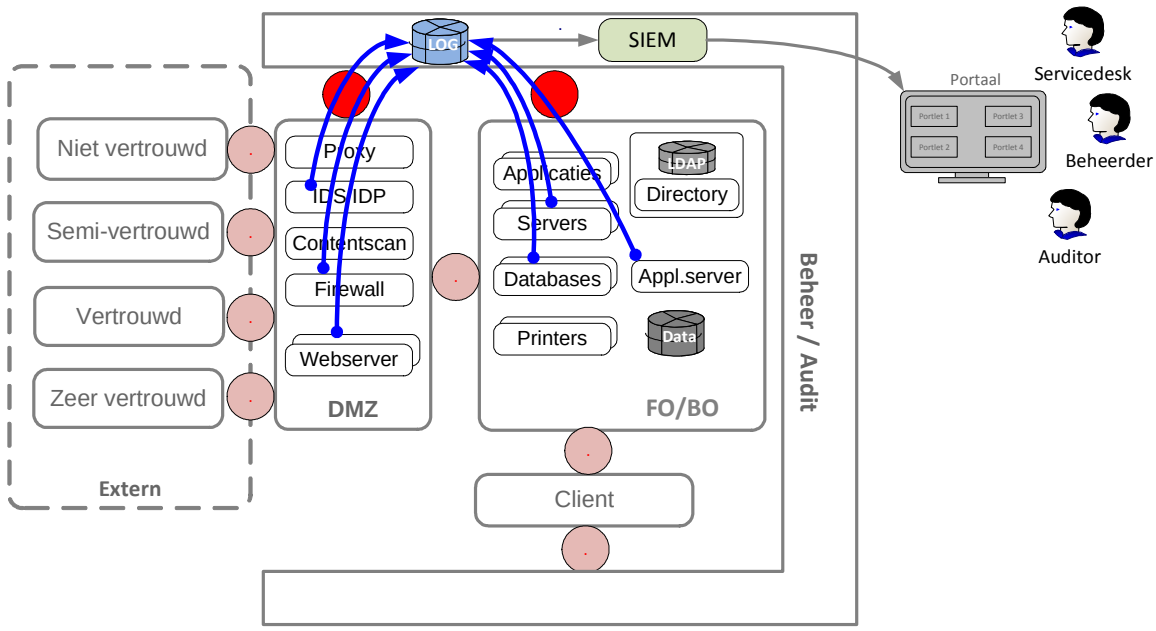
Criteria

Controleerbaarheid

Context

Veel gebeurtenissen die voor het beheer van IT-voorzieningen van belang zijn, hebben tevens betekenis voor informatiebeveiliging en worden daarom vastgelegd ofwel gelogd. Loggegevens kunnen zowel betrekking hebben op handelingen van natuurlijke personen als op het gedrag van informatiesystemen. Daarnaast zijn er andere doelen zoals technisch beheer, productiebesturing, capacitymanagement, configurationcontrol, SLA compliancemonitoring etc. Dit patroon beperkt zich tot vastleggen van gegevens voor informatiebeveiliging en richt zich op technische logging. Functionele logging door applicaties zoals *transactionele* logging en *audittrails* vallen hier buiten.

Loggegevens over personen kunnen dienen als wettig bewijsmateriaal, waarmee onwettige handelingen aangetoond kunnen worden. Loggegevens kunnen ook betrekking hebben op ongewenste handelingen, die niet in overeenstemming zijn met het organisatiebeleid. Deze gegevens worden daarom zeer vertrouwelijk behandeld.



Vastleggen van gebeurtenissen.

Probleem

De problematiek van het vastleggen van gebeurtenissen benaderen we vanuit twee gezichtpunten:
a) *Waarom* loggen? En b) *Wat komen we tegen* als we logfuncties willen inrichten of verbeteren?

1. De problemen die via het vastleggen van gebeurtenissen geheel of gedeeltelijk opgelost kunnen worden zijn:

a) **Misbruik** door gebruikers van informatiesystemen.
b) **Aanvallen** op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (systemen).
c) **Onderbrekingen** van dienstverlening als gevolg van gebruikersfouten of configuratiefouten.
d) **Falende componenten** en **kritisch- relevante meldingen** worden niet (tijdig) opgemerkt.

2. De problemen die zich voordoen bij het vastleggen van gebeurtenissen zijn de volgende:

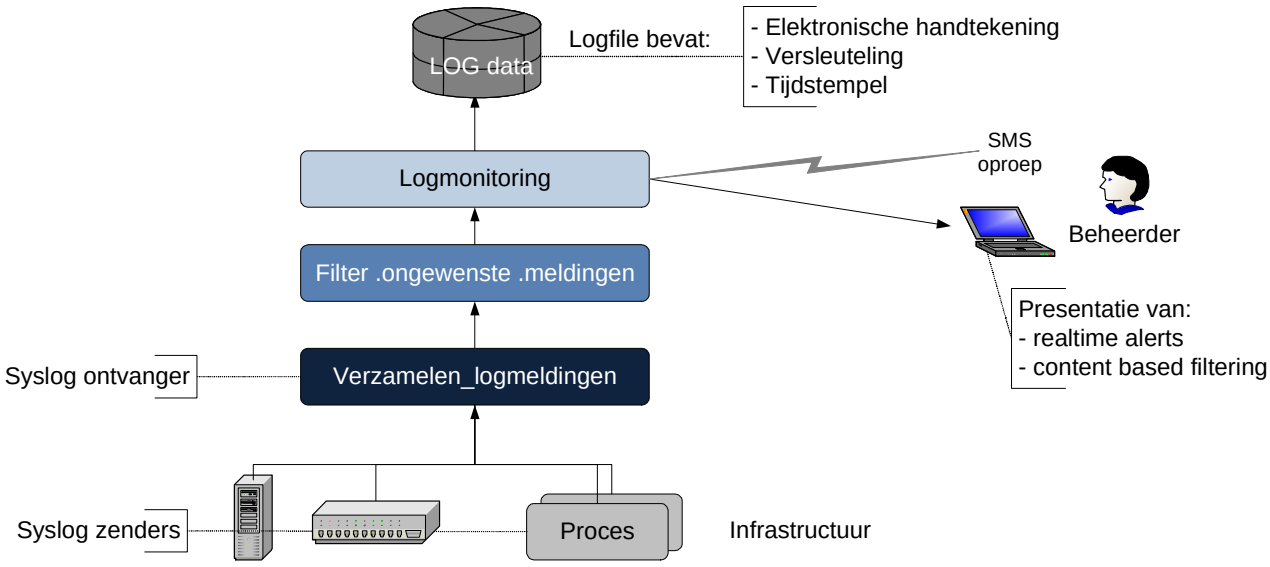
a) **Onduidelijk logbeleid**. Beleidsregels zijn niet duidelijk t.a.v. welke gebeurtenissen moeten worden gelogd en welke niet, wat leidt tot een “alles of niets” gebruik van logfuncties.
b) **Hoeveelheid meldingen** is zo groot dat dit leidt tot vollopen van opslagmedia.
c) **Beheerders kunnen logfiles wissen.** Configuratiefouten of misbruik door beheerders kunnen worden gemaskeerd omdat beheerders logfiles in systemen kunnen wissen.
d) Incidenten oplossen in plaats van het voorkomen van incidenten

Oplossing

Logbeleid wordt vastgesteld, waaruit kan worden afgeleid welk type gebeurtenissen moeten worden vastgelegd. Zie hiervoor richtlijnen voor logging in het toegepaste normenkader IT-voorzieningen.

Een ‘standaard’ technische voorziening voor logging van infrastructuur componenten is: *Syslog*. Syslog is een client/server protocol dat is beschreven in RFC 3164: “The BSD syslog Protocol”. Het wordt ondersteund door een groot aantal componenten en werkt over meerdere hardware platformen.

Werking: De Syslog zender stuurt kleine tekstberichten (< 1kB) van gebeurtenissen naar de Syslog ontvanger, die ‘*Syslogd’*, *‘Syslog deamon’ of ‘Syslog server’* wordt genoemd. Voor transport wordt het UDP netwerkprotocol, of SSL/TLS protocol gebruikt. Hieronder is de logarchitectuur geschetst.



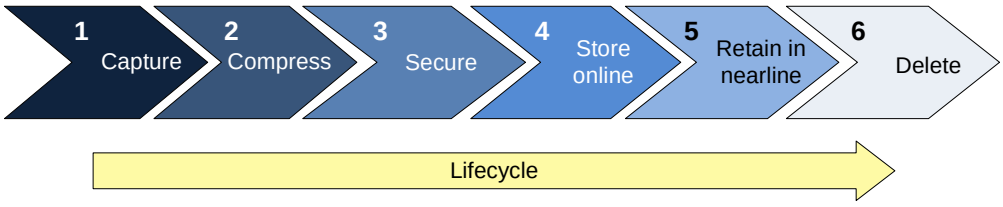
Architectuur van logging

De verzamelde logmeldingen worden vervolgens *gefilterd* en *gecomprimeerd*, waarmee de hoeveelheid te bewaren informatie aanzienlijk wordt beperkt. Filtering wordt ingesteld op basis van het vigerende *log-beleid* van een organisatie. Meldingen worden vanuit *kritische* bedrijfsfuncties ‘real-time’ gevolgd via de Log Monitoring functie, en wel op basis van z.g. ‘content-based filtering’. De alarmering wordt geregeld met behulp van SMS-oproepen. NB: deze alarmering is niet per definitie dezelfde als de monitoringfunctie van Security Information Event Management (SIEM), maar kan wel door een SIEM omgeving worden uitgevoerd.

