Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Baseline Informatiebeveiliging Rijksdienst

Operationele Handreiking

Versie 1.0

Datum 30 oktober 2013

Inhoudsopgave

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1 Inleiding

Deze versie van de Operationele baseline bouwt voort op het succes van de operationele baseline DWR en bevat alleen IT patronen. De overige onderwerpen uit de ISO-27002, waaruit procedurele patronen of operationele richtlijnen samengesteld kunnen worden, volgen in nieuwe versies van deze baseline. Het tactische deel van de BIR wordt in deze versie nog niet volledig gedekt door de operationele baseline.

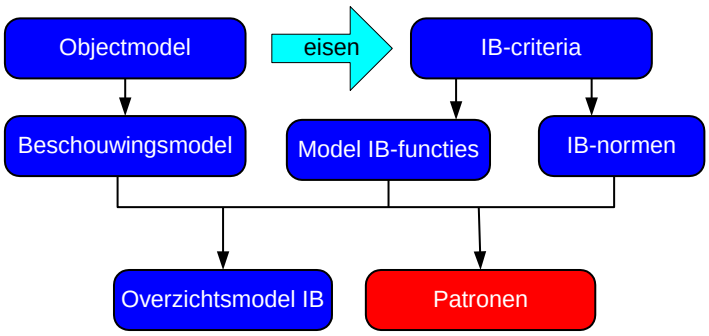
De patronen in dit document zijn goede voorbeelden voor het realiseren van beveiligingsfuncties in ICT omgevingen. Het gaat om voorbeelden, “best practices”. Het is niet verplicht om deze patronen te volegen maar ze leiden wel tot een goede manier van invullen van de BIR TNK. Daarnaast bevat de BIR TNK veel normen die niet geraakt worden door deze patronen. Het blijft dus nodig om een toets te doen op de normen uit de BIR TNK.

De patronen bevatten zo weinig mogelijk “magic numbers”. Hiervoor wordt verwezen naar bijlage 1, die minimale waarden bevat. Steeds geldt dat zo veel mogelijk aan een norm voldaan wordt, uiterlijk binnen de minimale waarde in de SLA. Voor eisen aan cryptografische producten en algoritmen wordt verwezen naar bijlage 2.

De normen en maatregelen in het BIR zijn gebaseerd op een niveau van vertrouwelijkheid, dat hoort bij de rubricering “Departementaal Vertrouwelijk*”* en het niveau WBP risicoklasse 2 verhoogd risico. Bij data met dit niveau van vertrouwelijkheid zal encryptie en sleutelmanagement zo geregeld moeten worden dat externe partijen (inclusief de leverancier van bijvoorbeeld een cloud) geen mogelijkheden hebben tot inzage van de data.

IB-Architectuur aanpak

De patronen zoals beschreven in deze operationele baseline, zijn architectuurbouwstenen als onderdeel van de NORA- architectuuraanpak Informatiebeveiliging, zoals hieronder schematisch is aangegeven.



Vanuit de bedrijfsfuncties (objectmodel) worden in de vorm van criteria Beschikbaarheid, Vertrouwelijkheid, Integriteit en Controleerbaarheid eisen gesteld aan informatiebeveiliging van IT-voorzieningen. Deze eisen zijn als IB-functies samengevat in het IB-functiemodel en verwoord in IB-normen op tactisch niveau. Zie voor meer informatie over deze modellering de e-Overheidssite:

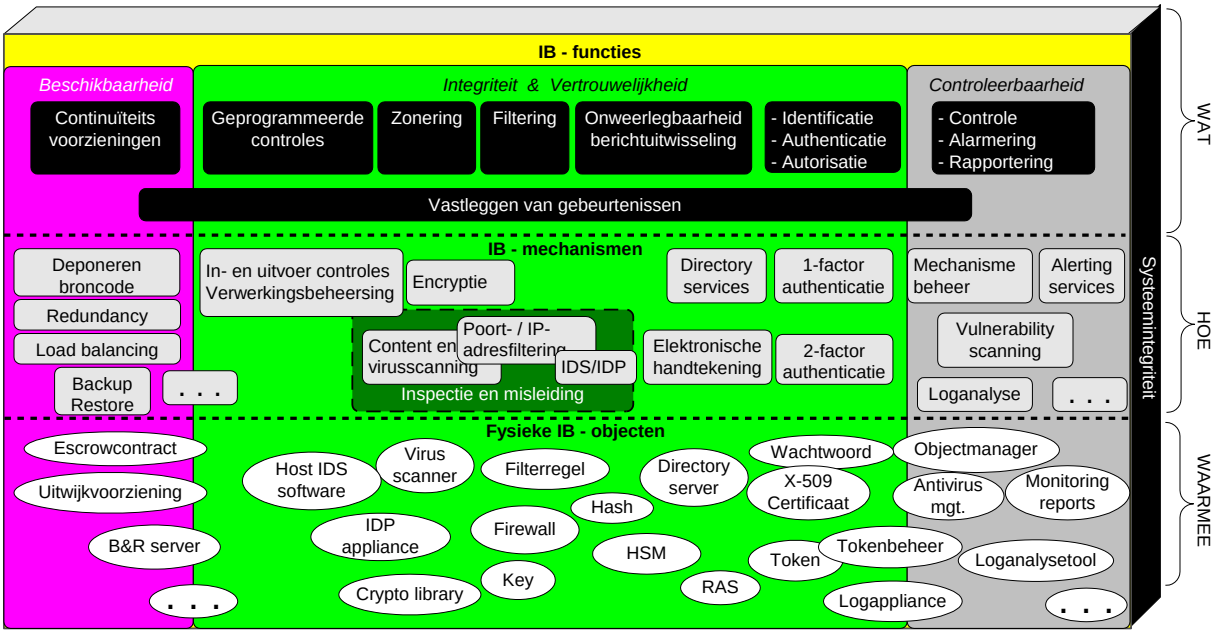
http://e-overheid.nl/onderwerpen/architectuur-en-nora/982-dossier-informatiebeveiliging
en speciaal het document over de architectuuraanpak
http://e-overheid.nl/images/stories/nieuws_2010/arch_aanpaknoradossier_informatiebeveiliging.pdf

De aanpak is universeel toepasbaar voor elk IB-normenkader dat zich baseert op ISO 27002.

Het referentiekader voor de patronen in dit document is het onderstaande NORA- model IB-functies, dat bedoeld is om te ordenen en te verbinden. Het model is een doorontwikkeling van ISO-NEN 7498-2[1].

Een IB-functie is een logische groepering van geautomatiseerde activiteiten, die op een bepaald beveiligingsdoel is gericht. In samenhang worden de negen afgebeelde beveiligingsfuncties dekkend geacht voor de informatiebeveiliging van IT voorzieningen (zwarte functieblokken + Systeemintegriteit).

In het architectuurmodel zijn deze IB-functies geprojecteerd op de kwaliteitscriteria voor informatiebeveiliging: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid. In samenhang vormen ze de “wat” laag van het model.



De IB-functies met bijbehorende mechanismen en fysieke objecten, zijn, op de criteria geprojecteerd, die ze *primair* ondersteunen, maar de functies voor integriteit en vertrouwelijkheid dragen bijvoorbeeld ook bij aan beschikbaarheid. Per IB-functie wordt een doelstelling, definitie, toelichting en motivering gegeven in de NORA best practice Normen informatiebeveiliging IT-voorzieningen, dat op de e-Overheidssite gepubliceerd is als Best Practice voor NORA 3.0.

De IB-mechanismen vormen de “hoe” laag en zijn technische concepten (technieken) die het WAT van de IB-functies invullen. Omdat techniek zich steeds verder ontwikkelt, illustreert de figuur slechts een aantal bekende voorbeelden.

De fysieke IB-objecten vormen de “waarmee” laag. Dit zijn IT-onderdelen, die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een besturingsprogramma of applicatie, maar worden ook als afzonderlijke fysieke modules uitgevoerd. Ook hier zijn slechts enkele bekende voorbeelden getekend. Hoewel

[1] ISO-NEN 7498-2[1] Information processing systems : Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture uit 1991

referentiearchitecturen de “hoe” en “waarmee” laag meestal niet beschrijven, is dat hier wel gedaan om duidelijk te maken hoe en waarmee beveiligingsfuncties uiteindelijk werkzaam kunnen zijn in de IT.

2 Beveiligingseisen en –richtlijnen

Dit hoofdstuk bevat de uitwerking van het tactisch normenkader in patronen. Er wordt geen volledigheid in het aantal patronen gepretendeerd. Het aantal is uitbreidbaar, voor deze versie zijn de voor de implementatie van BIR meest belangrijke patronen uitgewerkt.

Voor de volledigheid wordt nog vermeld dat de uitwerking in de operationele baseline zich beperkt tot technische maatregelen. Fysieke en procedurele maatregelen zijn grotendeels buiten beschouwing gelaten.
Er is gekozen voor gebruik van IB-patronen om de beveiligingsmaatregelen te structureren en beter toepasbaar te maken.

Een patroon bestaat uit de volgende onderdelen:

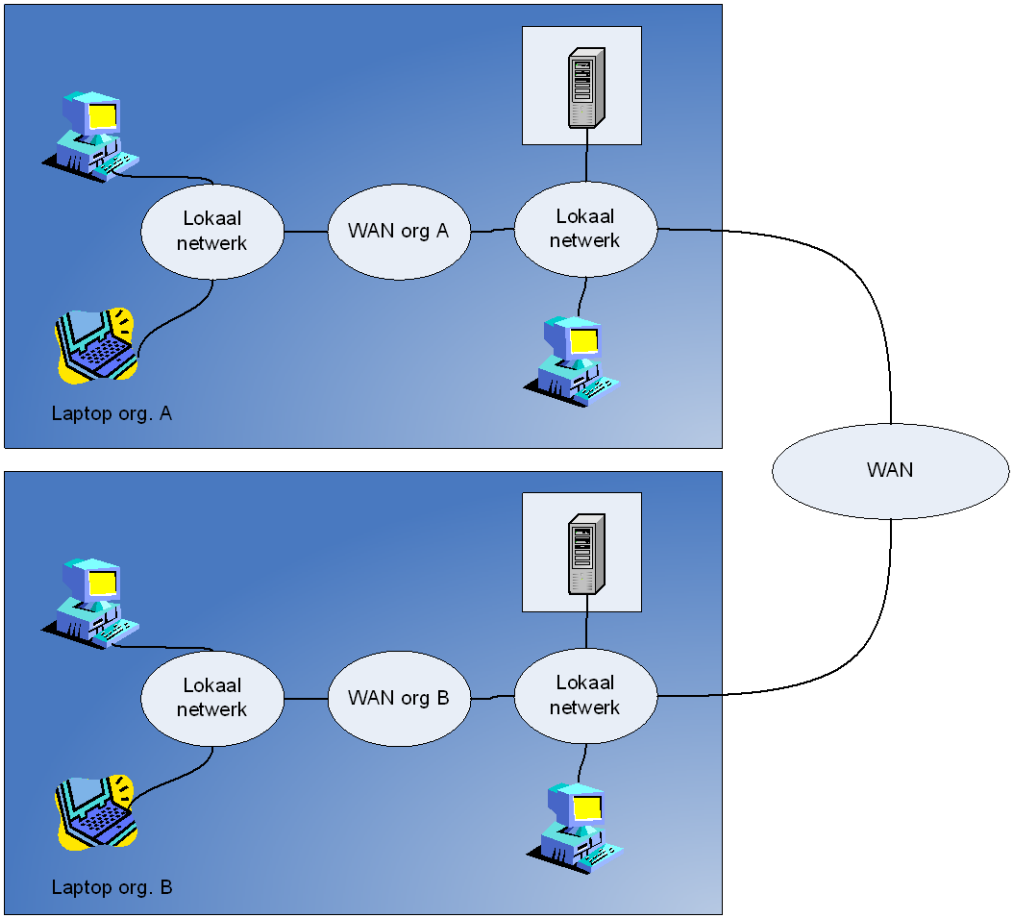
- **Rationale:** De rationale beschrijft vanuit welk oogpunt het patroon is opgezet. Dit is vaak een probleem dat kan worden opgelost door middel van de operationele maatregelen en richtlijnen in het patroon.
- **Context:** De context schetst de omgeving waarop het patroon van invloed is. Dit dient ook om duidelijk te maken wat wel binnen de scope van het patroon valt en wat niet.
- **Oplossing:** De oplossing schetst hoe het probleem beschreven in de context kan worden opgelost. Bij elke oplossing wordt aan de hand van een figuur aangegeven hoe de oplossing op hoofdlijnen werkt, wat de beveiligingsfuncties zijn die worden ingevuld en welke beveiligingsmechanismen daarvoor gebruikt worden.
- **Operationele Maatregelen:** De operationele maatregelen omvatten de lijst van operationele eisen die invulling geven aan de oplossing. Een norm is altijd bindend.
- **Relatie:** De relatie met de tactische normen.