De log-informatie wordt vervolgens voorzien van een *Hash*, een *Tijdstempel*, een *Severity*- (ernst) aanduiding en een *Sequencenummer*, waarna het vervolgens *‘write once’* versleuteld wordt opgeslagen in een database. Eventuele modificatie, toevoeging of verwijdering van de geregistreerde informatie wordt hiermee detecteerbaar. Vervolgens kan log-data voor analyse en auditing beschikbaar worden gesteld aan platform specifieke tools of aan generieke log-analyse systemen zoals SIEM.

Binnen een te loggen object kunnen diverse types logfiles ontstaan. Dit kunnen zowel “flatfiles” zijn, maar ook loginformatie, opgenomen in een database. Al deze types moeten door het verzameltool ingelezen kunnen worden. Het verwijderen van loggegevens moet met de nodige waarborgen omkleed zijn, zoals het ‘vier-ogen’ principe en het opmaken van een protocol.

De lifecycle van log-informatie doorloopt de onderstaande fasering:



Levenscyclus van loginformatie

Gevoeligheid van loginformatie

In elke zone (DMZ, Frontoffice, Backoffice etc.) vinden gebeurtenissen plaats, die voor registratie in aanmerking komen. De beveiligingsgerelateerde gegevens van die gebeurtenissen worden vastgelegd met toevoeging van datum/tijd, identificatie van locatie, machine, proces, applicatieversie en in geval van gebruikershandelingen de identificatie van de betrokken gebruiker en zijn privileges.

Om ongewenste vermenging tijdens collectie van loggegevens van verschillende gevoeligheidsniveaus tegen te gaan, wordt elk record voorzien van een gevoeligheidsaanduiding, in overeenstemming met de gevoeligheid van de loggingbron. Bij het extraheren van loggegevens wordt daarmee voorkomen dat hooggevoelige gegevens op ongewenste momenten in het extract terechtkomen. Het gevoeligheids- of beveiligingsniveau van een loggingbron wordt bepaald aan de hand van het beveiligingsbeleid.

Als loggegevens met verschillende gevoeligheidsaanduiding worden samengevoegd, krijgt de logfile het gevoeligheidsniveau, dat gelijk is aan dat van de meest gevoelige loggegevens.
Per logrecord wordt een *severity*-aanduiding vastgelegd. Tijdens de analyse kan hierop geselecteerd worden om b.v. in eerste instantie alleen de ernstigste meldingen te laten zien.

Doorgaande cyclische logging, waarbij op een bepaald moment de nieuwste records de oudste logs overschrijven, is niet toegestaan. Als een logfile een bepaalde instelbare maximumafmeting heeft bereikt, dan wordt deze na het toevoegen van een hash afgesloten en wordt een nieuwe logfile gestart. De hash wordt over de hele logfile berekend en is nodig om eventuele modificaties achteraf te kunnen aantonen.

Bij de opslag wordt de logfile write-once encrypted opgeslagen. Daarmee is de logfile beveiligd tegen modificatie en tegen onbevoegde raadpleging. Uitwisseling van informatie tussen systemen van twee organisaties wordt tweezijdig gelogd, voor wat betreft al dan niet succesvolle communicatie en het tijdstip waarop dit heeft plaatsgevonden.

Het loggingproces zelf wordt ook gelogd (beheer en beveiliging van beveiliging). Voor het beheer van het loggingproces geldt dezelfde eis als voor de logfiles: de beheerder (of securitymanager) heeft niet de mogelijkheid om zonder hulp van een tweede geautoriseerde persoon het loggingproces aan te passen of logfiles te verwijderen (4-ogen principe). Deze log wordt toegevoegd aan de collectie zelf en aan de nieuwe collectie.

Afwegingen

Om logging beheersbaar te houden en te voldoen aan de ‘geest’ van de wet, wordt bewust gekozen welke gebeurtenissen wel- of niet worden gelogd, op welke wijze logfiles worden opgeslagen (al dan niet versleuteld) en hoe lang de minimum- en maximum bewaartermijn kan- of moet zijn
(De archiefwet geeft geen bewaartermijnen aan).

Voorbeelden

Toepassingsmogelijkheden: Forensisch onderzoek, tactisch en operationeel beheer (SIEM), audit, SLA compliance monitoring.

Implicaties

- Als verleuteling wordt toegepast dient het sleutelbeheer adequaat geregeld zijn. (zie patroon Sleutelhuis).
- Opslag technieken kunnen veranderen, waardoor loginformatie op een nieuw medium moet worden opgeslagen, hetgeen om integriteitswaarborgen vraagt.
- Voor beheer van loggegevens zijn alle fasen van lifecycle management vereist, dat wil zeggen, vanaf registratie tot en met vernietiging (zie levenscyclus Log-informatie).
- Er moet rekening worden gehouden met de verplichting om logfiles na een bepaalde bewaarperiode te vernietigen. De bewaartermijn kan voor de diverse soorten logfiles, afhankelijk van de daarin vastgelegde gegevens, sterk verschillen.
- Het gaat om veel data: (gebeurtenissen/sec) x (sec/jaar) x (gemiddelde recordgrootte) = xyzTByte.

Gerelateerde patronen

- Elektronische handtekening voor zekerheid over de integriteit van logbestanden
- Symmetrische encryptie voor vertrouwelijke opslag
- SIEM voor verzamelen en correleren van loginformatie

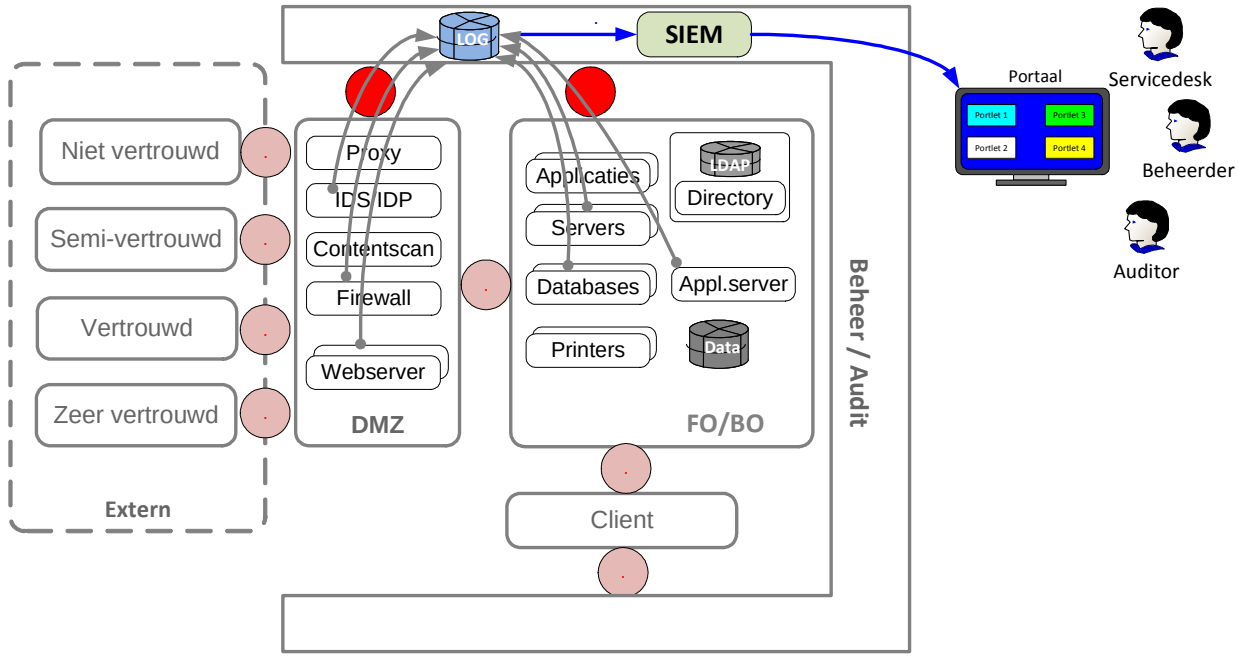
28. Security Information Event Management (SIEM)

Criteria

Integriteit en Controleerbaarheid

Context

Vastleggen van gegevens wordt gedaan op basis van doelstellingen en beleidsregels, zoals uiteen is gezet in het patroon Logging. Voor Monitoring geldt dezelfde context, maar nu gericht op het vertalen, bewerken en rapporteren van die gegevens aan de verschillende doelgroepen.



Gebruikers van vastgelegde gebeurtenissen

Probleem

In uitgebreide IT-infrastructuren is het onmogelijk om zonder geautomatiseerde hulpmiddelen voldoende inzicht en overzicht te houden op de beoogde werking van beveiligingsmaatregelen en welk afwijkend communicatiegedrag er plaatsvindt.

Oplossing

Voor bewaken en beoordelen van de werking van genomen beveiligingsmaatregelen in de IT-infrastructuur als resultaat van de naleving van beveiligingsbeleid worden de volgende services ingezet:

1. Security Information Event Management: *Monitoring & analyse van afwijkend gedrag in IT*
2. Vulnerability Management: *Vaststellen en wegnemen van kwetsbaarheden in IT*
3. Security Policy Compliancy Management : *Controleren implementatie van beleidsregels in IT*

Deze services vormen in samenhang het geheel van de beveiligingsfunctie: Controle, Alarmering en Rapportering.

Dit patroon geeft een uitwerking van service *Security Information Event Management (*SIEM). Deze service is evenals logging gepositioneerd in het beheerdomein. SIEM is een belangrijk onderdeel voor de toetsing op naleving van beveiligingsbeleid, maar is daarin slechts één van de drie instrumenten. De naleving van het beleid steunt daarom evenzeer op de processen voor *Vulnerability Management* en *Policy Compliance Management*. Deze services vereisen in hun probleemstelling en oplossing echter ieder een eigen patroon.

SIEM is een stelsel van voorzieningen, dat voorziet in het continu, (near-) realtime monitoren van beveiligingsmaatregelen en afwijkend gedrag in infrastructuren. Het voorziet in lange-termijn opslag van verzamelde gegevens en in historische- en trendanalyse van die gegevens.

SIEM biedt naast monitoring ook functies voor forensisch onderzoek.

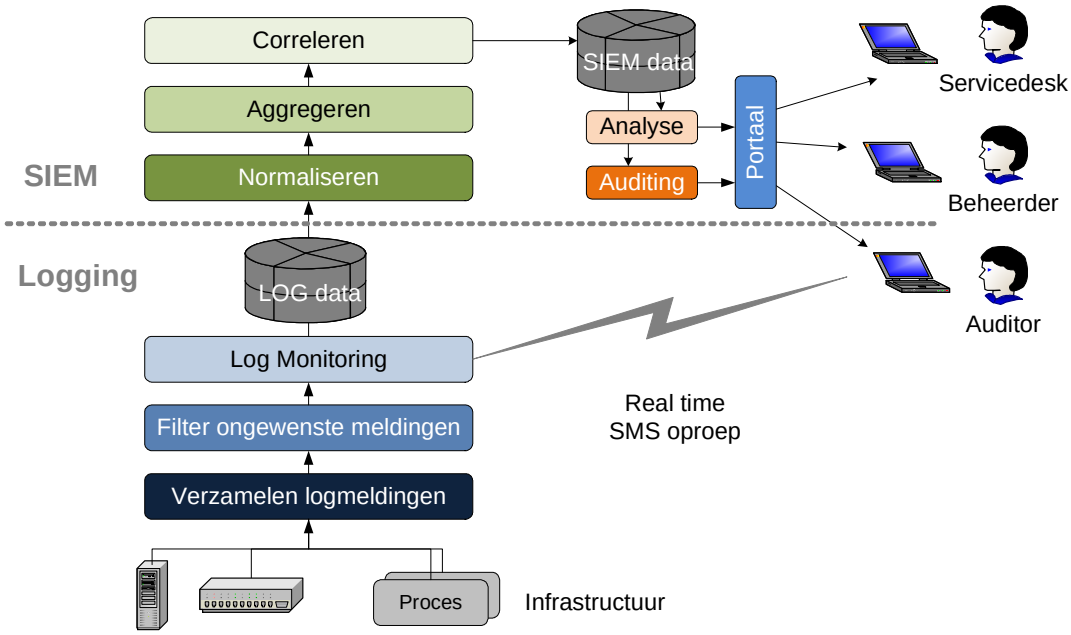
Onderstaand figuur geeft aan uit welke functieblokken SIEM is opgebouwd. Vanuit de verschillende bronsystemen wordt log- en andere relevante systeeminformatie verzameld.

De subprocessen voeren in samenhang met logging-functie de volgende bewerking uit op de informatie:

1. Logging : log- en statusinformatie wordt vanuit verschillende platformen opgevraagd en opgeslagen in een LOG database.
2. Normaliseren : omzetten van logfiles uit verschillende platformen naar een standaard formaat.
3. Verrijken : toevoegen van context, waarmee de informatiewaarde op het gewenste niveau gebracht wordt.
4. Aggregeren : intelligent bundelen van log gegevens van verschillende gebeurtenissen.
5. Correleren : leggen van relaties tussen gebeurtenissen

Vervolgens wordt deze informatie met de originele melding tijdelijk opgeslagen en voor weergave op een dashboard en geschikt gemaakt als rapportagefunctie. De Security Information Datawarehouse functioneert als een ‘verzamelbak’ van beveiligingsgerelateerde informatie voor lange termijn opslag.

SIEM maakt gebruik van Network Behavior Anomalies (NBA) technieken. Op basis van baselines wordt afwijkend gedrag in netwerk-gebruik gedetecteerd en desgevraagd gecorreleerd met andere gebeurtenissen.



Totale keten van logging en SIEM

Met behulp van correlatie van de data uit de logfiles kunnen afwijkende patronen gevonden worden die tot een alarm in de beheersystemen kunnen leiden. Dit proces vindt plaats zonder dat een beheerder de mogelijkheid heeft om bepaalde gegevens uit de geaggreeerde en gecorreleerde logdata te verwijderen of te veranderen.

Het portaal biedt op basis van strikte autorisaties (en functiescheiding) toegang aan de verschillende gebruikers in de servicedesk, voor beheer en audit. Het biedt samengevat functies om verzamelde en gecorreleerde gebeurtenissen in te zien en te gebruiken. Vanuit het portaal kunnen rapportages worden gegenereerd over SIEM-data.

Analyse
In het proces Analyse voert een bevoegde medewerker analyses uit op de data. Dit is uitsluitend mogelijk via een daartoe toegeruste analyse tool, bij voorkeur via een portaal. Het portaal verzorgt toegangscontrole en logging van het analyseproces, omdat ongecontroleerde raadpleging niet toegestaan is. De tool moet op diverse aspecten van de loggegevens kunnen selecteren, zoals: datum/tijd, sequencenummer, gevoeligheidsniveau, severity, persoons- of procesidentificatie en combinaties daarvan.

Auditing
De raadpleegtool kan desgewenst extracten voor juridisch gebruik produceren, waarbij de integriteit van de gegevens moet worden gewaarborgd. Bewijsmateriaal voor juridische doeleinden wordt alleen verzameld na afstemming met het hoogste management. Auditloggegevens, als onderdeel van SIEM data, worden gedurende een afgesproken periode (b.v. 5 jaar) bewaard.

Afwegingen

Bij de keuze van SIEM producten moet overwogen worden of de inherente complexiteit, die SIEM met zich meebrengt en de eisen die SIEM systemen aan de infrastructuur stellen qua kosten en inspanning, opwegen tegen de informatiebehoefte van het management. Er kan ook besloten worden om in plaats van SIEM gebruik te maken van individuele rapportagetools van de verschillende hardware platforms.

Implicaties

Randvoorwaarde van het gebruik van SIEM is dat de te monitoren IT in staat is om logfiles te exporteren naar Security Management services (zoals SIEM). Dit geldt zowel voor infrastructuur als voor applicaties. Ook aan de SIEM-beheerders en security-officers moeten eisen worden gesteld.
Aan zelfbouwapplicaties worden afhankelijk van het type applicatie en de omgeving waarin de applicatie functioneert specifieke eisen gesteld voor het aanleveren van logregels aan de Logging en SIEM apparatuur.

Gerelateerde patronen

- Logging
- Koppelvlakken Beheer

29. Themapatroon Bedrijfscontinuïteit (BCM)

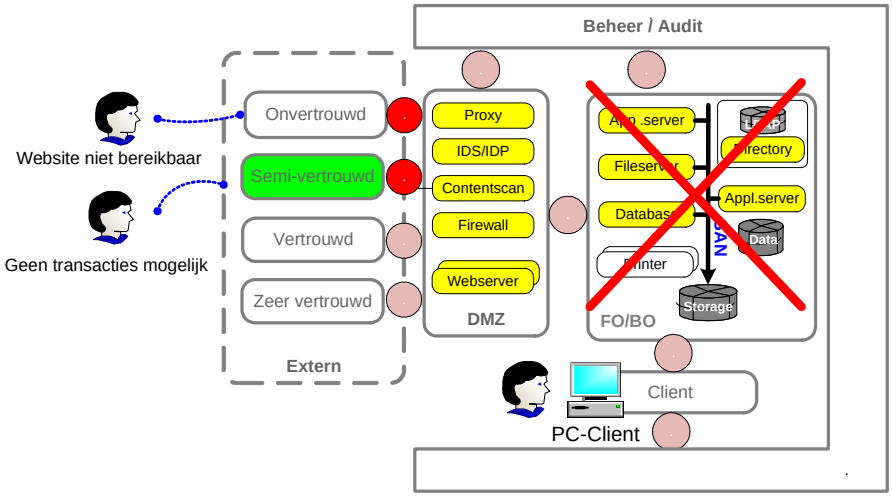
Leeswijzer
Dit patroon beschrijft een oplossing voor de algemene probleemstelling van bedrijfscontinuïteit; ook wel genoemd: Business Continuïty Management (BCM). Het patroon legt de focus op IT voorzieningen.

Criteria

Beschikbaarheid

Context

Onder druk van de markt, beïnvloed door Internet services en e-Commerce voor just-in-time processen, ervaren organisaties een toenemend belang van processen en voorzieningen voor bedrijfscontinuïteit.