2.1 Patroon generieke netwerkconfiguratie

2.1.1 Rationale

De netwerkomgeving maakt communicatie tussen verschillende compartimenten (zones) mogelijk. Er is sprake van een netwerkketen: het niveau van beveiliging van een zone kan invloed hebben op dat van andere compartimenten. Dit patroon beschrijft daarom de generieke maatregelen die genomen moeten worden in de netwerkinfrastructuur om de meest voorkomende risico's te verminderen.

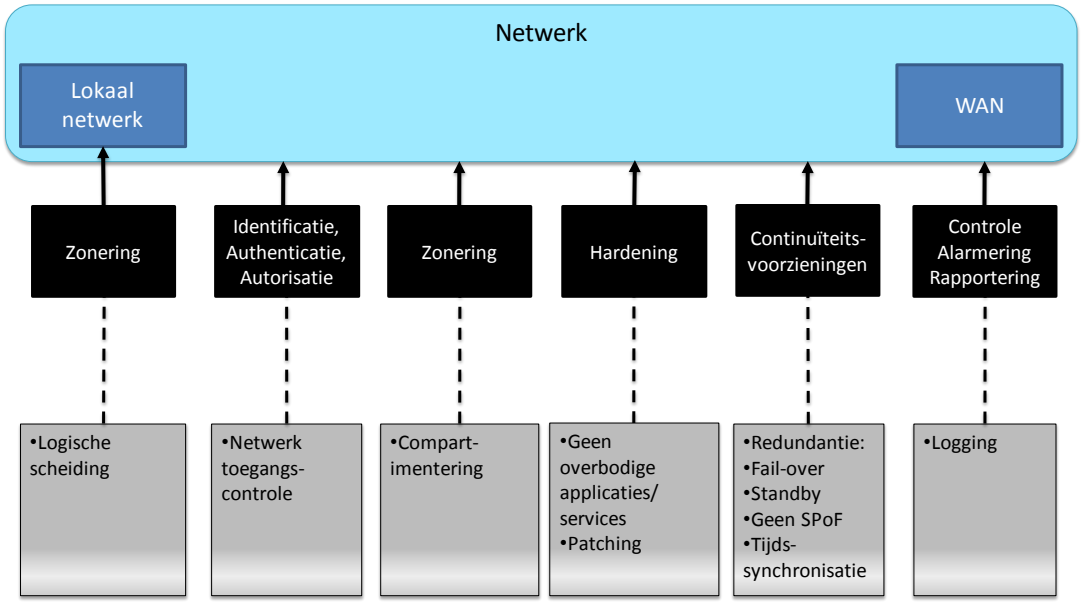
2.1.2 Context



Figuur 1: Generieke netwerkconfiguratie

Om de communicatie te beveiligen wordt gebruik gemaakt van koppelvlakken tussen de verschillende compartimenten (zie figuur 1). Op deze koppelvlakken wordt in de volgende patronen ingegaan. Het netwerk bestaat uit verschillende netwerkelementen: routers, switches, netwerkkabels en firewalls. Deze patronen beschrijven hoe deze elementen veilig gebruikt kunnen worden.

2.1.3 Oplossing



Figuur 2: Beveiligingsfuncties generieke netwerkconfiguratie

De blauwe vlakken in figuur 2 geven de elementen aan die beveiligd moeten worden. De zwarte vlakken noemen de verplichte beveiligingsfuncties. De grijze vlakken geven voorbeelden van maatregelen om die functies te bereiken. Alle patronen figuren bij de patronen zijn op deze wijze beschreven.

De netwerkconfiguratie in figuur 2 is gericht op waarborgen van integriteit en beschikbaarheid van de netwerkinfrastructuur. Daarvoor dient het netwerk gescheiden (ten minste logisch) te zijn van andere niet relevante netwerken (bijvoorbeeld een testomgeving). Het netwerk dient een in een SLA beschreven beschikbaarheid te hebben (Alle specifieke waarden en criteria voor operationele netwerken moeten in een SLA beschreven worden, zie bijlage 1 voor een voorbeeld). Hoge beschikbaarheid kan bijvoorbeeld bereikt worden door redundantie of automatische failover. Bij toepassing van redundantie zijn er geen “Single Points of Failure”. Het netwerk dient alleen te bestaan uit goedgekeurde[2] componenten en dient zo afgeschermd te zijn dat het niet mogelijk is om willekeurige apparatuur aan te sluiten. Voor de beheertoegang tot de netwerkcomponenten dient authenticatie plaats te vinden. Daarnaast is de integriteit van de netwerkcomponenten gebaat bij hardening. Om de beschikbaarheid te bewaken wordt signalering gebruikt.

2.1.4 Operationele maatregelen

Zonering

1. Het netwerk is minimaal logisch gescheiden van andere niet-relevante netwerken (waaronder Ontwikkel, Test en Acceptatie netwerken).
2. Binnen het netwerk zijn compartimenten gecreëerd die in geval van een besmetting kunnen worden afgeschakeld van de rest van het netwerk (Quarantaine).

[2] Onder “goedgekeurd” wordt verstaan “vooraf door onafhankelijke deskundigen aangetoond dat het bestand is tegen de bij BIR voorziene dreigingen”.

3. Alle vertrouwelijke informatie die over onvertrouwde netwerken[3] getransporteerd wordt is versleuteld.
4. Voor beheerdoeleinden wordt een (minimaal) logisch gescheiden netwerk gebruikt.

Identificatie, authenticatie, autorisatie

5. Alleen door netwerkbeheer goedgekeurde netwerkapparatuur wordt gebruikt binnen het netwerk.
6. Ongeautoriseerde toegang tot het netwerk is niet mogelijk[4].

Hardening

7. Op netwerkcomponenten draaien geen overbodige diensten.
8. Daar waar mogelijk zijn producten gebruikt die volgens een internationaal geaccepteerde standaard/organisatie geëvalueerd zijn.

Continuïteitsvoorzieningen

9. Er zijn beschikbaarheidseisen gedefinieerd en vastgelegd in het SLA (zie bijlage 1).
10. De netwerkcomponenten maken gebruik van een stabiele tijdbron zodat timestamps geen grotere afwijking van UTC hebben dan in de SLA (zie bijlage 1) is vastgelegd.

Controle, Alarmering, Rapportering

11. De belasting van systemen wordt automatisch gemeten en kan worden uitgelezen via SNMP zie bijlage 1 voor minimale versie).
12. Alle netwerkkoppelingen zijn geregistreerd en voor geautoriseerde beheerders inzichtelijk.
13. Netwerkhardware ondersteunt centraal wachtwoordmanagement.

Interoperabiliteit/beheer

14. Het is mogelijk om versleutelde informatie over het netwerk te versturen

2.1.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.1.4.1	10.1.4	Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.
2.1.4.1	11.4.5	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
2.1.4.2	10.4.1.4	Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).
2.1.4.3	12.3.1.1	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
2.1.4.3	12.3.1.2	Bij de inzet van cryptografische producten volgt een afweging van de risico's aangaande locaties, processen en behandelende partijen.
2.1.4.3	12.3.1.3	De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
2.1.4.4	11.4.5.4	Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone

[3] Onder "Vertrouwde Netwerken" wordt verstaan: netwerken waarvan door de verantwoordelijke lijnmanager (na deskundig advies) is vastgesteld dat de netwerken geschikt zijn voor transport van het betreffende vertrouwelijkheidsniveau (voor BIR is dat minimaal "Departementaal Vertrouwelijk").

[4] Dit kan met technische (bijvoorbeeld 802.1x) of fysieke (bijvoorbeeld een beveiligde ruimte) maatregelen.

Operationele norm	TNK referentie	TNK norm
2.1.4.5	11.4.3.1	Alleen geïdentificeerde en geauthenticeerde apparatuur kan worden aangesloten op een vertrouwde zone. Eigen, ongeauthenticeerde, apparatuur (Bring Your Own Device) wordt alleen aangesloten op een onvertrouwde zone.
2.1.4.6	11.4.1	Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.
2.1.4.7	11.4.4	De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.
2.1.4.7	11.4.5.5	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
2.1.4.8	12.1.1.5	Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV goedkeuring of certificering volgens ISO/IEC 15408 (common criteria)
2.1.4.8	12.3.1.3	De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
2.1.4.9	10.2	Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij. Opm. Geldt ook voor interne dienstverleners
2.1.4.9	10.6.2	Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
2.1.4.10	10.10.6.1	Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.
2.1.4.11	10.3.1.1	De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheideis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
2.1.4.11	10.10.1.5	Controle op opslag van logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).
2.1.4.12	10.3.1.3	In koppelpunten met externe of onvertrouwde zones worden maatregelen getroffen om aanvallen te signaleren en hierop te reageren. Het gaat hier om aanvallen die erop gericht zijn de verwerkingscapaciteit zodanig te laten vollopen, dat onbereikbaarheid of uitval van computers het gevolg is (Denial of Service attacks).
2.1.4.13	11.5.3	Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

Operationele norm	TNK referentie	TNK norm
2.1.4.14	Impliciet (b.v. 10.9.2.2)	Opm. Impliciet omdat sommige berichten versleuteld moeten worden verzonden (b.v. 10.9.2.2) 10.9.2.2: Een transactie is versleuteld, de partijen zijn geauthenticeerd en de privacy van betrokken partijen is gewaarborgd.

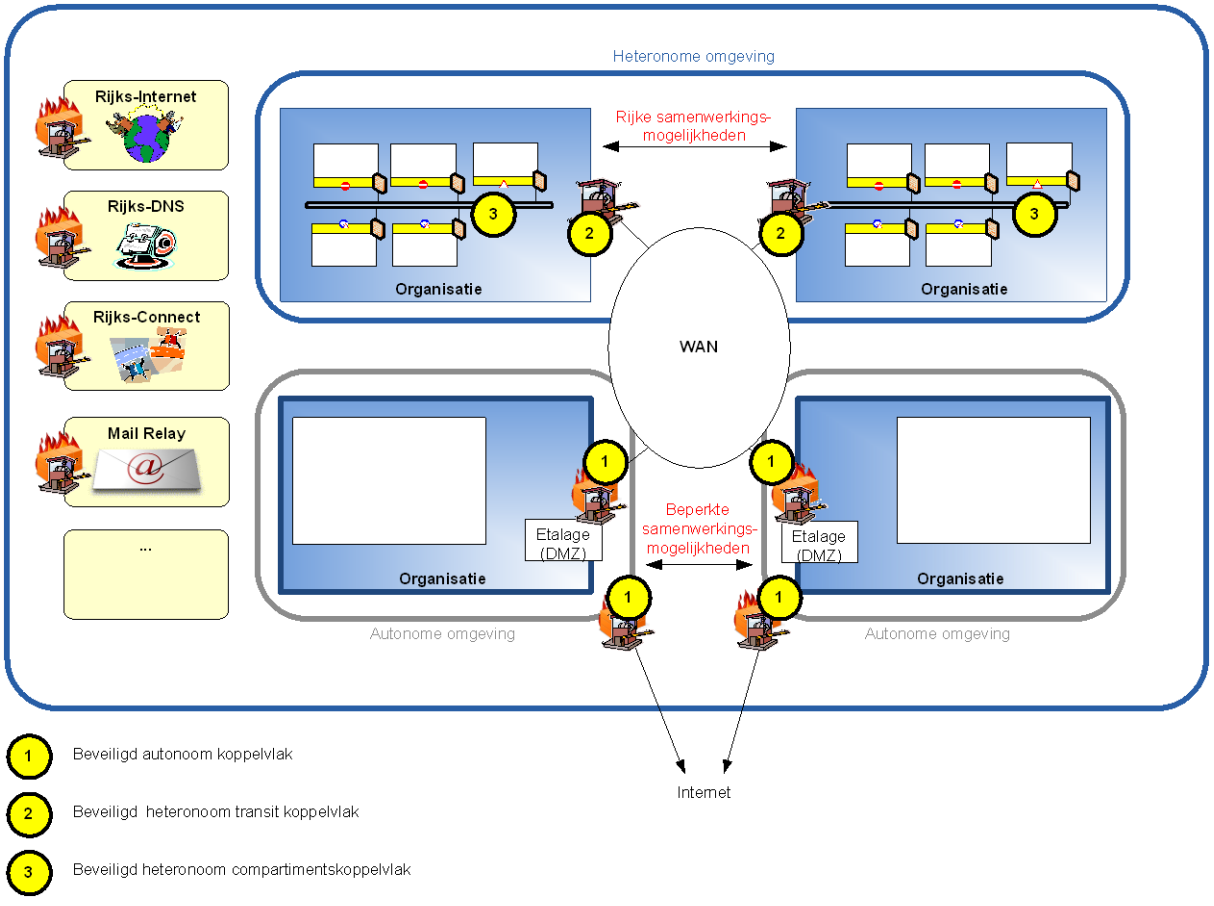
2.2 Patroongroep koppelvlakken

2.2.1 Rationale

Netwerken hebben koppelingen met zowel vertrouwde als onvertrouwde netwerken. De koppelvlakken die hier beschreven worden zorgen ervoor dat de koppeling geen afbreuk doet aan het algehele beveiligingsniveau. De wijze van inrichting van het koppelvlak hangt af van de mate waarin het andere netwerk en de informatie die wordt uitgewisseld vertrouwd wordt.