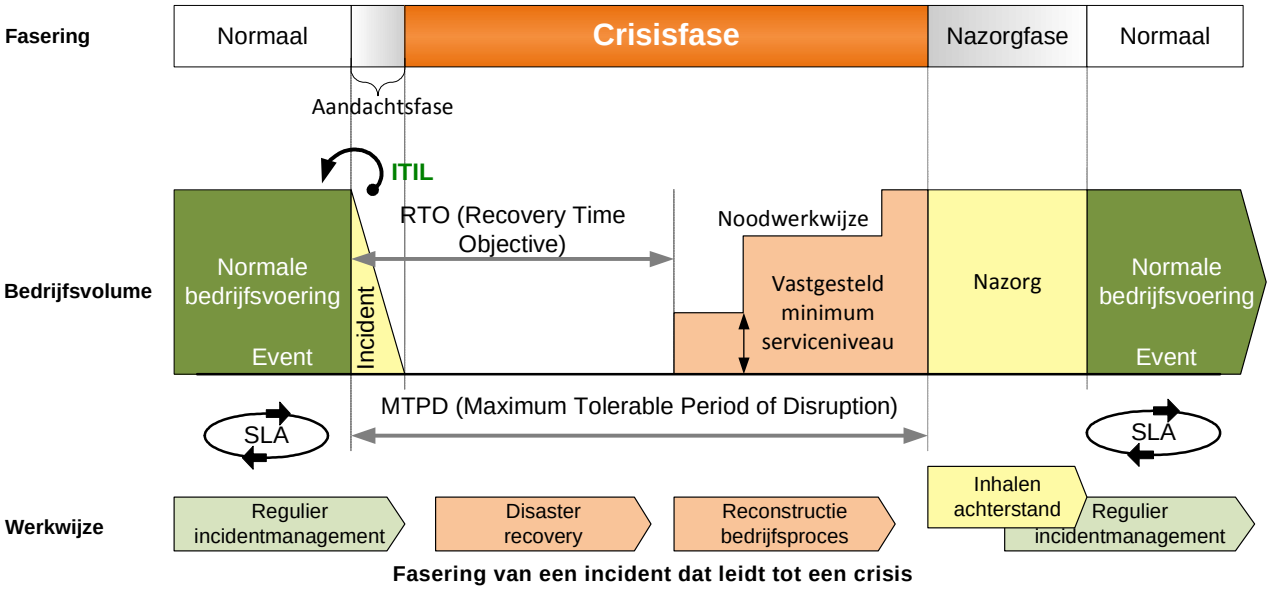
Uitval van een rekencentrum als gevolg van een crisis

De figuur schetst de gevolgen voor de klant van het uitvallen van een deel van een rekencentrum als gevolg van een *crisis*. Lang niet elk incident zal binnen de normale bedrijfsvoering kunnen leiden tot grootschalige uitval van IT-voorzieningen. Het reguliere incidentmanagementproces zorgt er in meer dan 99,9% van de gevallen voor dat de normale bedrijfsvoering binnen de SLA afgesproken tijd wordt hersteld.

De **SLA** (Service Level Agreement) definieert de *beschikbaarheid* binnen regulier incidentmanagement.

De **RTO** (Recovery Time Objective) is de door de business vastgestelde *maximale* tijd waarbinnen het voor de bedrijfsvoering cruciale*, minimum serviceniveau* moet zijn hersteld.

De **MTPD** (Maximum Tolerable Period of Disruption) is de door business vastgestelde *maximale* tijd dat een crisis mag duren inclusief de incident (aandachts-)fase.



Fasering van een incident dat leidt tot een crisis

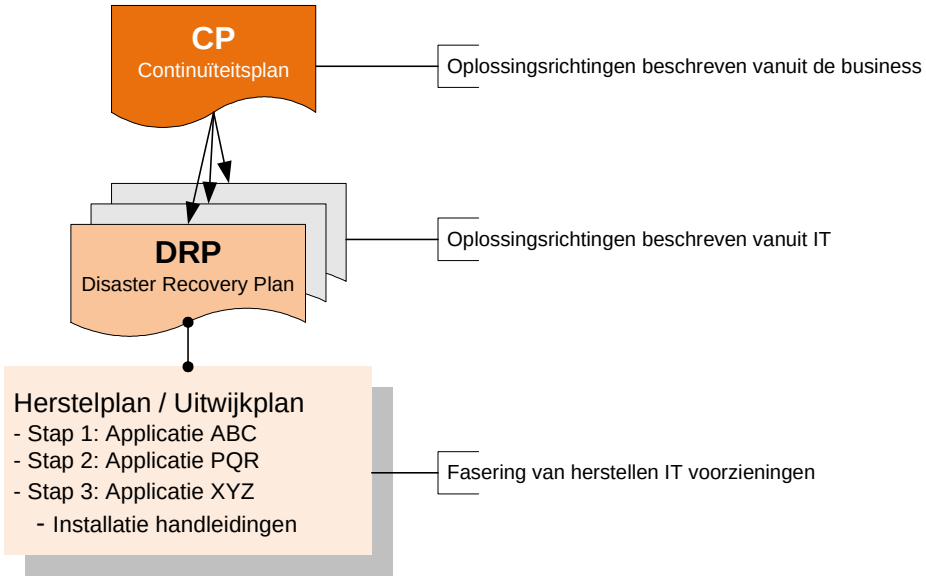
Definitie:
Een crisis is een toestand na een onverwachte gebeurtenis, met dermate negatieve gevolgen, dat de reguliere probleemoplossende activiteiten onvoldoende zijn voor het herstel van de normale situatie, waarbij de continuïteit van de bedrijfsvoering in gevaar is.

Probleem

Wanneer incidenten leiden tot grootschalige verstoringen van de bedrijfsprocessen, of zelfs tot een totale vernietiging van bedrijfsmiddelen (waaronder IT-voorzieningen), dan ontbreken op het moment van voorval de mogelijkheden om adequate maatregelen te treffen, wanneer deze niet vooraf zijn bedacht en voorbereid.

Oplossing

1. Een crisisteam neemt in geval van een crisis (wanneer de SNO/SLA garanties niet meer gelden) de centrale besturing van de organisatie (of bedrijfsonderdeel) over en beperkt zich tot crisismanagement processen. Crisismanagement begint in de figuur bij een vooraf gedefinieerde ‘drempel’ die bepaald wordt door de ernst of de duur van een incident. In de nazorgfase zorgt het crisisteam voor de terugkeer tot de normale bedrijfsvoering.
2. Het lijnmanagement geeft opdracht tot het *opstellen en het regelmatig testen* van een *Continuïteitsplan* (CP), dat beschrijft welke IT-systemen cruciaal zijn voor het voortbestaan van de organisatie (-onderdeel). Het management geeft tevens opdracht tot het *ontwikkelen van een visie* en uitwerking daarvan op *redundantie van IT-voorzieningen*, resp. van *Hot* of *Cold* standby. Behalve voor IT-voorzieningen beschrijft het CP de fasering, de noodwerkwijze en alle benodigde maatregelen voor personeel, organisatie, huisvesting en logistiek om de organisatie tijdens een crisis te kunnen laten ‘overleven’. De noodwerkwijze is een alternatieve werkwijze, die de bedrijfsvoering op een *minimaal* acceptabel (service)niveau gaande houdt. Reconstructie is het herstel van data (ook niet digitale), huisvesting etc. Een CP omvat samengevat de *aanvalsstrategie* voor een crisis.
3. Vanuit het CP worden Disaster Recovery Plannen (DRP) opgesteld, die van de cruciale IT-systemen in volgorde aangeven welke applicaties het eerst moeten worden hersteld op basis van welke infrastructuur, al dan niet gelegen op een uitwijklocatie. De CP en de DRP’s worden periodiek getest op de beoogde werking.



DRP als IT-onderdeel van een continuïteitsplan.

Gerelateerde patronen

- **Backup en Restore strategie.** Dit patroon geeft aanwijzingen voor het organisatiebreed overwegen en plannen van de noodzaak voor het veiligstellen en terugzetten van bedrijfsgegevens.
- **Disaster Recovery (DR).** Dit patroon geeft een voorbeeld invulling aan een DR aanpak voor uitwijk van een rekencentrum.

Meer kaders voor BCM zijn te vinden in de BS 25999 part 1 en 2: [13] en de ISO 27002 hoofdstuk 14.

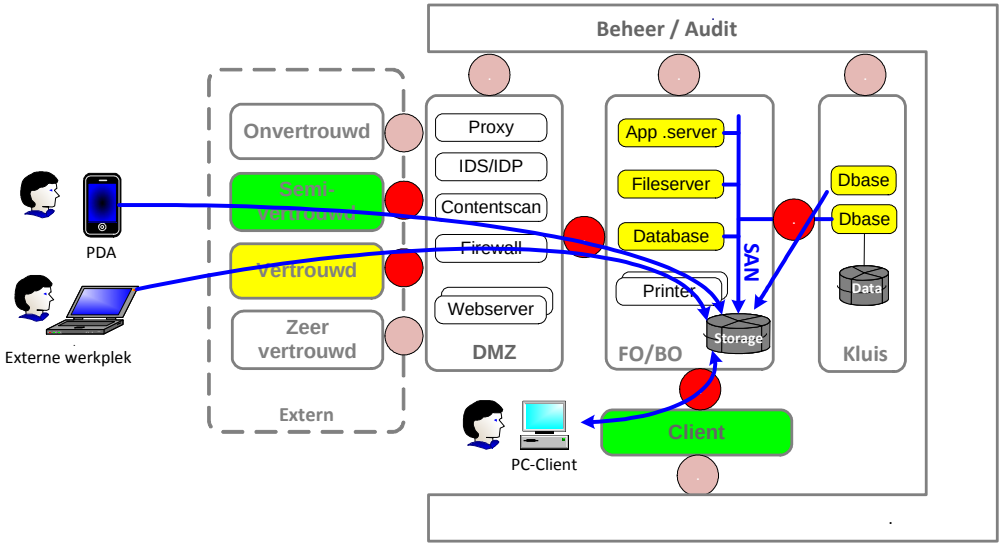
30. Back-up & Restore strategie

Criteria

Beschikbaarheid,

Context

Afgewogen Back-up en Restore (B&R) keuzes, vastgelegd in een B&R-*strategie* is bijna net zo belangrijk als het technische ontwerp voor het veiligstellen van de data zelf. Deze strategie is essentieel voor de keuze en verantwoording over investeringen in relevante opslag technologie en de begeleiding van de uitvoering. Er bestaat geen 'one-size-fits-all' oplossing voor B&R. In dit patroon worden vijf verschillende object typen beschouwd waarvoor B&R geregeld wordt en biedt overzicht bij het maken van keuzes voor B&R van: *Mobiele apparaten, Clients, Servers, Files, Databases en Transacties.*



Omgeving van objecten voor B&R

Probleem

1. Afstemming met bedrijfsvoering en gegevenseigenaren van een toereikende B&R strategie én over de aantoonbaarheid van de goede werking van de restore.
2. Niet alle objecttypen hebben dezelfde prioriteit / periodiciteit voor het veiligstellen, terwijl ze in dezelfde (te grote) dataset kunnen bestaan.
3. B&R kunnen uitvoeren binnen het z.g. *service-window*. De technische mogelijkheden voor snelle opslag zijn nauwelijks meegegroeid met de hoeveelheid gegevens in de verschillende objecten.