Koppeling met Internet verdient speciaal de aandacht omdat een Internetverbinding door iedereen gebruikt kan worden om een communicatieverbinding met interne systemen op te zetten. Daarom is het van belang dat dit verkeer geïnspecteerd en gefilterd wordt op mogelijke dreigingen. Hierdoor kan de integriteit en beschikbaarheid van de systemen worden verhoogd.

2.2.2 Context



Figuur 3: Koppelvlakken

Figuur 3 geeft een voorbeeld van verschillende netwerken en de koppelvlakken daartussen
Door het netwerk onder te verdelen in compartimenten wordt het beheer eenvoudiger: filter-regels worden bijvoorbeeld niet meer gebaseerd op individuele systemen maar op compartimenten. Daarnaast zorgt een

gemeenschappelijke zoneringsmethodiek er voor dat de samenhang en compatibiliteit optimaal is waardoor er minder problemen voor de beschikbaarheid te verwachten zijn.

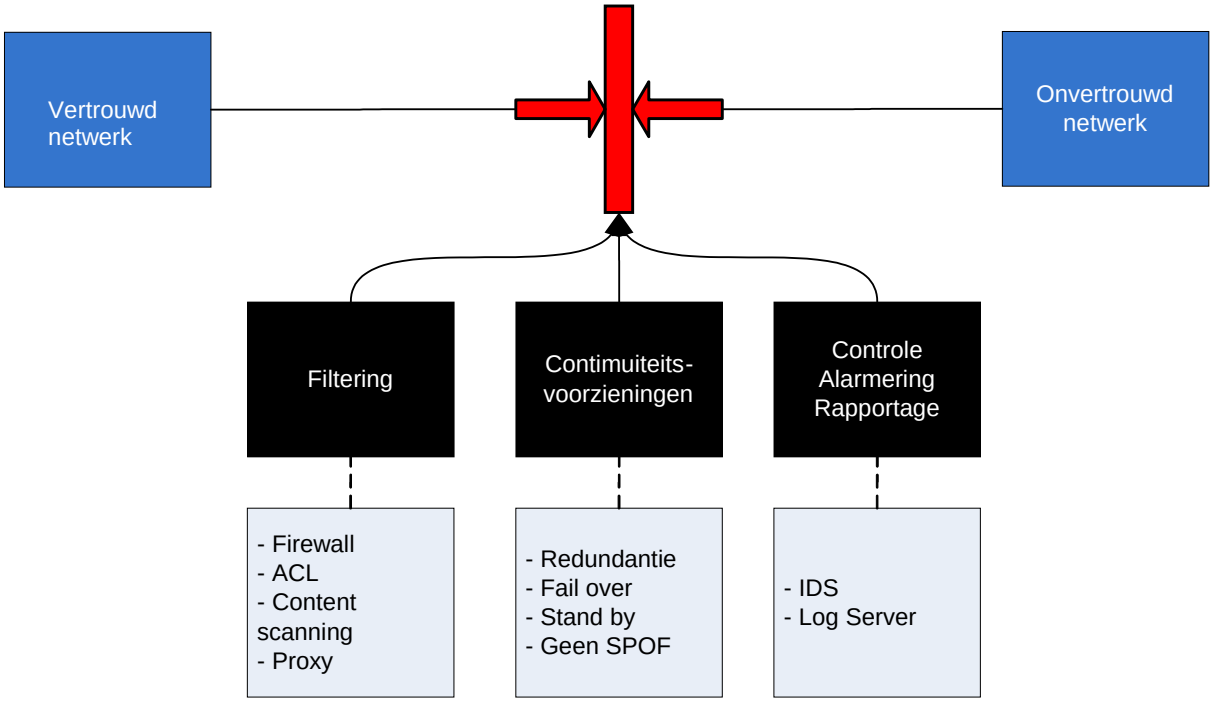
De netwerkarchitectuur voor het Rijk is op te splitsen in departementale netwerkcompartimenten en een centraal netwerkcompartiment. Hoewel in principe het beveiligingsniveau identiek is, is ook hier een koppelvlak nodig; niet zozeer voor preventie van incidenten maar voor de detectie ervan. Dit maakt het achterhalen van de bron en oorzaak van (beveiligings-) incidenten eenvoudiger, waardoor problemen sneller opgelost kunnen worden en het beveiligingsniveau gehandhaafd blijft. Koppelvlakken voor vertrouwde netwerken zijn aangegeven met cijfer 2.

Koppelvlakken voor onvertrouwde netwerken zijn aangegeven met cijfer 1. Deze koppelvlakken koppelen de netwerkarchitectuur voor het Rijk aan externe partijen. Dit zijn partijen die niet aan de beveiligingsmaatregelen (hoeven te) voldoen die wel aan de departementen worden gesteld. Om ervoor te zorgen dat het risico op beveiligingsincidenten die door deze koppeling wordt veroorzaakt tot een acceptabel niveau wordt teruggebracht moeten maatregelen getroffen worden.

De inrichting van de koppelvlakken aan de hand van patronen is hierna uitgewerkt voor 2 verschillende varianten:

- Beveiligd koppelvlak voor onvertrouwde netwerken
- Beveiligd koppelvlak voor vertrouwde netwerken

2.3 Subpatroon beveiligd koppelvlak onvertrouwde netwerken



2.3.1 Oplossing

Figuur 4: koppelvlak met onvertrouwd netwerk

figuur 4 toont de IB-functies en mechanismen voor het subpatroon beveiligd koppelvlak voor onvertrouwde netwerken. Om de *integriteit* en *vertrouwelijkheid* van computersystemen in een netwerk te waarborgen wanneer gekoppeld wordt met een onvertrouwd netwerk wordt *zonering* toegepast. De afscherming van de computersystemen binnen het netwerk vindt plaats door *filtering* toe te passen in het koppelvlak van het netwerk. Aangezien gekoppeld wordt met een onvertrouwd netwerk, is de filtering gericht op het alleen doorlaten van vereiste verkeersstromen en inspecteren van doorgelaten verkeersstromen. Voor binnenkomende verkeersstromen is de doelstelling primair de integriteit van de eigen computersystemen. Voor uitgaande verkeersstromen is de doelstelling primair de vertrouwelijkheid (tegengaan van onbedoeld weglekken van informatie).

De filtering kan worden uitgevoerd door een *firewall (netwerkniveau)* of een *reverse proxy (applicatieniveau)* die geplaatst is in het koppelvlak. De filtering bestaat uit *protocol validatie* en *content- en virusscanning* van al het verkeer door het koppelvlak. Informatie over de filtering wordt *gelogd* en indien urgent gekoppeld aan *alarmering*. Dit ten behoeve van *controle, alarmering en rapportering*.

Als er diensten aan externe partijen geboden worden staan de servers hiervoor in een DMZ (zie patroon DMZ). Een reverse proxy is een logische scheiding tussen de aangeboden diensten in het ene netwerk en de clients in het andere. De reverse proxy is geplaatst in de DMZ en schermt de interne servers af van de buitenwereld door alle inkomende verzoeken te filteren. Andersom worden er geen gegevens (IP adres, software versies) over de interne servers gelekt naar buiten.

Een IDS controleert al het netwerkverkeer en detecteert mogelijke aanvallen. De detectie gebeurt door controle op signatures van bekende aanvallen, controle op correct gebruik van protocollen en statistische controle op grote afwijkingen van het normale gebruik (anomaly based). Vooral de laatste categorie kan veel false positives geven. Om de beschikbaar te kunnen garanderen wordt aanbevolen geen IPS te gebruiken. Een false positive zou dan een dienst onbereikbaar kunnen maken en de kans op DOS aanvallen vergroten.

2.3.2 Operationele maatregelen

Filtering

1. Het koppelvlak heeft een default deny policy (voor netwerkpoorten) en alleen geautoriseerd dataverkeer is toegestaan.
2. Netwerkverkeer wordt gecontroleerd op de aanwezigheid van malware.
3. Een firewall controleert op de juiste format van protocolheaders en blokkeert datastromen die afwijken van de standaard voor het gebruikte protocol.
4. Een reverse proxy controleert op de juiste syntax en format van de informatie aan de hand van de specificaties behorend bij de applicatie en blokkeert ongeldige datastromen.
5. Rechtstreekse verbinding tussen systemen binnen het productie netwerk en systemen in het onvertrouwde netwerk worden voorkomen.

Continuïteitsvoorzieningen

6. Het koppelvlak heeft een in de sla omschreven beschikbaarheid.

Controle, Alarmering, Rapportering

7. Informatie over de inkomende en uitgaande datastromen wordt minimaal 3[5] maanden bewaard (niet de inhoud van de datastroom maar o.a. timestamp, bron IP/poort, doel IP/poort, protocol).
8. Informatie over de datastromen is alleen inzichtelijk voor geautoriseerde personen.
9. Een element (reverse proxy, firewall, ids) op de grens naar een onvertrouwd netwerk lekt nooit informatie (ip adres, software versie) van interne servers naar het externe netwerk .
10. Een Intrusion Detection Systeem detecteert netwerk gebaseerde aanvallen middels signatures, protocol validation en anomaly detection
11. Er worden IDS signatures voor bekende aanvallen op alle extern bereikbare diensten gebruikt.
12. IDS signatures worden regelmatig (interval bepaald in het SLA) bijgewerkt.
13. Protocolheaders worden gevalideerd.
14. Het IDS houdt rekening met fragmentatie van pakketten.
15. IDS alerts worden geanalyseerd.

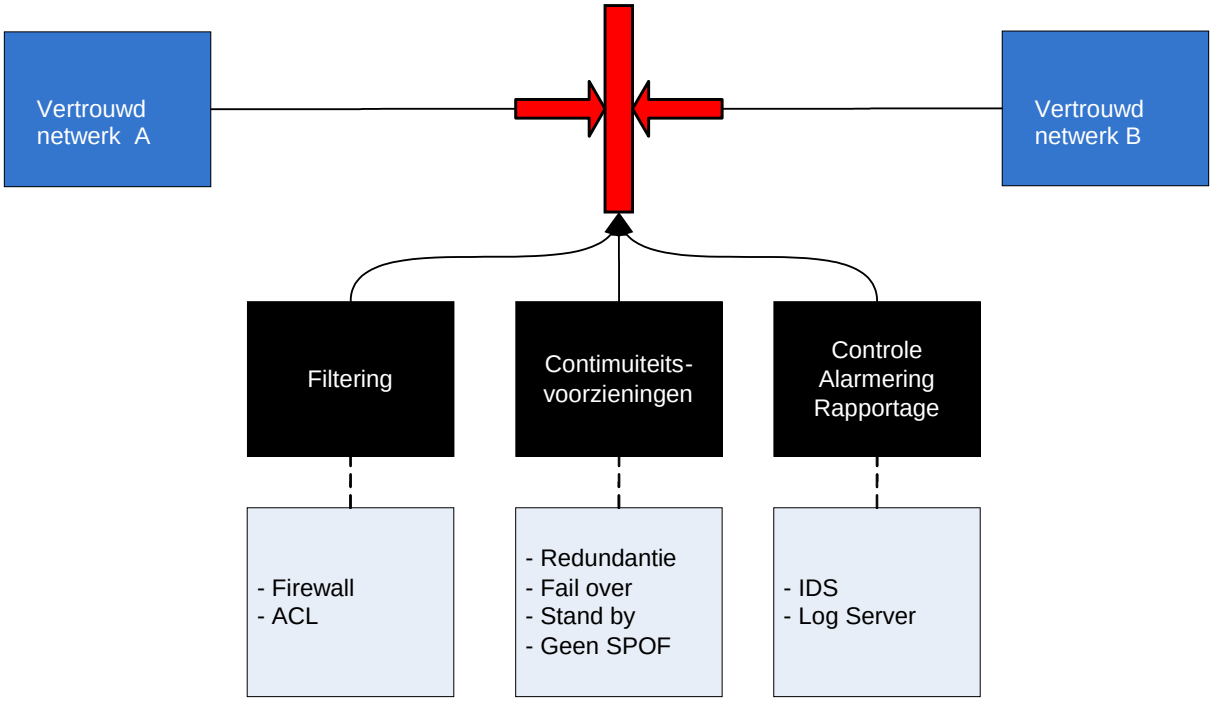
[5] Deze termijn is de minimaal bewaartermijn voor logs volgens het Voorschrift Informatiebeveiliging Rijksdienst – Gerubriceerde Informatie.

2.3.3 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.3.2.1	11.4.5	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
2.3.2.2	10.4.1.1	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
2.3.2.2	10.4.1.2	Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
2.3.2.3	11.4.5.3	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
2.3.2.4	10.4.1.1	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats
2.3.2.4	11.4.5.3	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
2.3.2.5	11.4.6	Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen
2.3.2.5	12.5.4.1	Op het grensvlak van een vertrouwde en een onvertrouwde omgeving vindt content-scanning plaats
2.3.2.6	Hfdstk 2.2	De BIR:2012 definieert een basisset aan eisen voor beschikbaarheid voor de departementale en interdepartementale infrastructuur. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de dienstenleverancier. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening er een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.
2.3.2.7	10.10.1	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
2.3.2.7	10.10.1.2	Een logregel bevat minimaal: • een tot een natuurlijk persoon herleidbare gebruikersnaam of ID • de gebeurtenis (zie 10.10.2.1) • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis
2.3.2.8	10.10.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
2.3.2.9	12.5.4	Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

Operationele norm	TNK referentie	TNK norm
2.3.2.10	10.4.1	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.
2.3.2.11	Geen referentie naar TNK	Opm. Nadere invulling van 2.3.10
2.3.2.12	Geen referentie naar TNK	Opm. Nadere invulling van 2.3.10
2.3.2.13	Geen referentie naar TNK	Opm.: is het nodig deze te handhaven? Dit doet 2.3.10 al.
2.3.2.14	Geen referentie naar TNK	Opm. Nadere invulling van 2.3.10
2.3.2.15	10.10.1.1	Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
2.3.2.15	13.2.3.1	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

2.4 Subpatroon beveiligd koppelvlak vertrouwde netwerken



2.4.1 Oplossing

Figuur 5: Koppelvlak vertrouwd netwerk

Figuur 5 schetst de IB-functies en mechanismen voor het subpatroon beveiligd koppelvlak voor vertrouwde netwerken. Om de *integriteit* van computersystemen in een netwerk zoveel mogelijk te waarborgen kan *zonering* worden toegepast door middel van een beveiligd koppelvlak. De afscherming van de computersystemen binnen een netwerk vindt dan plaats door *filtering* toe te passen in het koppelvlak van het netwerk. Aangezien het koppeling van vertrouwde netwerken betreft, is de filtering vooral gericht op detectie van mogelijke problemen. Informatie met betrekking tot de filtering dient te worden *gelogd* en indien urgent te worden gekoppeld aan *alarmering*.

2.4.2 Operationele maatregelen

Filtering

1. De geautoriseerde datastromen die door het koppelvlak gaan worden niet geblokkeerd of gewijzigd.
2. Het koppelvlak heeft een default deny policy en alleen geautoriseerd dataverkeer is toegestaan.
3. Alleen compartimenten die bereikbaar moeten zijn, mogen bereikbaar zijn.
4. Een Intrusion Detection Systeem detecteert netwerk gebaseerde aanvallen middels signatures, protocol validation en anomaly detection
5. Er worden IDS signatures voor bekende aanvallen op alle extern bereikbare diensten gebruikt.
6. IDS signatures worden regelmatig (interval bepaald in SLA) bijgewerkt.
7. Protocolheaders worden gevalideerd.
8. Het IDS houdt rekening met refragmentatie van pakketten.

Continuïteitsvoorzieningen

9. Het koppelvlak heeft een in de sla beschreven beschikbaarheid.

Controle, Alarmering, Rapportering

10. Informatie over de inkomende en uitgaande datastromen wordt minimaal 3 maanden bewaard (niet de inhoud van de datastroom maar timestamp, bron IP/poort, doel IP/poort, protocol)
11. Informatie over de datastromen is alleen inzichtelijk voor geautoriseerde personen en beveiligingsfunctionarissen.
12. IDS alerts worden geanalyseerd.

2.4.3 Relatie tactische normen

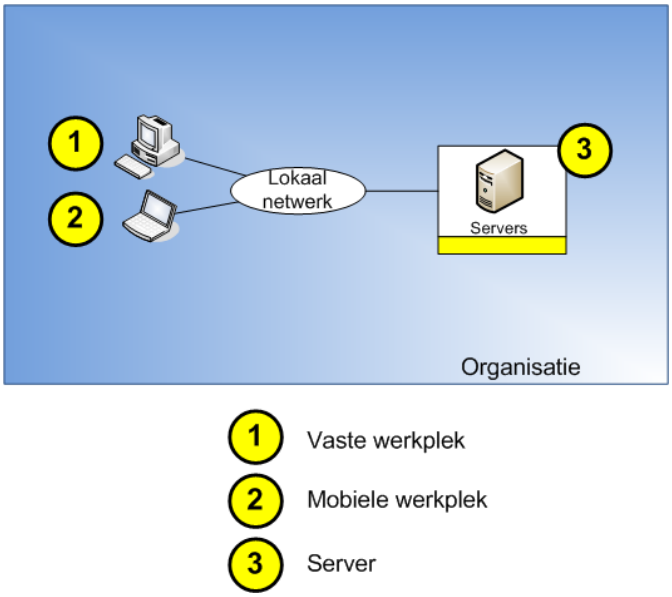
Operationele norm	TNK referentie	TNK norm
2.4.2.1	Geen referentie	Opm. Impliciete maatregel die een gevolg is van wederzijds vertrouwen.
2.4.2.2	11.4.5	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
2.4.2.3	11.4.1	Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.
2.4.2.4	10.4.1	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.
2.4.2.5	Geen referentie naar TNK	Opm. Nadere invulling van 2.3.10
2.4.2.6	Geen referentie naar TNK	Opm. Nadere invulling van 2.3.10
2.4.2.7	Geen referentie naar TNK	Opm.: is het nodig deze te handhaven? Dit doet 2.3.10 al.
2.4.2.8	Geen referentie naar TNK	Opm. Nadere invulling van 2.3.10
2.4.2.9	Hfdstk 2.2	De BIR:2012 definieert een basisset aan eisen voor beschikbaarheid voor de departementale en interdepartementale infrastructuur. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de dienstenleverancier. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening er een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.
2.4.2.10	10.10.1	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
2.4.2.10	10.10.1.2	Een logregel bevat minimaal: • een tot een natuurlijk persoon herleidbare gebruikersnaam of ID • de gebeurtenis (zie 10.10.2.1) • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis
2.4.2.11	10.10.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
2.4.2.12	10.10.1.1	Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
2.4.2.12	13.2.3.1	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

2.5 Patroongroep servers en werkplekken

2.5.1 Rationale

Servers en werkplekken worden gebruikt om toegang tot diensten en applicaties mogelijk te maken en zijn kwetsbaar voor besmetting (malware), ongeautoriseerde toegang en dataverlies (bij bijvoorbeeld diefstal of inbraak). Om deze diensten, applicaties en de informatie die verwerkt wordt te beschermen, moeten er maatregelen getroffen worden op de servers en werkplekken.

2.5.2 Context



Figuur 6: Servers en werplekken

Figuur 6 toont de verschillende systemen die zijn te onderscheiden. Het is mogelijk om vanuit een werkplek toegang te krijgen tot departementale diensten en applicaties, maar ook webapplicaties die extern worden aangeboden. Een voorbeeld hiervan is P-direct. Bij de werkplekken is er onderscheid in vaste werkplekken en mobiele werkplekken. Mobiele werkplekken kunnen ook gebruikt worden buiten het departement en zonder netwerktoegang.

Diensten en applicaties worden geïnstalleerd op servers, die via het netwerk aan elkaar en de werkplekken verbonden zijn. Servers kunnen departementaal of centraal worden geplaatst.

De configuratie van de systemen aan de hand van patronen is hierna uitgewerkt in een generieke systeemconfiguratie voor alle systemen en generieke configuraties voor de onderscheiden typen systemen:

1. Generieke werkplekconfiguratie (vaste werkplek)
2. Generieke werkplekconfiguratie (mobiele werkplek)
3. Generieke serverconfiguratie

Niet alle relevante beveiligingsaspecten zijn in de subpatronen verwerkt; er is voor gekozen om bepaalde maatregelen te groeperen in specifieke patronen, zoals:

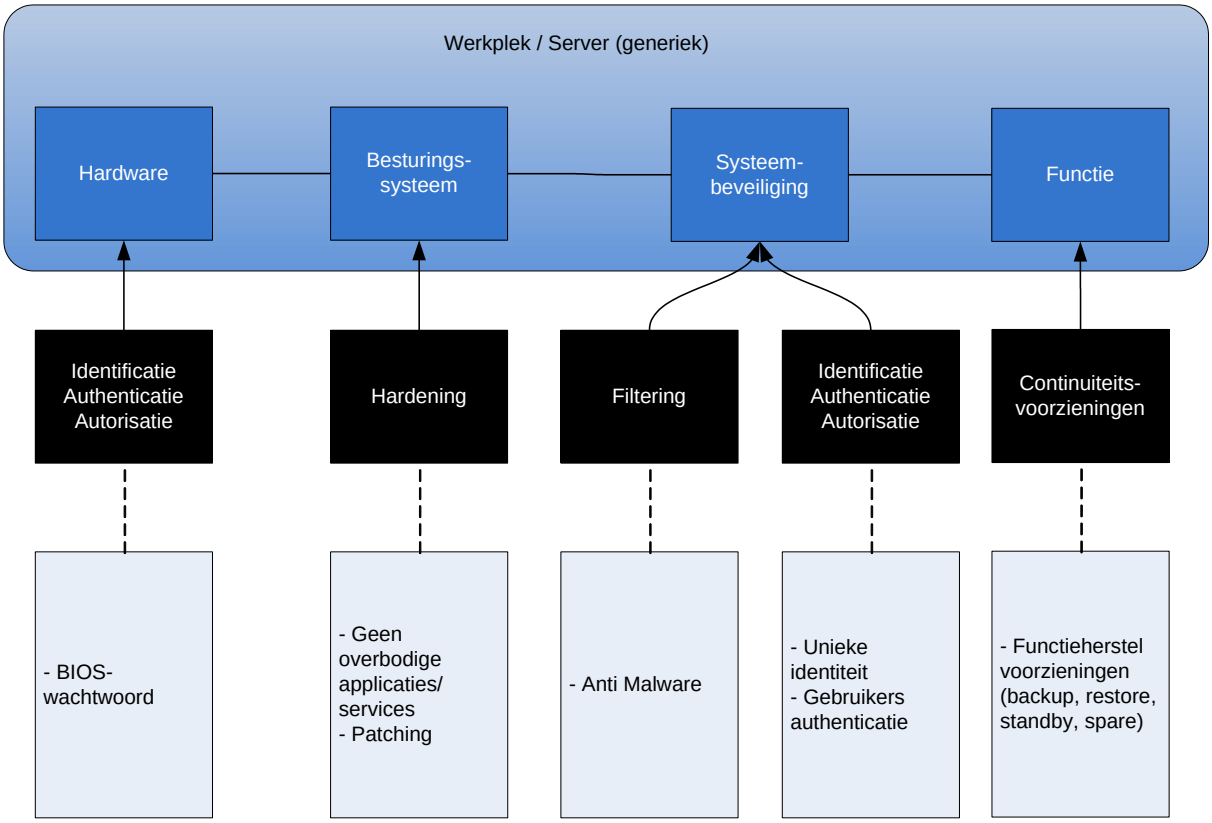
- Patroon Generieke applicatieconfiguratie (Programma-controles)
- Patroon Identificatie, Authenticatie, Autorisatie (IAA)

- Patroon Logging/Monitoring (Controle, alarmering, rapportering)
- Patroon Backup (Continuïteitsvoorzieningen)

Fysieke maatregelen zijn niet in deze baseline uitgewerkt. Voldoen aan de eisen hiervoor uit het Tactisch Normenkader zou voldoende moeten zijn, en niet tot implementatie- of interoperabiliteitsproblemen moeten leiden.

2.6 Subpatroon generieke systeemconfiguratie

2.6.1 Oplossing



Figuur 7: generieke systeemconfiguratie

Figuur 7 schetst de IB-functies en mechanismen voor het subpatroon generieke systeemconfiguratie. Dit subpatroon is van toepassing op zowel alle servers als alle werkplekken.

Systeemconfiguratie is primair gericht op de *integriteit* van het betreffende systeem. Dit is te bereiken door het systeem te *hardenen* en periodiek dan wel real-time te *filteren op virussen en malware*. Om het risico van malware te beperken (zonder grote performance impact op de werkplek) kan *defense-in-depth* worden toegepast door op servers op een andere wijze te scannen op malware en virussen dan op de werkplek. Daarnaast is *authenticatie* nodig voor het kunnen wijzigen van systeemconfiguraties.

2.6.2 Operationele maatregelen

Identificatie, authenticatie, autorisatie

1. Het is met gebruikersaccounts niet mogelijk automatisch in te loggen (anders dan nodig voor Single Sign On). Alleen systeemprocessen met functionele accounts mogen geautomatiseerd aanloggen.
2. Er zijn gescheiden accounts voor beheertaken en gebruikerstaken.
3. Toegang tot de BIOS/Firmware is voorzien van een wachtwoord

Hardening

4. Besturingssystemen draaien geen overbodige diensten en er zijn geen overbodige applicaties op geïnstalleerd.
5. Rechten van accounts zijn geminimaliseerd
6. Software updates worden binnen de periode genoemd in het SLA geïnstalleerd.
7. Na beoordeling als kritisch getypeerde updates/patches die van een vertrouwde en geautoriseerde bron komen worden binnen de periode genoemd in het SLA (zie bijlage 1) geïnstalleerd.