Oplossing

Stap 1 van de oplossing is het samen met de eigenaren van de bedrijfsprocessen en gegevens bepalen, van *welke* objecten de gegevens periodiek of online moeten worden veiliggesteld. Per object worden vervolgens keuzes gemaakt qua interval, doorlooptijd, acceptabel dataverlies en draagbare kosten.

	Betekenis	Object en resultaten
Object	Wat moet worden veiliggesteld?	PDA, Client, Server, File, Database of Transactie
Wie	Wie voert de back-up uit?	Gebruiker, Operator of Geautomatiseerd
Waar	Locatie waar de back-up wordt gemaakt	Lokaal, of op afstand
Media	Welke back-upmedia wordt toegepast?	Tape, Disk, Backup Server (BS), Fileserver (FS), Fault Tolerant Server (FTS)
Interval	Max tijd tussen back-upprocedures	Dagen, Uren, Minuten,Seconden of op het zelfde moment
Hersteltijd	Doorlooptijd van herstelprocedure	Globaal de minimale lengte van het servicewindow
Periodiciteit	Hoe vaak moet goede werking van de restore worden aangetoond?	Maanden, Weken, Dagen
Verlies	Is dataverlies voor de business draagbaar?	Wordt door de gegevenseigenaar beantwoord
Kosten	Totale kosten van bedrijfsbrede toepassing	Inschatting: Laag, Midden, Hoog

Stap 2: Vervolgens worden vanuit kosten/baten- of impactanalyse de B&R processen ontworpen op de technische herstelmogelijkheden tot een veiliggestelde situatie, inclusief periodieke restore-testen. Onderstaand overzicht geeft een *voorbeeld* van practische waarden per type object en helpt bij de overweging en uitvoering van Stap 1 en Stap 2 voor het maken van keuzes van oplossingsrichtingen.

Object	Wie	Waar	Media	Interval	Hersteltijd	Verlies	Kosten
Mobiel	Gebruiker	Lokaal	Laptop	Dagen	Minuten	ja	Laag
	Geautomatiseerd	Lokaal	Laptop	Dagen	Minuten	ja	Laag
	Gebruiker	Afstand	BS	Uren	Minuten	ja	Midden
	Geautomatiseerd	Afstand	BS	Uren	Minuten	ja	Midden
Client	Gebruiker	Lokaal	Tape	Uren	Uren	ja	Hoog
	Gebruiker	Lokaal	Disk	Uren	Uren	ja	Midden
	Gebruiker	Lokaal	FS	Uren	Uren	ja	Laag
	Gebruiker	Afstand	FS	Uren	Uren	ja	Midden
	Geautomatiseerd	Afstand	FS	Uren	Uren	ja	Midden
Server	Operator	Lokaal	Tape	Uren	Uren	ja	Midden
	Operator	Lokaal	FS	Uren	Uren	ja	Midden
	Operator	Afstand	BS	Uren	Uren	ja	Hoog
	Geautomatiseerd	Lokaal	FS	Uren	Uren	ja	Midden
	Geautomatiseerd	Afstand	BS	Uren	Uren	ja	Hoog
Files	Gebruiker	Lokaal	FS	Seconden	Seconden	ja	Laag
	Gebruiker	Lokaal	Tape	Minuten	Uren	ja	Midden
	Gebruiker	Lokaal	Disk	Minuten	Minuten	ja	Laag
	Gebruiker	Afstand	FS	Seconden	Seconden	ja	Midden
	Geautomatiseerd	Lokaal	FS	Seconden	Minuten	nee	Midden
	Geautomatiseerd	Afstand	BS	Seconden	Minuten	nee	Hoog
Database	Operator	Lokaal	Tape	Uren	Uren	ja	Laag
	Operator	Lokaal	Disk	Uren	Minuten	ja	Midden
	Operator	Lokaal	FS	Uren	Minuten	ja	Midden
	Geautomatiseerd	Afstand	Tape	Uren	Uren	ja	Laag
	Geautomatiseerd	Afstand	Disk	Uren	Uren	ja	Midden
	Geautomatiseerd	Afstand	BS	Uren	Minuten	ja	Midden
	Geautomatiseerd	Lokaal	FTS	Online	Online	nee	Hoog
Transactie	Geautomatiseerd	Lokaal	FTS	Online	Online	nee	Hoog
	Operator	Lokaal	Tape	Seconden	Dag	nee	Midden
	Geautomatiseerd	Lokaal	BS	Seconden	Uren	nee	Midden
	Geautomatiseerd	Afstand	FTS	Online	Online	nee	Hoog
	Operator	Afstand	Tape	Minuten	Dag	ja	Midden
	Geautomatiseerd	Afstand	BS	Seconden	Uren	nee	Midden

Betekenis: **FS**: File Server, **FTS**: Fault Tolerant real-time redundant Server, **BS**: Backup Server.

De gewenste periodiciteit voor het aantonen van de goede werking van een restore hangt in sterke mate af van de eisen die de bedrijfsvoering stelt aan het object.

Afwegingen

- Bepalen van de juiste B&R strategie is geen zaak voor IT alleen, maar moet in overleg met de proces- en gegevenseigenaren van de organisatie worden bepaald.
- Aandacht voor B&R is niet zo triviaal als het lijkt. Het moet bovendien meegroeien met de snelle verandering van gegevensomvang, organisatorische aanpassingen, regelgeving, kosten en technische mogelijkheden. Vanuit de B&R strategie kan een servicewindow worden bepaald.
- Storage hardware: Gebruik disk arrays als *default* target voor B&R. Dit is eenvoudiger dan tape.
- Serveromgeving: Rekening houden met complexe oplossingen voor individuele fysieke servers en Storage Area Network (SAN). Minimaliseer server complexiteit, waarmee tevens de B&R-implementatie eenvoudiger wordt.

31. Disaster Recovery / Uitwijk

Criteria

Beschikbaarheid, Integriteit

Context

Een *disaster* (of crisis) is een gebeurtenis met een impact en schaalgrootte, waardoor er geen sprake meer kan zijn van een normale bedrijfsvoering. Een crisis zoals hier bedoeld leidt meestal tot grote materiële en immateriële verliezen.

Probleem

1. Een crisis zal afhankelijk van hun aard en schaalgrootte impact hebben op veel, zo niet alle aspecten en hulpbronnen van een organisatie.
2. Niet alle bedrijfsfuncties en voorzieningen kunnen in geval van een crisis op korte termijn worden hersteld.

Oplossing

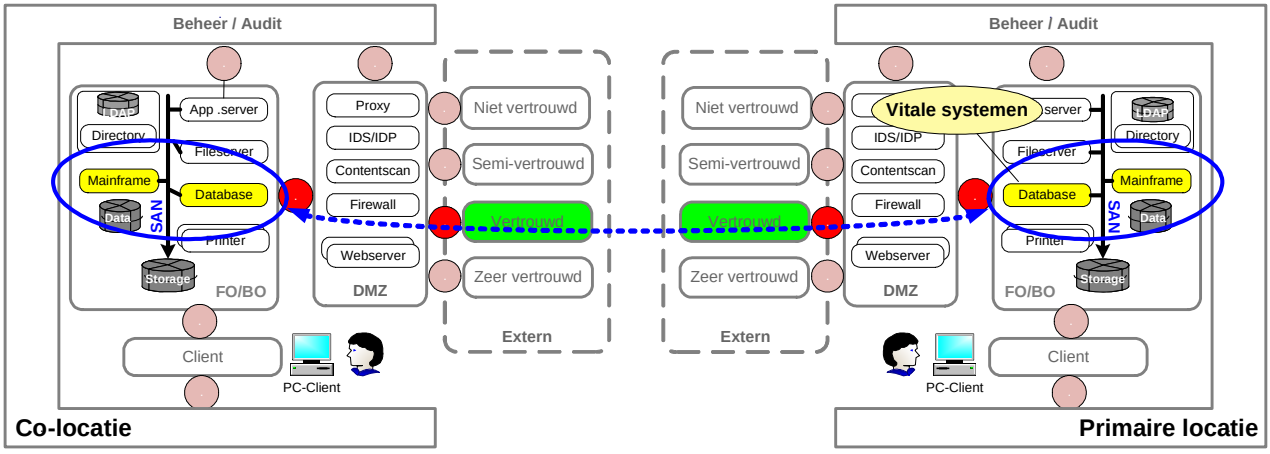
Planning. DR planning omvat alle aspecten van de 'business': een succesvol DR plan omvat:

- Human Resources die vitaal zijn voor de bedrijfsvoering.
- Fysieke faciliteiten, back-up van stroomvoorziening en koeling en Internet Service Providers (ISP)
- Alternatieven voor toeleveranciers en distributiekanalen.
- Communicatiekanalen naar de klant en ondersteuning.
- Welke gegevens, applicaties, servers, clients, netwerken, communicatiekanalen van cruciale betekenis zijn voor het voortbestaan van de organisatie (en de bedrijfsprocessen).
- Welke applicaties achtereenvolgens moeten worden hersteld op basis van welke infrastructuur.