Filtering

8. Indien mogelijk is op ieder systeem een virusscanner aanwezig, als dit niet mogelijk is wordt deze functionaliteit in ieder geval in het netwerk gerealiseerd. Voor servers geldt dat real-time scanning niet vereist is. Virusscanning dient periodiek (interval bepaald in SLA) plaats te vinden. Voor werkplekken is naast periodiek scanning ook real-time scanning vereist.
9. Virus scanners op servers, werkstations en netwerk zijn van verschillende leveranciers en bevatten verschillende engines
10. Malware patterns/signatures die van een vertrouwde bron en geautoriseerde komen worden (na beoordeling) binnen de periode genoemd in het SLA (zie bijlage 1) toegevoegd.

Continuïteitsvoorzieningen

11. Systemen kunnen worden hersteld in de staat van voor een update (rollback).
12. Updates op besturingssystemen worden eerst getest in een testomgeving om te controleren of de juiste werking van de systemen niet wordt beïnvloed

2.6.3 Relatie tactische normen

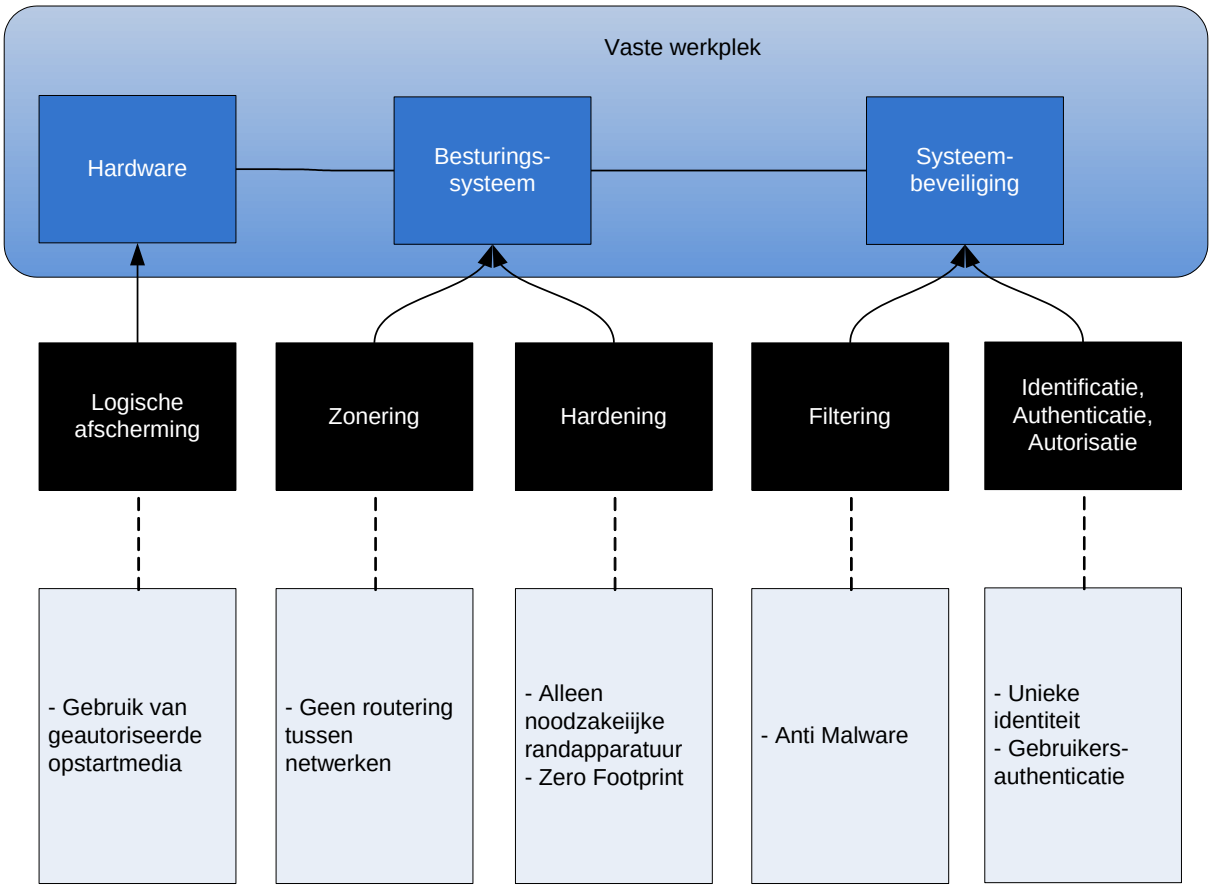
Operationele norm	TNK referentie	TNK norm
2.6.2.1	11.3.1.1	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: • Wachtwoorden worden niet opgeschreven. • Gebruikers delen hun wachtwoord nooit met anderen. • Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde. • Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).
2.6.2.2	10.1.3.4	Verantwoordelijkheden voor beheer en wijziging van gegevens en bijbehorende informatiesysteemfuncties moeten eenduidig toegewezen zijn aan één specifieke (beheerders)rol.
2.6.2.2	11.2.2	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.
2.6.2.3	11.2.2	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.
2.6.2.4	geen	Opm.: Niet specifiek in BIR TNK (overwegen voor volgende versie) maar goede ICT praktijk.
2.6.2.5	11.1.1	Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.
2.6.2.6	12.6.1.4	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde
2.6.2.7	12.6.1.4	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig

Operationele norm	TNK referentie	TNK norm
		mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde
2.6.2.8	10.4.1.1	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
2.6.2.8	10.4.1.2	Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
2.6.2.8	11.7.1.2	Er zijn, waar mogelijk, voorzieningen om de actualiteit van anti-malware programmatuur op mobiele apparaten te garanderen.
2.6.2.9	10.4.1.3	In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirusprogrammatuur van verschillende leveranciers toegepast.
2.6.2.10	12.6.1.2	Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
2.6.2.11	12.4.1.6	Er is een rollbackstrategie.
2.6.2.12	12.6.1.3	Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).

2.7 Subpatroon generieke werkplekconfiguratie

2.7.1 Oplossing

Vaste werkplek



Figuur 8: Generieke werkplekconfiguratie

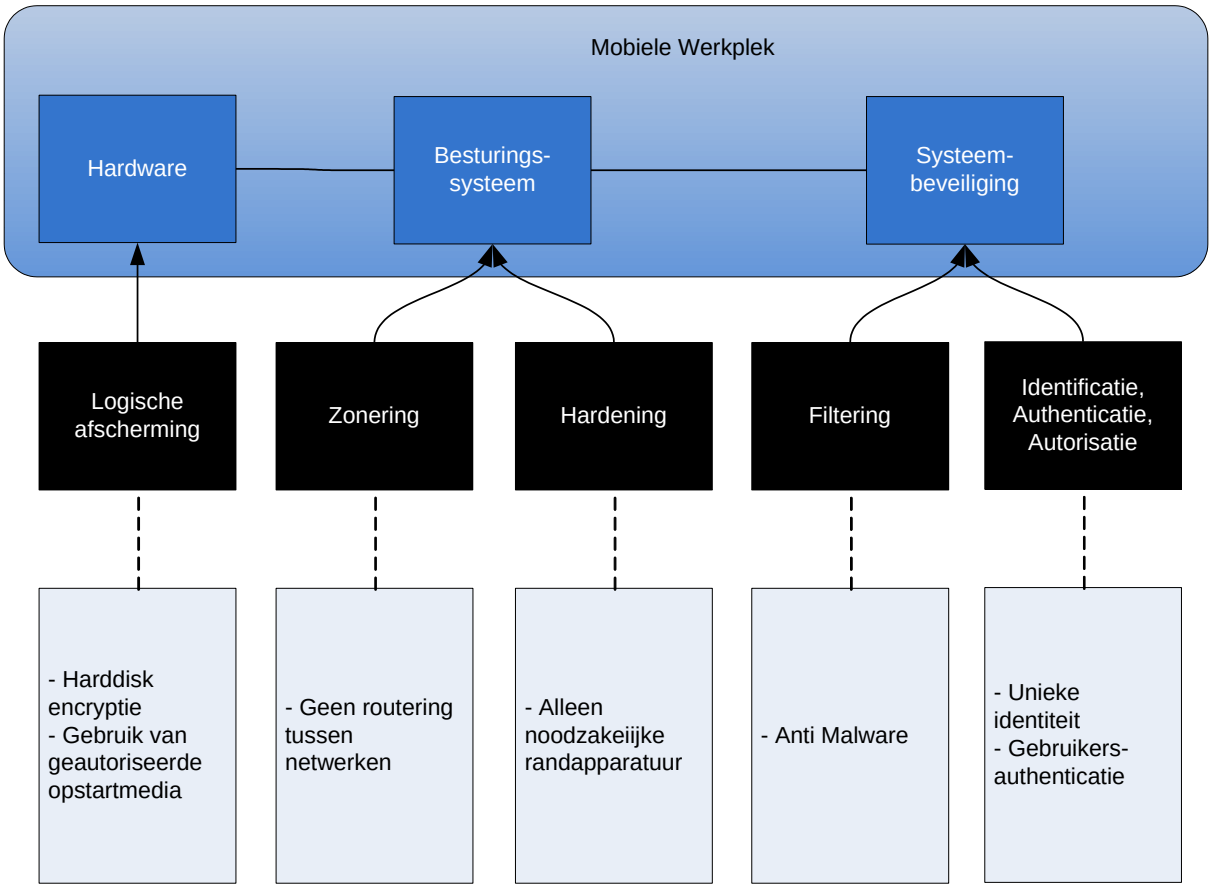
Figuur 8 schetst de IB-functies en mechanismen voor het subpatroon generieke werkplekconfiguratie (vast werkplek). De configuratie van de vaste werkplek is primair gericht op het waarborgen van *integriteit* en secundair van *vertrouwelijkheid*. *Beschikbaarheid* is minder belangrijk omdat de werkplekken *redundant* zijn uitgevoerd en een gebruiker uit kan wijken naar een andere werkplek. Voor integriteit is het essentieel dat het risico van infectie door malware e.d. wordt beperkt door gebruik van *virusscanners* en de lokale *firewall*. Dit risico kan verder worden beperkt door in principe geen randapparatuur toe te staan en het opstarten van de werkplek dusdanig in te richten dat het voor een aanvaller vrijwel onmogelijk is om hiertussen te komen.

Het risico van onbevoegde toegang tot de werkplek (d.w.z. niet de gebruiker zelf of een beheerder) dient beperkt te worden omdat naast de integriteit van de werkplek zelf ook die van het netwerk in het geding is. De werkplek zou door een aanvaller kunnen worden gebruikt als opstap voor een aanval richting het netwerk. Een gebruiker mag zijn werkplek nooit onbeschermd achter laten. Omdat een gebruiker dit kan vergeten dient de werkplek ook automatisch

te blokkeren als deze een bepaalde tijd niet wordt gebruikt. Verder mag een werkplek fysiek slechts gekoppeld zijn aan één netwerk.

De *vertrouwelijkheid* van de (gebruiker van de) werkplek kan worden gewaarborgd door de toegang tot de werkplek door een beheerder alleen toe te staan na toestemming van de gebruiker en door *sterke authenticatie* te eisen voor beheerders. Afhankelijk van de mate van *fysieke afscherming* van de werkplek kan nog gekozen worden om na gebruik geen informatie lokaal op de werkplek achter te laten (zero footprint principe) of deze informatie *versleuteld* op te slaan. Hiermee heeft een aanvaller zelfs bij wegnemen van de werkplek geen inzage in informatie of de mogelijkheid de werkplek te manipuleren.

Mobiele werkplek



Figuur 9: Beveiligingsfuncties mobiele werkplek

Figuur 9 schetst de IB-functies en mechanismen voor het subpatroon generieke werkplekconfiguratie (mobiele werkplek). Bij de mobiele werkplek is het risico vrij groot dat deze in vreemde handen komt (verlies, diefstal) terwijl

het juist wel gewenst is dat lokaal op de werkplek informatie wordt opgeslagen (geen zero footprint). Daarom dient de informatie op de werkplek lokaal *versleuteld* te worden opgeslagen. Hiermee heeft een aanvaller zelfs bij wegnemen van de werkplek geen inzage in informatie of de mogelijkheid de werkplek te manipuleren.

2.7.2 Operationele maatregelen vaste werkplek

Hardening

1. Op vaste werkplekken wordt het zero-footprint principe toegepast.

Logische afscherming

2. Vaste werkplekken starten alleen op vanaf vooraf geautoriseerde media.

2.7.3 Operationele maatregelen mobiele werkplek

Logische afscherming

1. De data op de harddisk is versleuteld (volgens het pre-boot harddisk encryptie principe).
2. Om lokaal data op te slaan is een aparte partitie beschikbaar. De partitie waar het besturingssyteem op staat is niet door de gebruiker aan te passen.