Uitwerking. Dit patroon richt zich op DR van rekencentra en de IT-aspecten.
De keuze van DR oplossingen zijn minimaal afhankelijk van bedrijfskundige factoren waarbij steeds het criterium geldt: *voorkomen van een niet te dragen schade voor de bedrijfsvoering.* Die factoren zijn:

1. De maximale tijd van uitval voor een informatiesysteem (MTU). Internationaal wordt dit begrip *Recovery Time Objective* (RTO) genoemd.
2. Hoeveel data – of transacties mogen er maximaal verloren gaan? (MDV = Maximaal Data Verlies, internationaal heet dit RPO, Recovery Point Objective)
3. Hoe hoog mogen de directe en indirecte financiële verliezen maximaal bedragen?

Geografisch gescheiden sites
Systemen met een lage RTO van nul tot maximaal enkele dagen, vereisen een z.g. **Warm Site** oplossing, waarbij het rekencentrum voor wat betreft de *vitale systemen* is gespiegeld over twee of meer sites, ook wel *co-locatie* of *uitwijklocatie* genoemd. Afhankelijk van de hoeveelheid data of transacties die verloren mogen gaan, hoe groot de geografische afstand is en de beschikbare bandbreedte wordt er gekozen voor een synchrone- of asynchrone vorm van replicatie.



Koppeling van geografisch gescheiden sites voor vitale systemen

Synchrone of asynchrone replicatie
Synchroon: Dataverlies moet nul zijn, afstand tussen de sites kleiner dan 60 km[8], grote bandbreedte.
Asynchroon: Dataverlies geoorloofd, onbeperkte afstand tussen de sites en beperkte bandbreedte.

Voor beide synchronisatiemethoden geldt, dat de bandbreedte tussen de sites groter moet zijn dan de *gemiddelde* transactionele bitrate van de vitale systemen. Is dit niet het geval, dan leidt dit alsnog tot dataverlies.

Systemen waarvoor een RTO geldt van meer dan enkele dagen, kunnen voor bedrijfscontinuïteit volstaan met z.g. **Cold Site** oplossingen. Een cold site is een gereserveerde, niet-actieve systeemomgeving, die in de organisatie gebruikt kan worden zodra de crisis dit vereist.
Alle bedrijfsmiddelen zijn op de uitwijklocatie aanwezig om vitale systemen op te kunnen bouwen tot een werkende configuratie, inclusief back-ups van programmatuur en data.

Afwegingen

- De meest kosteneffectieve oplossing voor bedrijfscontinuïteit is die van *snapshot-herstelpunten*, gekoppeld aan asynchrone replicatie. Deze combinatie beperkt de opslag-overhead en biedt vanuit de 'snapshot-ankers' voor het opnieuw opbouwen van transacties.
- De meest kostbare, maar ook meest betrouwbare oplossing voor transactionele recovery is de synchrone replicatie.
- Organisaties moeten co-locaties overwegen als ze nog niet in gebruik zijn. Kritische web- en internet gebaseerde services zijn de eerste kandidaten voor co-locaties. Niet internet gebaseerde services, zoals Office file- en print profiteren nauwelijks van co-locaties en kunnen beter geborgd worden door gebruik te maken van alternatieve DR voorzieningen.

Voorbeelden

Warm Site oplossing: Twin-datacentre van grote organisaties, voorzien van synchrone koppeling op basis van applicatieserver- ‘mirroring’.
Cold Site oplossing: Uitwijklocatie van een partnerorganisatie.

Implicaties

- Effectiviteit van DR wordt bepaald door een stelsel van personele, organisatorische en technische maatregelen. Wanneer deze beperkt worden tot IT, wordt de scope ‘disaster’ beperkt tot ‘incident’.
- Back-up en Recovery moeten op zowel de primaire als de uitwijklocatie op orde zijn, om lange termijn uitwijk behoeften en het herstel van gegevensverzamelingen te kunnen garanderen.
- Virtualisatie is aan te bevelen om DR relatief eenvoudig te kunnen realiseren. De mogelijkheden voor virtualisatie zijn echter beperkt voor systemen met een zeer hoge I/O verwerkingssnelheden zoals grote transactionele databases. Deze systemen vereisen een fysieke tegenpool op de uitwijklocatie, of platformspecifieke oplossingen zoals beschikbaar zijn voor mainframes.

Gerelateerde patronen

- Themapatroon BCM
- Koppelvlak vertrouwde derden
- Server Virtualisatie
- Uitbesteding

[8] De maximale afstand wordt bepaald door de latency (vertragingstijd) die nog toelaatbaar is voor het functioneren van de betreffende applicaties en infrastructur. Afstanden van 30-60 km zijn daarbij realistische waarden.

32. Uitbesteding IT diensten

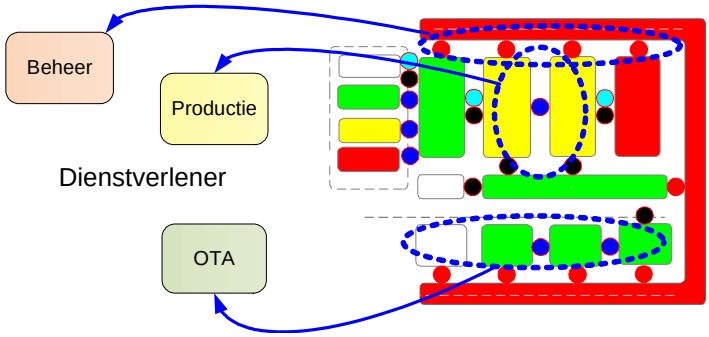
Leeswijzer
Dit patroon beschrijft de algemene probleemstelling en randvoorwaarden van IT-uitbesteding. De focus van de oplossingen is gericht op de voor de dienstverlener op te stellen koppelvakken.

Criteria

Beschikbaarheid, Vertrouwelijkheid, Integriteit, Controleerbaarheid

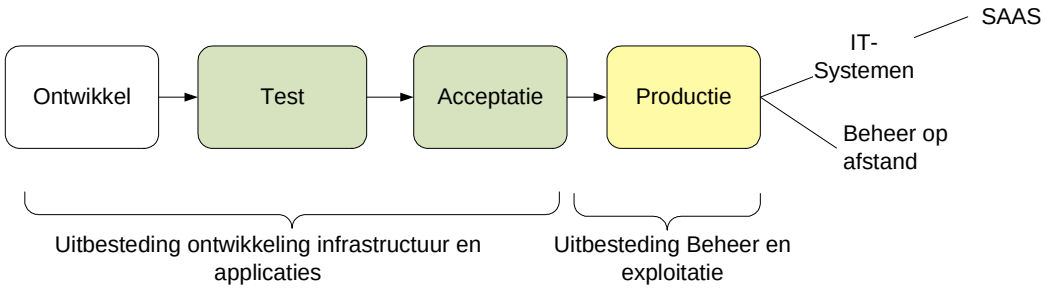
Context

Uitbesteding van IT-diensten omvat een breed aandachtsgebied, dat voor wat betreft IB-maatregelen lastig in enkele patronen is samen te vatten. De ambitie van het hier uitgewerkte patroon is daarom beperkt tot het bieden van *handvatten* voor opstellen van RFI's t.a.v. uitbesteding van IT en om overzicht en inzicht te krijgen in welke consequenties uitbesteding heeft voor informatiebeveiliging.



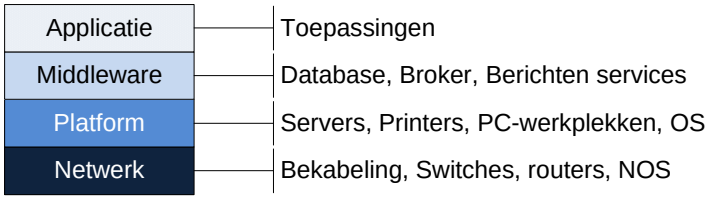
Omgeving Uitbesteding IT-diensten

In het voorbeeld van bovenstaande figuur is zowel de ontwikkel- als productieomgeving van IT-systemen geheel uitbesteed. Alleen cruciale data in de datazone, de DMZ en de clientomgeving staan nog onder beheer van de eigen organisatie. De rest is ondergebracht bij een dienstverlener.
In onderstaande figuren is de fasering van de IT-omgeving verder uitgewerkt en is aangegeven in welke onderdelen deze uitbesteed kan worden. Een stap verder is het afnemen van software services: SAAS (Software As A Service).



OTAP omgeving

Uitbesteding kan plaats vinden op verschillende 'lagen' van de IT-voorziening, waarbij elke laag in de stack zijn specifieke beveiligingseisen stelt.



IT-Stack van uitbesteding

Probleem

De uitwerking van dit patroon beperkt zich tot oplossingen voor *zonering* en *koppelvlakken*: Hoe regel je de logische verbindingen voor de onderstaande sourcingsvarianten?

Oplossing

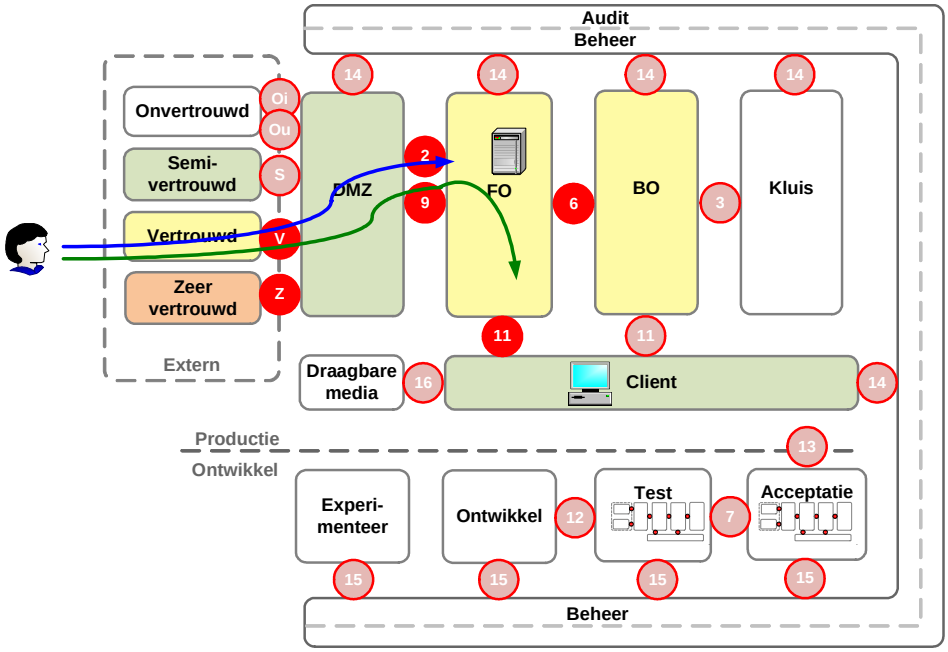
De reikwijdte van sourcing is de omvang van het IT landschap wat voor uitbesteding in aanmerking komt. Deze reikwijdte bepaalt de soort van maatregelen die voor beveiliging met leveranciers moet worden afgesproken. Voor de volgende sourcingsvarianten geldt:

I. **Applicatieontwerp en bouw (OT) is uitbesteed**. De focus van beveiliging ligt hierbij op geheimhouding en het toetsen van beveiligingsfuncties en de afwezigheid van ongewenste eigenschappen. Voor deze vorm van uitbesteding is het patroon “Kanaal (s) naar Semi-Vertrouwd” van toepassing.

II. **Applicaties en delen van infrastructuur (OTAP)** zoals werkstations en netwerk. Hiervoor geldt bovenstaande (I) plus een uitgebreide set van beveiligingseisen, die specifiek voor sourcing vastgesteld wordt. Voor deze vorm van uitbesteding is het patroon “Kanaal (v) naar Vertrouwd” van toepassing.

Idem II + technisch beheer en exploitatie (OTAP) . Waar in dit geval de focus gelegd moet worden, hangt af van wie de eigenaar is van de infrastructuur. Bij uitbesteding van beheer en exploitatie is steeds de meest uitgebreide set van beveiligingseisen van toepassing. Feitelijk is hier het gehele spectrum van informatiebeveiliging, zoals vastgelegd in het te hanteren IB-normenkader van de eigen organisatie van toepassing. Voor deze variant, inclusief technisch beheer is voor de koppeling met de service provider het patroon “Kanaal (z) naar Zeer vertrouwd” van toepassing.

III. De uitbestedingsvarianten voor exploitatie, waarbij de leverancier IT-diensten biedt aan de klant zijn:
   a. Met behulp van de infrastructuur & applicaties van de klant (beheerservices)
   b. Met behulp van eigen infrastructuur & applicaties op de locatie van de klant. (Mg. Service)
   c. Vanuit voor de klant afgezonderde infrastructuur op locatie van de leverancier (fysiek buiten).
   d. Vanuit eigen infrastructuur & applicaties inclusief opslag van bedrijfsgegevens (Cloud computing)



Leverancier biedt IT beheerservices op de infrastructuur van de klant

De tabel geeft aan welke koppelvlakken per uitbestedingsvariant voor de serviceprovider moeten worden opengesteld en bewaakt. Zie de patronen Koppelvlakken voor meer informatie.

Stack	Zone/ object	Beheerservice	Mgt.service	Fysiek buiten	Cloud /SAAS
Gegevens		n.v.t.	n.v.t.	V,2,9,11	V,2,9,11
Applicaties	FO	V,2	V,2	V,2,9,11	V,2,9,11
	BO	V,2,6	V,2	6	n.v.t.
Middleware		V,2,6	V,2	n.v.t.	n.v.t.
Platforms	OS	V,2,6	V,2	n.v.t.	n.v.t.
Client	Interne client	V,2,6,11	n.v.t.	n.v.t.	n.v.t.
Netwerken	LAN	V,2,6	n.v.t.	n.v.t.	n.v.t.
	WAN	n.v.t.	n.v.t.	n.v.t.	n.v.t.

Voor serviceproviders van WAN diensten worden geen koppelvlakken opengesteld.

Afwegingen

Met de toenemende globalisering van dienstverleners, worden beveiligingsrisico's steeds moeilijker te kwantificeren en te doorzien. Alvorens uit te besteden moet onderzocht en overwogen worden:

- Waar worden de eigen gegevens en back-ups opgeslagen? In virtuele, internationale omgevingen? Denk aan eisen voor privacybescherming!
- Wie voert in welk land de automatisering van de organisatie uit m.b.t. ontwikkeling, onderhoud en beheer?
- Hoe krijgen we grip op wie zich met automatisering bezig houdt bij onderuitbesteding?
- In hoeverre kun je vertrouwen op audits betreffende naleving van beveiligingsnormen in landen binnen of buiten de EU?
- Welke exit strategie wordt gevolgd? Wat moet er afgesproken en ingeregeld worden om uitbestedingen ongedaan te kunnen maken.

Voorbeelden

- Internet koppelvlakken (managed service).
- Uitbesteding van software ontwikkeling naar lage lonen landen (Oost Europa of Azië).
- Clientbeheer door externe partij (legio voorbeelden).
- Cloud services en SAAS.

Implicaties

Algemene voorwaarden om over te kunnen gaan op uitbesteding van IT-diensten zijn:

a) De vraagorganisatie moet *volwassen* genoeg zijn om tegenspel te kunnen bieden aan de externe IT-dienstverleners.
b) De vraagorganisatie moet bereid- en in staat zijn tot *samenwerking* met partners.
c) Vanuit eigen of ingehuurde expertise moet beoordeeld kunnen worden of de IT-dienstverlener kan voldoen aan de gestelde beveiligingsnormen.
d) De vraagorganisatie moet het *eigen huis moet op orde* hebben qua beheer en eigenaarschap van bedrijfsmiddelen en gegevens.
e) Bestuurders en deskundigen van de vraagorganisatie *beschikken over referenties*; ze hebben ervaringen geëvalueerd met relevante partijen die soortgelijke uitbesteding toepassen.
f) De *exit strategie* is vastgesteld.

Specifieke voorwaarden t.a.v. informatiebeveiliging voor uitbesteding zijn:

I. Het beoogde *vertrouwensniveau* is afgestemd tussen vraagorganisatie en dienstverlener.
II. Toereikende *beveiligingseisen* zijn opgesteld voor de specifieke uitbestedingssituatie (sourcing).
III. *Proactief beheer* van eigen beveiligingsnormatiek en contractontwikkeling is ingeregeld.
IV. De vraagorganisatie ontvangt periodiek bevindingen over *beveiligingsaudits* bij de dienstverlener.
V. De dienstverlener *realiseert* de *aanbevelingen* vanuit de beveiligingsaudits.
VI. De dienstverlener geeft *garanties* over de vertrouwelijkheid van de bedrijfsinformatie van de uitbestedende organisatie en het handhaven van de privacy regels van Nederland. Dit geldt vooral voor uitbestede systemen die gehost worden in lage-lonen landen en landen buiten Europa. In de VS is de overheid bij wet (Patriot Law) gerechtigd om in geval van terrorismedreiging *alle data* in te zien van systemen die op Amerikaanse bodem staan, of die daar rechtstreeks mee verbonden zijn.

Gerelateerde patronen

Koppelvlakken

Bijlage 1: Relatie met Normen informatiebeveiliging

Patronen zijn niet bedoeld als volledige implementaties van normen voor informatiebeveiliging, voor zover de normen betrekking hebben op de technische infrastructuur van IT. Patronen bieden door architectuurviews inzicht en overzicht in *oplossingsrichtingen*. Patronen gaan per definitie niet in op functionele details, waar normen vaak wel op ingaan. De abstractieniveaus en doelstellingen van normen en patronen dekken elkaar maar voor een beperkt deel, hoewel zowel patronen als Nora-normen en ISO 27002 Code voor informatiebeveiliging als tactische documenten (kunnen) worden ervaren. In onderstaande tabellen worden de relaties van patronen met Nora en ISO norm in beeld gebracht.