2.7.4 Operationele maatregelen vaste en mobiele werkplek

Logische afscherming

1. Per departement is vastgesteld of, en welke mobiele datadragers worden toegestaan. Dit wordt (onafhankelijk van de locatie) afgedwongen.

Zonering

2. Het is niet mogelijk om verschillende netwerken via de werkplek te verbinden.
3. Vertrouwelijke gegevens worden alleen versleuteld (zoals beschreven in bijlage 2) opgeslagen op mobiele datadragers.

Hardening

4. Standaard wordt randapparatuur niet ondersteund, naast de uitzonderingen voor o.a. toetsenborden, muizen en mobiele datadragers.

Filtering

5. Het besturingssysteem gebruikt beveiligingssoftware waaronder anti – virussoftware, tools tegen spyware; anti-phishingsoftware, encryptiesoftware (zie eisen in bijlage 2) en een (alleen centraal) configureerbare lokale firewall.
6. De virus scanner controleert bestanden periodiek (interval bepaald in het SLA) en op het moment dat ze geopend worden.
7. Werkplekken staan inkomend netwerkverkeer van andere werkplekken (anders dan beheerwerkplekken) niet toe.
8. Netwerkverkeer op werkplekken wordt met een lokale firewall beperkt tot expliciet toegestane verkeersstromen.

Identificatie, authenticatie, autorisatie

9. Het wachtwoord van het lokale administrator account (indien aanwezig) wordt centraal opgeslagen en beheerd.
10. Gebruikers kunnen niet ongeautoriseerd lokale administrator rechten verkrijgen.

11. Gebruik van lokale administrator rechten is zichtbaar voor geautoriseerde personen.
12. De werkplekken zijn voorzien van een screensaver met wachtwoord die inschakelt na een periode van inactiviteit zoals bepaald in het SLA (zie bijlage 1).
13. Beheertoegang van afstand vereist expliciete goedkeuring van de gebruiker, waarbij de gebruiker de mogelijkheid heeft om de beheersessie te beëindigen.
14. Het is niet toegestaan om automatisch als een bepaalde gebruiker in te loggen.
15. Applicaties en gebruikers op werkplekken krijgen niet meer rechten dan noodzakelijk is voor de uitvoering.

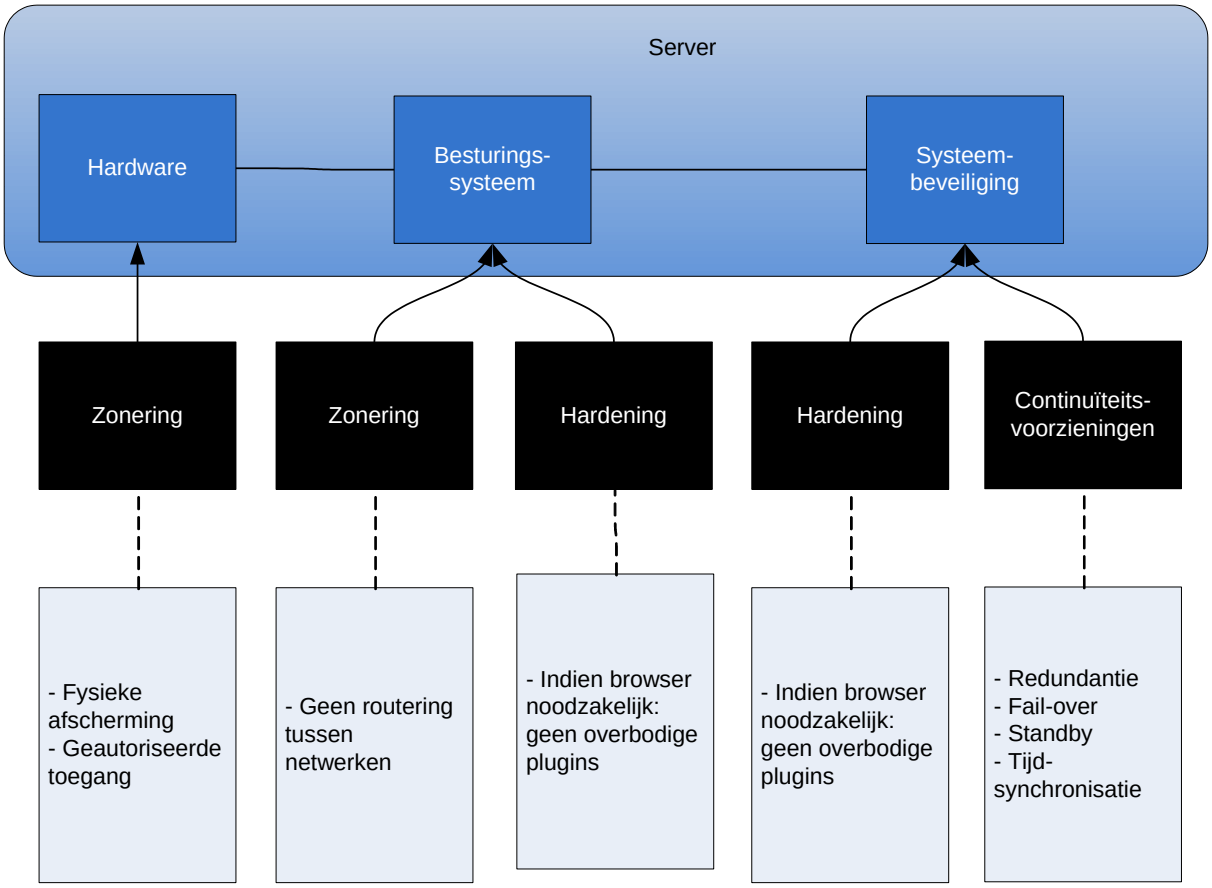
2.7.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.7.2.1	geen	Opm.: Zero footprint in TNK is alleen voorgeschreven voor mobiele werkplekken: 11.7.1.1 en 11.7.2.2;
2.7.2.2	geen	Opm.: Niet in TNK maar dit is wel goede ICT praktijk.
2.7.3.1	11.7.1.1	Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen (“zero footprint”). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats
2.7.3.2	geen	Opm.: Niet in TNK maar dit is wel goede ICT praktijk.
2.7.4.1	5.1.1	Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen
2.7.4.2	11.4.5.1	Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
2.7.4.3	11.7.1.1	Het mobiele apparaat is waar mogelijk zo ingericht dat geen bedrijfsinformatie wordt opgeslagen (“zero footprint”). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, geldt: een mobiel apparaat (zoals een handheld computer, tablet, smartphone, PDA) biedt de mogelijkheid om de toegang te beschermen d.m.v. een wachtwoord en versleuteling van die gegevens. Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats
2.7.4.3	10.8.3	*Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.*
2.7.4.3	10.8.3.1	Om vertrouwelijke informatie te beschermen worden maatregelen genomen, zoals: • versleuteling • bescherming door fysieke maatregelen, zoals afgesloten containers • gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • persoonlijke aflevering • opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes

Operationele norm	TNK referentie	TNK norm
2.7.4.3	10.8.3.2	Fysieke verzending van bijzondere informatie dient te geschieden met ministerieel goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.
2.7.4.4	geen	Opm.: Speciaal m.b.t. printen: TNK 11.7.1.1 zegt: Het mobiele apparaat …….Voor printen in onvertrouwde omgevingen vindt een risicoafweging plaats.
2.7.4.5	10.4.1	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.
2.7.4.5	10.4.1.1	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
2.7.4.5	10.4.1.2	Inkomende en uitgaande e-mails worden gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, (automatisch) plaats.
2.7.4.6	10.4.1.1	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
2.7.4.7	geen	
2.7.4.8	geen	
2.7.4.9	geen	
2.7.4.10	11.2.2	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.
2.7.4.11	10.10.2	Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.
2.7.4.12	11.3.3.3	Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.
2.7.4.13	geen	
2.7.4.14	11.3.1.1	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: • Wachtwoorden worden niet opgeschreven. • Gebruikers delen hun wachtwoord nooit met anderen. • Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde. • Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).
2.7.4.15	11.2.2.3	Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties en commando's.

2.8 Subpatroon generieke serverconfiguratie

2.8.1 Oplossing



Figuur 10: Generieke serverconfiguratie

Figuur 10 schetst de IB-functies en mechanismen voor het subpatroon generieke serverconfiguratie. *Beschikbaarheid* van gemeenschappelijke diensten is essentieel voor het functioneren de informatievoorziening. Ook de aspecten *integriteit* en *vertrouwelijkheid* zijn van belang. Servers dienen daartoe fysiek te worden afgeschermd. Voor kritische diensten dienen *continuïteitsvoorzieningen* te worden getroffen, bijvoorbeeld op basis van *redundantie*. Ook voor de servers dient *hardening* en *jailing* te worden toegepast om het risico van mogelijk misbruik van kwetsbaarheden te beperken. Wijzigingen in de serverconfiguratie (zoals bijvoorbeeld updates) dienen voor wijziging uitvoerig te worden getest om er zeker van te zijn dat door de wijziging de *beschikbaarheid* van de server niet in gevaar komt. Om bij mogelijke incidenten adequaat te kunnen optreden is het van belang dat de *logging* is te correleren en daartoe dienen servers dezelfde tijdreferentie aan te houden.

2.8.2 Operationele maatregelen

Zonering

1. Servers bevinden zich in een afgesloten ruimte, waarbij alleen geautoriseerd personeel fysiek toegang heeft tot de systemen.

Hardening

2. Security updates en patches worden binnen de periode bepaald in het SLA (zie bijlage 1) ingevoerd op de productieomgeving.
3. Indien het nodig is op servers mobiele code (javascript, active-x, enz.) uit te voeren (bijv. in de browser) dan mag dit alleen vooraf geautoriseerde mobiele code zijn.
4. Daar waar mogelijk worden producten gebruikt die volgens een geaccepteerde standaard en deskundige organisatie geëvalueerd zijn.
5. Extern bereikbare services draaien nooit onder een system/root/admin account, maar altijd onder een account met minimale privileges nodig voor de service.

Filtering

6. Voor servers geldt dat periodiek (interval bepaald in het SLA) wordt gecontroleerd op virussen en andere malware in de bestanden die zijn opgeslagen.

Continuïteitsvoorzieningen

7. Kritische netwerkdiensten en webapplicaties zijn beschikbaar zoals gedefinieerd in het SLA.
8. Systemen maken gebruik van een stabiele tijdbron zodat timestamps geen grotere afwijking van UTC hebben dan in het SLA is vastgelegd.
9. Geografische scheiding van redundante systemen is zo uitgevoerd dat de kans dat beide locaties geraakt worden door dezelfde calamiteit minimaal is. De minimale afstand tussen de locaties is vastgelegd in het SLA.
10. Bij redundantie kan er zodanig overgeschakeld worden naar het redundante systeem (hardware + software/applicatie) dat de vereiste beschikbaarheid wordt behaald.

2.8.3 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.8.2.1	9.2.1.1	Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningbeveiliging.
2.8.2.2	12.6.1.4	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde
2.8.2.3	10.4.2.1	Mobile code wordt uitgevoerd in een logisch geïsoleerde omgeving (sandbox) om de kans op aantasting van de integriteit van het systeem te verkleinen. De mobile code wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt.
2.8.2.3	10.4.2.2	Een gebruiker moet geen extra rechten kunnen toekennen aan programma's (bijv. internet browsers) die mobiele code uitvoeren.

Operationele norm	TNK referentie	TNK norm
2.8.2.4	12.1.1.5	Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV[6] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria)
2.8.2.5	11.2.1	Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
2.8.2.6	10.4.1	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.
2.8.2.7	5.1.1.1	Er is beleid voor informatiebeveiliging door het lijnmanagement vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten. Het VIR:2007, VIRBI en BIR zijn vastgesteld rijksbreed beleid, het lijnmanagement is verantwoordelijk voor de invulling en uitvoering hiervan.
2.8.2.7	2.2	De BIR:2012 definieert een basisset aan eisen voor beschikbaarheid voor de departementale en interdepartementale infrastructuur. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de dienstenleverancier. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening er een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.
2.8.2.8	10.10.6	De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.
2.8.2.9	9.1.4.2	Reserve apparatuur en backups zijn op een zodanige afstand ondergebracht dat één en dezelfde calamiteit er niet voor kan zorgen dat zowel de hoofdlocatie als de backup/reserve locatie niet meer toegankelijk zijn.
2.8.2.10	geen	

[6] NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.