Relatie patronen met ISO 27002

ISO 27002 : 2005	Patronen
6.2.1 Identificatie van risico's die betrekking hebben op externe partijen d) beheersmaatregelen om informatie te beschermen voor toegang door externe partijen	21. Thema Encryptie 22. Symmetrische Encryptie 23. Public Key Infrastructure 24. Elektronische Handtekening 26. Secure E-Mail
10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie b) Ontwikkelings- en operationele programmatuur uitvoeren in verschillende domeinen. c) Compilers, tekstverwerkingsprogramma's en andere systeemhulpmiddelen niet toegankelijk vanuit productiesystemen.	8. Thema Koppelvlakken + onderliggende KV-patronen 11. Interne KV voor ontwikkelomgeving 20. Vertrouwd ToegangsPad
10.4.1 Maatregelen tegen virussen d.1) controleren van bestanden die via netwerken zijn ontvangen; d.2) controleren van e-mailbijlagen en gedownloade bestanden (op e-mailservers, desktopcomputers en bij de toegang tot het netwerk); d.3) controleren van webpagina's.	8. Thema Koppelvlakken + onderliggende KV-patronen 2. Client 3. Server
10.4.2 Maatregelen tegen 'mobile code' a) uitvoeren van 'mobile code' in een logisch geïsoleerde omgeving	8. Thema Koppelvlakken + onderliggende KV-patronen
10.4.2 Maatregelen tegen 'mobile code' f) cryptografische beveiligingsmaatregelen om 'mobile code' uniek te authenticeren.	21. Thema Encryptie 22. Symmetrische encryptie 24. Elektronische handtekening
10.5 Back-up	30. Back-up & Restore strategie
10.5 Back-up h) in gevallen waar vertrouwelijkheid van belang is, behoren back-ups te worden beschermd door middel van encryptie	21. Thema Encryptie + onderliggende Encryptie-patronen
10.6.1 Maatregelen voor netwerken c) vertrouwelijkheid en integriteit waarborgen van gegevens die via openbare netwerken en over draadloze netwerken worden verzonden en om de aangesloten systemen en toepassingen te beschermen; d) waarborgen dat de uitvoer van toepassingssystemen waarmee gevoelige informatie wordt verwerkt alleen wordt verzonden naar computerterminals en locaties met een autorisatie **10.6.2 Beveiliging van netwerkdiensten** **10.7.3 Procedures voor de behandeling van informatie** b) toegangsbeperkingen **10.8.1. Beleid en procedures voor informatie-uitwisseling** b) bescherming tegen virussen via elektronische communicatie g) cryptografische technieken om informatie te beschermen	8. Thema Koppelvlakken + onderliggende KV-patronen 21. Thema Encryptie 22. Symmetrische Encryptie 23. Public Key Infrastructure 24. Elektronische Handtekening 26. Secure E-mail 5. Netwerk 6. Draadloze netwerken

ISO 27002 : 2005	Patronen
10.8.4 Elektronisch berichtenuitwisseling m.u.v. e) voorafgaande toestemming voor gebruik externe openbare diensten **10.9.1 E-commerce** a) betrouwbaarheideisen van elkaars beweerde identiteit; d) voldoen aan eisen voor bewijs van verzending en ontvangst **10.9.2 Online transacties** a) het gebruik van elektronische handtekeningen; b) waarborgen dat: 1) geldige gebruikersgegevens; 2) vertrouwelijkheid transactie 3) de privacy betrokken partijen; c) communicatieroute versleuteld; f. beveiliging geïntegreerd in de gehele keten van certificaat/handtekeningbeheerproces	21. Thema Encryptie 22. Symmetrische Encryptie 23. Public Key Infrastructure 24. Elektronische Handtekening 26. Secure E-mail
10.9.3 Openbaar beschikbare informatie d) geen onbedoelde toegang tot publicatiesysteem	8. Thema Koppelvlakken + onderliggende KV-patronen
10.10.2 Controle van systeemgebruik	28. SIEM
10.10.3 Bescherming van informatie in logbestanden	27. Logging
11.2.1 Registratie van gebruikers a) gebruik van unieke gebruikersidentificaties (ID) g) een formele registratie bijhouden	15. Identity Management (IdM)
11.4.2 Authenticatie van gebruikers bij externe verbindingen	21. Thema Encryptie 22. Symmetrische Encryptie 23. Public Key Infrastructure 24. Elektronische Handtekening 26. Secure E-mail
11.4.5 Scheiding van netwerken **11.4.6 Beheersmaatregelen voor netwerkverbindingen** **11.4.7 Beheersmaatregelen voor netwerkrouting**	8. Thema Koppelvlakken + onderliggende KV-patronen
11.5.2 Gebruikersindentificatie en –authenticatie	15. Identity Management (IdM) 17. Federated Identity & Access Management 18. Single Sign-On / Single Sign-Off
11.5.3 Systemen voor wachtwoordbeheer i) wachtwoorden in beschermde vorm (bijvoorbeeld versleuteld) op te slaan en te verzenden	21. Thema Encryptie + onderliggende Encryptie-patronen
11.6.1 Beperken van toegang tot informatie a) menu's om toegang tot functies te beheersen	19. Portaal – toegangsserver
11.6.2 Isoleren van gevoelige systemen	8. Thema Koppelvlakken + onderliggende KV-patronen
11.7.1 Draagbare computers en communicatievoorzieningen **11.7.2 Telewerken** c) communicatiebeveiliging: toegang tot de interne systemen	9. Externe koppelvlakken 21. Thema Encryptie
12.2.3 Integriteit van berichten	21. Thema Encryptie 22. Symmetrische Encryptie 23. Public Key Infrastructure 24. Elektronische Handtekening 26. Secure E-mail
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen c) encryptie voor gevoelige informatie op draagbare of verwijderbare media, apparatuur of verzonden over communicatielijnen; g) de gevolgen van inspectie van de inhoud van versleutelde informatie (bijvoorbeeld virusdetectie).	8. Thema Koppelvlakken 21. Thema Encryptie
12.3.2 Sleutelbeheer	23. Public Key Infrastructure 25. Sleutelhuis
14 Bedrijfscontinuïteitsbeheer	29. Thema Bedrijfscontinuïteit 31. Disaster Recovery

Relatie met NORA Normen IT-voorzieningen

Overzicht Nora-normen waaraan patronen een (globale) uitwerking geven. De Nora-normen zijn in overeenstemming met het IB-Functiemodel voor IT-voorzieningen ingedeeld.

Normen (beheerdoelstelling/-maatregel)	Patronen (evt. implementatierichtlijnen)
3. Continuïteitsvoorzieningen	29 Themapatroon Bedrijfscontinuïteit
3.1 Dubbele uitvoering van II-Voorzieningen	31 Disaster Recovery / Uitwijk
3.2 Herstelbaarheid van verwerking	30 Backup & Restore Strategie, 31. Disaster Recovery
5 Zonering	
5.1 Zonering Technische Infrastructuur	8 Thema KV + onderliggende KV-patronen, VTP (7,8)
5.2 Eisen te stellen aan zones	8 Thema KV + onderliggende KV-patronen
5.3 Encryptie ten behoeve van zonering	21 Thema Encryptie, 22. Symm. Encryptie, 23.PKI, 24. Elektr.Handtek.
5.4 Sterkte van de encryptie	21 Thema Encryptie, 22. Symm. Encryptie, 23.PKI, 24. Elektr.Handtek.
5.5 Vertrouwelijkheid en integriteit sleutels	21 Thema Encryptie, 22. Symm. Encryptie, 23.PKI, 24. Elektr.Handtek., 26. Secure E-Mail
6. Filtering	
6.1 Controle op communicatiegedrag	8 Thema KV + onderliggende KV-patronen
6.2 Controle op gegevensuitwisseling	8 Thema KV + onderliggende KV-patronen
7 Onweerlegbaarheid berichtuitwisseling	22 Symm. Encryptie, 23.PKI, 24. Elektr.Handtek., 26. Secure E-Mail
8 Identificatie, Authenticatie en Autorisatie	
8.1 Identificatie	15 Idm, 17. Federated IdM, 18. SSO, 23.PKI, 24. Elektr.Handtek.
8.2 Authenticatie	22 Symm. Encryptie, 23.PKI, 24. Elektr.Handtek., 26. Secure E-Mail
8.4 Instellingen aanmelden op een systeem	19 Portaal – Toegangsserver
8.8 Beheersbaarheid autorisaties	16 Access Management
8.9 Volledigheid toegangsbeveiliging	16 Access Management
9 Vastleggen van gebeurtenissen	27 Logging
10 Controle, alarmering en rapportering	28 Security Information Event Management (SIEM)

Bijlage 2: Bronverwijzingen

1. Template Patronen; Open Group forum
2. Normen Informatiebeveiliging IT-voorzieningen; NORA best practices, versie1.0; 2009; Bart Bokhorst en Jaap van der Veen: http://e-overheid.nl/onderwerpen/architectuur-en-nora/982-dossier-informatiebeveiliging
3. Architectuuraanpak; versie 1.0 September 2009; Jaap van der Veen en Bart Bokhorst; http://e-overheid.nl/onderwerpen/architectuur-en-nora/982-dossier-informatiebeveiliging
4. Dynamic Software Security Testing, Web Scanning 2011, versie 2,0 Maart 2011 door Ramon Krikken Burton Group
5. SSO voor mijnOverheid.nl, stichting ICTU info@mijnoverheid.nl, www.mijnonverheid.nl , pip.overheid.nl
6. Presentatie PvIB over SIEM Special februari 2009; Ir.Ernst J.Mellink: patroon Logging
7. Data Protection: Have a Plan and Be a Hero; versie 1.0; Maart 2011; Gene Ruth; Burton Group: patroon B&R
8. Backup and Recovery; versie 1.0; Januari 2006; Fred Cohen; Burton Group: patroon B&R
9. Survival of the fittest: Disaster Recovery Design for Data Center, Richard Jones, 1.0 september 2007; Burton Group
10. ISO-27002; Code voor Informatiebeveiliging 2005
11. BS 25999 Code of practice; part 1 en part 2; British Standards (BSI), 2006
12. New Directions in Federation; versie 1.0 Oktober 2009; Gerry Gebel; In-depth Research Report Burton Group
13. Federated Identity, November 2010; Bob Blakly; Burton Group
14. Identity and Privacy Planning Guide; Maart 2011; Bob Blakly; Burton Group
15. Doelarchitectuur “Toegang”, Ministerie BZK, 2012
16. PvIB Expertbrief- “Access Management”, Oktober 2009
17. Building Scalable Syslog Management Solutions, Cisco Whitepaper, April 2011
18. Baseline Informatiebeveiliging Rijksdienst (BIR) versie 1.0, Ministerie BZK, 2012