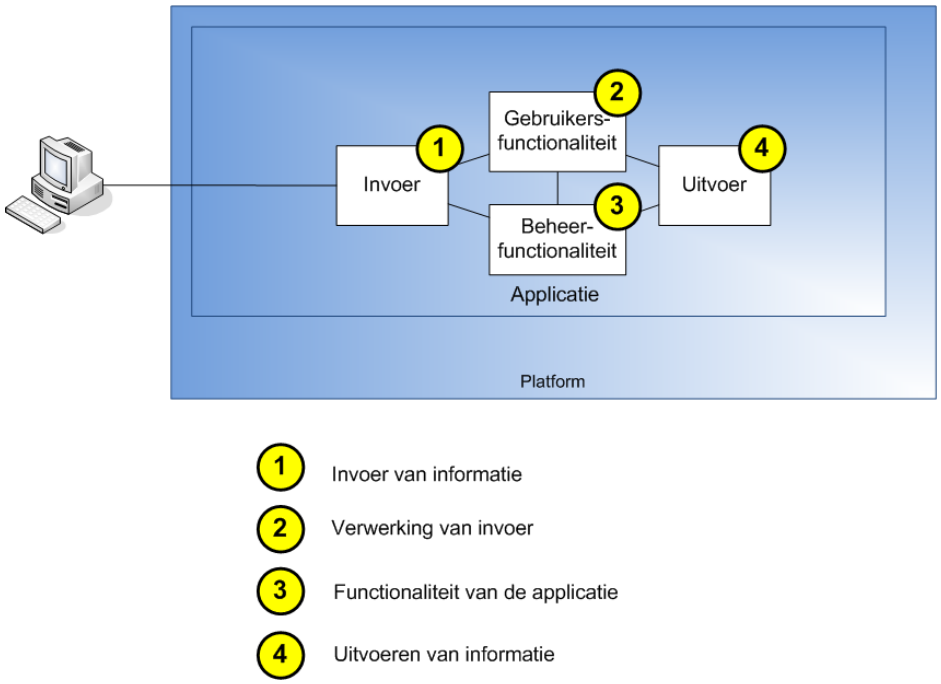
2.9 Patroon generieke applicatieconfiguratie

2.9.1 Rationale

De applicaties die worden aangeboden, zowel generieke applicaties die door alle departementen worden gebruikt als departementaal specifieke applicaties, zijn een potentiële bron van beveiligingsincidenten. Zo hebben applicaties toegang tot informatie, kunnen ze netwerkverkeer genereren en hebben ze de mogelijkheid om de gebruiker aan te sturen (denk aan het vragen om een gebruikersnaam/wachtwoord). Het is daarom van belang dat er afspraken gemaakt worden over beveiligingseisen voor deze applicaties. Hierbij worden twee soorten applicaties onderscheiden: desktop applicaties en webapplicaties. De generieke operationele maatregelen gelden voor beiden. Voor webapplicaties zijn er aanvullende operationele maatregelen

2.9.2 Context

Desktop applicatie



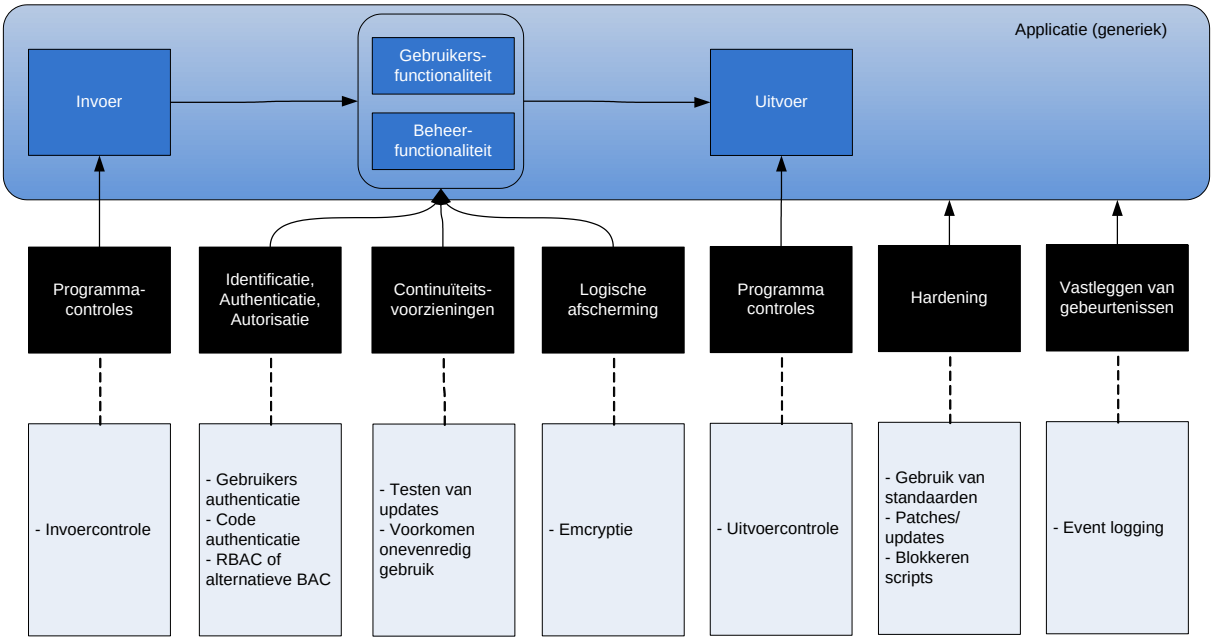
Figuur 11: Generieke applicatieconfiguratie

Figuur 11 schetst de elementen van een applicatie. De belangrijkste dreigingen voor applicaties (waar applicaties maatregelen tegen kunnen treffen) bestaan uit aanvallen vanaf de gebruikersinterface. Door de invoer te controleren op geldigheid wordt misbruik voorkomen (Programma-controles). Daar bovenop zorgt het afschermen van toegang tot de applicatie dat ongeautoriseerde gebruikers geen mogelijkheid hebben om de applicatie aan te vallen (IAA, Filtering). Het minimaliseren van de rechten van de applicatie zorgt er voor dat de schade beperkt blijft als er toch ongeautoriseerde toegang is verkregen Door handelingen van gebruikers te loggen is het mogelijk om na een incident te bepalen wie het incident heeft veroorzaakt (logging, alarmering, rapportering). Tot slot kan een dienst/applicatie maatregelen treffen om onevenredig gebruik door één gebruiker te voorkomen, wat de beschikbaarheid voor de andere gebruikers garandeert (Continuïteitsvoorzieningen).

Webapplicatie

Veel van de gedetecteerde aanvallen op internet zijn gericht op webapplicaties. Daarvan betreft een groot deel Cross-site scripting en SQL-injection aanvallen. Webapplicaties draaien vaak op servers in de DMZ, maar bedienen externe clients. Hiermee zijn ze onderdeel van de perimeter geworden en lopen ze een groter risico dan desktop applicaties. Er zijn dus extra beveiligingsmaatregelen nodig voor webapplicaties.

2.9.3 Oplossing



Figuur 12: Beveiligingsfuncties generieke applicatieconfiguratie

Figuur 12 schetst de IB-functies en mechanismen voor het patroon generieke applicatieconfiguratie. De configuratie van applicaties is gericht op:

- Betrouwbaarheid van informatie met betrekking tot de applicatie
- Beperken van het risico van aantasting van de betrouwbaarheid van werkplek en DWR netwerk

Het gebruik van *functiescheiding* beperkt het risico dat informatie binnen de applicatie kan worden gemanipuleerd. Verder dient ingevoerde informatie te worden gevalideerd om het risico te beperken dat een mogelijke kwetsbaarheid binnen de applicatie wordt misbruikt. Het risico dat een applicatie de betrouwbaarheid van de werkplek of het interne netwerk kan schaden wordt beperkt door alleen *geautoriseerde applicaties* toe te staan en applicaties voor productie uitvoerig te testen op eventuele beïnvloeding van de omgeving. Ook dient hiertoe *logging en loganalyse* plaats te vinden met betrekking tot gebruik en uitvoering van de applicatie.

2.9.4 Operationele maatregelen desktop en webapplicaties

Programma controles

1. Alle ingevoerde gegevens worden gecontroleerd op juistheid en geldigheid, zodat foutieve invoer tot een minimum wordt beperkt. Ongeldige invoer wordt niet geaccepteerd.

2. Indien dubbele invoer tot inconsistentie kan leiden (niet idempotente berichten) wordt er gecontroleerd op dubbele invoer van gegevens. Bij detectie wordt de gebruiker gewaarschuwd.
3. Een applicatie biedt geen mogelijkheid voor gebruikers tot het versturen van spamberichten.
4. Als bepaalde informatie op meerdere plaatsen wordt bijgehouden, wordt periodiek (interval bepaald in het SLA) gecontroleerd of de informatie consistent is.

Identificatie, authenticatie, autorisatie

5. Applicaties maken functiescheiding tussen bijv. beheerfuncties, lees- en schrijffuncties mogelijk.
6. De op de werkplek aangeboden applicaties hebben geen hoge of systeemrechten nodig om op de werkplek te functioneren. Deze kunnen dus met de standaard gebruikersrechten functioneren.
7. Applicaties maken gebruik van gebruikersauthenticatie om te voorkomen dat ongeautoriseerde personen toegang hebben tot de applicatie.
8. Wanneer een applicatie voor meerdere gebruikers toegankelijk is, moeten maatregelen worden getroffen om onevenredig gebruik door één gebruiker te voorkomen.

Continuïteitsvoorzieningen

9. Updates voor applicaties moeten eerst worden getest om te controleren of de juiste werking van de systemen niet wordt beïnvloed.

Logische afscherming

10. Voor encryptie moet een voldoende sterk algoritme worden gebruikt (zie bijlage 2).
11. Er worden standaard communicatieprotocollen gebruikt die geen afbreuk doen aan het gewenste beveiligingsniveau.
12. Cryptografische applicaties ondersteunen de minimale sleutellengte zoals bepaald in het SLA en beschreven in bijlage 2.

Hardening

13. Indien van toepassing ondersteunt een applicatie Code Signing (met een digitale handtekening) om te bepalen of scripts wel of niet uitgevoerd mogen worden.
14. Security updates worden toegepast binnen de periode genoemd in het SLA (zie bijlage 1).
15. Javascript, Word macro's en andere scripts worden in een sandbox uitgevoerd.
16. Alle applicaties draaien in user space volgens het least priviliges principe
17. Een virusscanner detecteert ongebruikelijk gedrag van applicaties

Vastleggen gebeurtenissen

18. Applicaties slaan loggegevens op van beveiligings-relevante informatie. Voorbeelden hiervan zijn: gelukte en mislukte login-pogingen, toegang tot data, poging tot uitvoeren van acties waar de gebruiker geen rechten voor heeft en software-crashes.

2.9.5 Operationele maatregelen webapplicaties

19. Foutmeldingen geven geen informatie over de werking van de applicatie.
20. Waar mogelijk worden prepared statements gebruikt voor queries.
21. Waar mogelijk wordt de zender van de data geverifieerd (whitelisting)
22. De user accounts en data van een applicatie staan in logisch gescheiden databases

2.9.6 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.9.4.1	12.2.1	Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.
2.9.4.2	12.2.1	Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.
2.9.4.3	12.2.1.1	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen en inconsistentie van gegevens.
2.9.4.4	12.2.1 .1	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen en inconsistentie van gegevens.
2.9.4.4	11.2.1.2	Authenticatiegegevens worden bijgehouden in één bronbestand) zodat consistentie is gegarandeerd.
2.9.4.5	10.1.3.2	Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerswerkzaamheden worden alleen uitgevoerd wanneer ingelogd als beheerder, normale gebruikstaken alleen wanneer ingelogd als gebruiker.
2.9.4.5	11.6.1.1	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
2.9.4.6	11.2.2	Opm.: Dit is impliciet aan de norm dat gebruikers geen administratierechten mogen hebben Zie TNK 11.2.2: De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.
2.9.4.7	11.2.1	Opm.: Impliciet aan 11.2.1: *Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.*
2.9.4.7	11.6.1	Opm.: Impliciet aan 11.6.1: *Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.*
2.9.4.8	geen	
2.9.4.9	12.6.1.2	Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
2.9.4.9	12.6.1.3	Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
2.9.4.10	12.3.1.1	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
2.9.4.10	12.3.1.3	De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
2.9.4.11	geen	Opm.: ICT best practice

Operationele norm	TNK referentie	TNK norm
2.9.4.12	geen	
2.9.4.13	geen	
2.9.4.14	12.6.1.4	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde
2.9.4.15	10.4.2.1	Mobile code wordt uitgevoerd in een logisch geïsoleerde omgeving (sandbox) om de kans op aantasting van de integriteit van het systeem te verkleinen. De mobile code wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt.
2.9.4.16	11.2.2.3	Gebruikers krijgen slechts toegang tot een noodzakelijk geachte set van applicaties en commando's.
2.9.4.17	10.4.1.1	Bij het openen van bestanden worden deze geautomatiseerd gecontroleerd op virussen, trojans en andere malware. De update voor de detectiedefinities vindt frequent, minimaal één keer per dag, automatisch plaats.
2.9.4.17	10.10.2.1	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore • gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases) • handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels • ***beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities***, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services) • verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen) • handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.

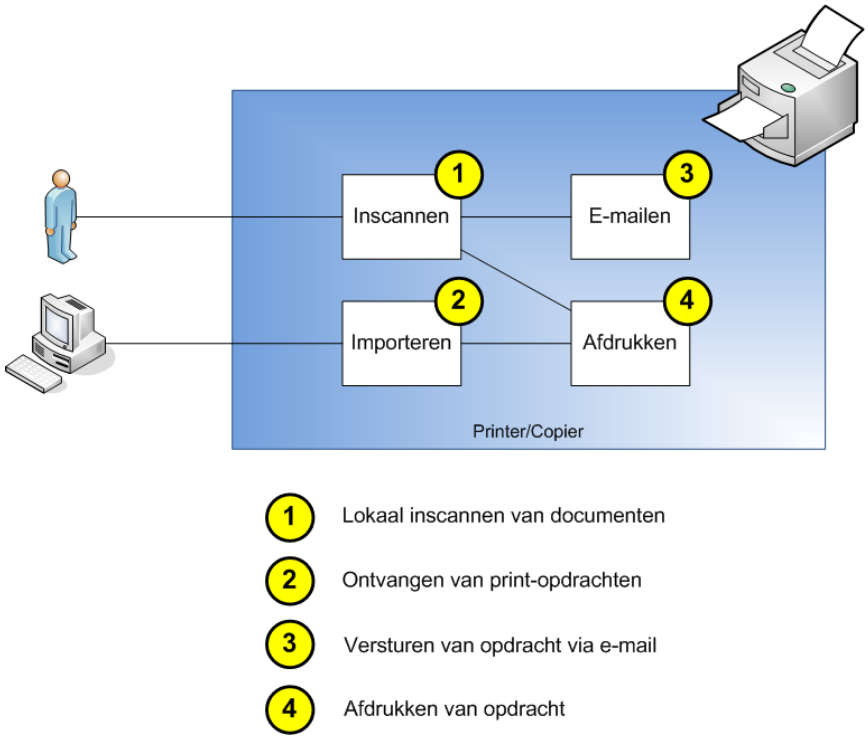
Operationele norm	TNK referentie	TNK norm
2.9.4.18	10.10.2.1	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore • gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases) • handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels • beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services) • verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen) handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.
2.9.4.19	geen	
2.9.4.20	12.2.1.1	Opm.: nadere precisering van TNK 12.2.1.1 12.2.1.1: Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen en inconsistentie van gegevens.
2.9.4.21	geen	
2.9.4.22	geen	

2.10 Patroon multifunctional configuratie

2.10.1 Rationale

Op multifunctionals zoals printers kan gevoelige informatie worden afgedrukt. Het is van belang dat de multifunctionals goed beveiligd zijn. De beveiliging is een interdepartementale aangelegenheid, omdat ook andere departementen gebruik kunnen maken van een multifunctional, bijvoorbeeld als een medewerker bij een ander departement aanwezig is

2.10.2 Context



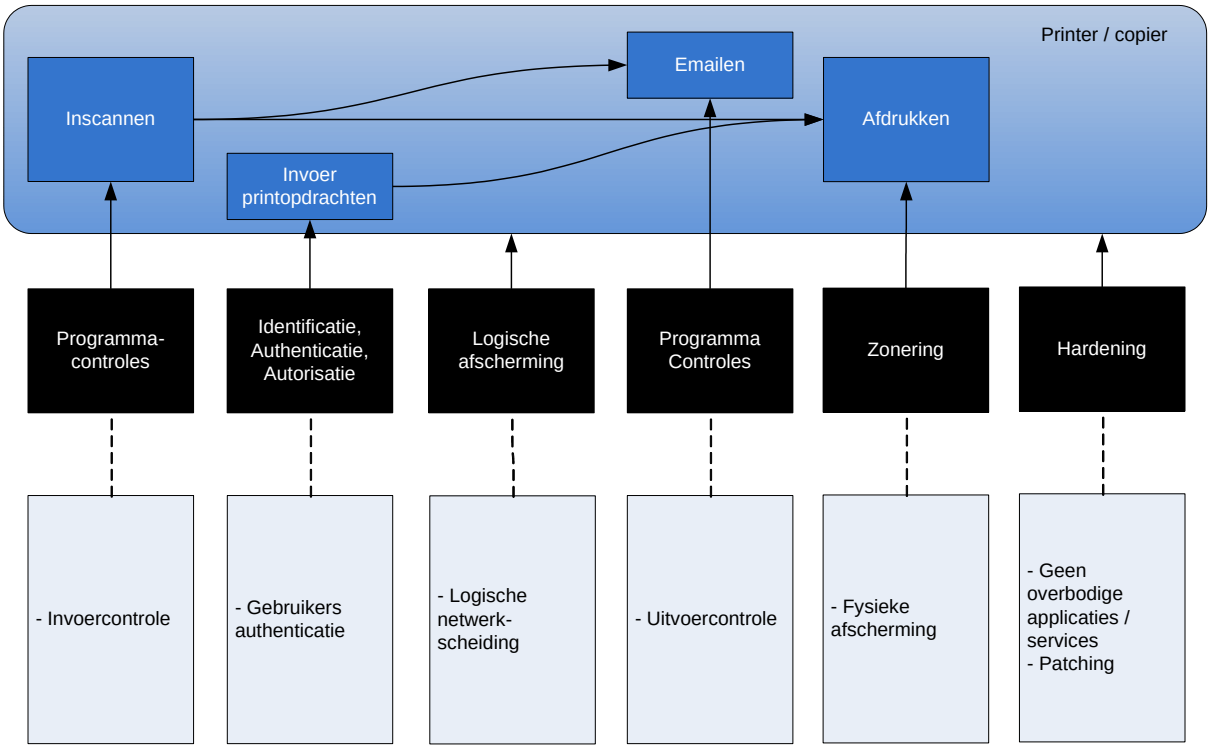
Figuur 13: Multifunctional configuratie

Figuur 13 schetst de situatie rond multifunctionals in een netwerk. De functionaliteit van een printer is hierbij verbreed naar die van een multi-functional copier: naast het afdrukken biedt de printer ook de mogelijkheid tot inscannen van documenten en emailen van ingescande documenten.

Multifunctionals hebben in principe drie verschillende toegangsmogelijkheden; fysieke toegang, toegang tot de beheersinterface en toegang tot de print functionaliteit. By fysieke toegang is het belangrijk dat niet iedereen bij de printer kan komen, dit kan worden opgelost door printers in afgeschermde ruimtes te plaatsen (Zonering, Filtering). Zo wordt tot op zekere hoogte voorkomen dat afdrukken door onbevoegden worden meegenomen. Via het netwerk is de multifunctional ook te benaderen voor het versturen van print opdrachten. Hierbij moet worden vastgelegd welke persoon welke print opdracht heeft verstuurd, zodat het annuleren van print opdrachten mogelijk is (IAA). Voor beheer mogen alleen geautoriseerde personen de instellingen van de printer kunnen wijzigen (IAA). Niet alle netwerkelementen hebben toegang tot de multifunctionals nodig, en moeten daarom worden afgeschermd (Zonering, Filtering). De status van de multifunctional moet worden vastgelegd en gerapporteerd (Controle,

alarmering, rapportering). Het reageren op deze meldingen, en maatregelen zoals het toepassen van meerdere papierbakken zorgen voor een hogere beschikbaarheid (Continuïteitsvoorzieningen).

2.10.3 Oplossing



Figuur 14: Beveiligingsfuncties multifunctional configuratie

Figuur 14 schetst de IB-functies en mechanismen voor het patroon multifunctional configuratie. Multifunctionals zijn volwaardige systemen die mogelijk gebruikt kunnen worden voor een aanval richting het netwerk. Daarom dienen multifunctionals ontdaan te worden van niet noodzakelijke functionaliteit (*hardening*) en dient de toegang tot de multifunctional zowel logisch als fysiek zo veel mogelijk beperkt te worden (*afscherming*, *autorisatie*) om de *integriteit* van de multifunctional te waarborgen.

2.10.4 Operationele maatregelen

Identificatie, authenticatie, autorisatie

1. Alleen geautoriseerde gebruikers kunnen gebruik maken van de multifunctionals.
2. Gebruikers moet de mogelijkheid hebben om beveiligd te printen.
3. Op de beheersinterface van de multifunctional zijn toegangsrestricties aangebracht zodanig dat alleen geautoriseerde personen de beheersinstellingen kunnen wijzigen.

Logische afscherming

4. Alle netwerk multifunctionals worden logisch afgeschermd van de werkstations.
5. Netwerk multifunctionals worden logisch afgeschermd van systemen waarmee geen communicatie nodig is.

6. Indien de multifunctional opslagmedia bevat worden deze op veilige wijze gewist of vernietigd voordat de multifunctional afgevoerd wordt.

Zonering

7. Fysieke toegang tot de multifunctionals is niet mogelijk vanuit publieke ruimtes.
8. Er worden geen vertrouwde netwerken met onvertrouwde netwerken worden gekoppeld via de op de multifunctional aangesloten apparatuur (bijvoorbeeld fax).

Hardening

9. Multifunctionals bieden uitsluitend noodzakelijke functionaliteiten en protocollen.
10. Security updates worden toegepast binnen de periode genoemd in het SLA (zie bijlage 1).

Interoperabiliteit/beheer

11. Meldingen over de status van de multifunctional worden doorgestuurd naar beheer.

2.10.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.10.4.1	12.2.4.3	Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need to know).
2.10.4.2	12.2.4.3	Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need to know).
2.10.4.3	12.2.4.3	Alleen gegevens die noodzakelijk zijn voor de doeleinden van de gebruiker worden uitgevoerd (need to know).
2.10.4.4	11.4.5.3	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
2.10.4.5	11.4.5.3	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
2.10.4.6	9.2.6.1	Bij beëindiging van het gebruik of bij een defect worden apparaten en informatiedragers bij de beheersorganisatie ingeleverd. De beheerorganisatie zorgt voor een verantwoorde afvoer zodat er geen data op het apparaat aanwezig of toegankelijk is. Als dit niet kan wordt het apparaat of de informatiedrager fysiek vernietigd. Het afvoeren of vernietigen wordt per bedrijfseenheid geregistreerd.
2.10.4.7	9.1.1	Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.
2.10.4.8	11.4.5	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
2.10.4.9	geen	
2.10.4.10	12.6.1.4	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde

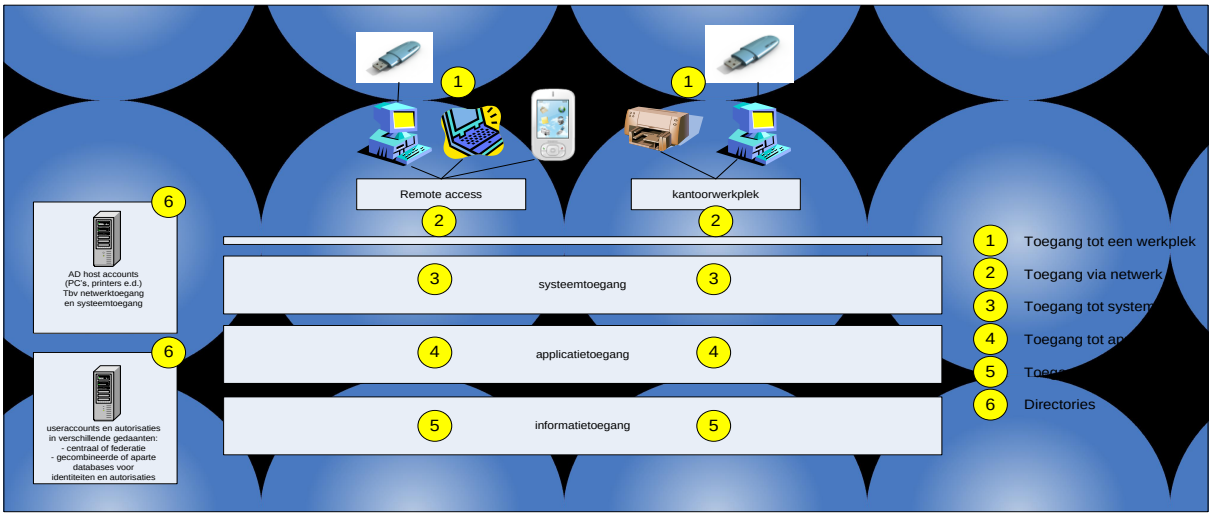
Operationele norm	TNK referentie	TNK norm
2.10.4.11	10.10.2.1	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore • gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases) • handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels • beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services) verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen) handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.

2.11 Patroon identificatie, authenticatie en autorisatie

2.11.1 Rationale

Toegang tot de verschillende objecten dient te worden gelimiteerd tot alleen geautoriseerd personeel, om zo de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen.

2.11.2 Context

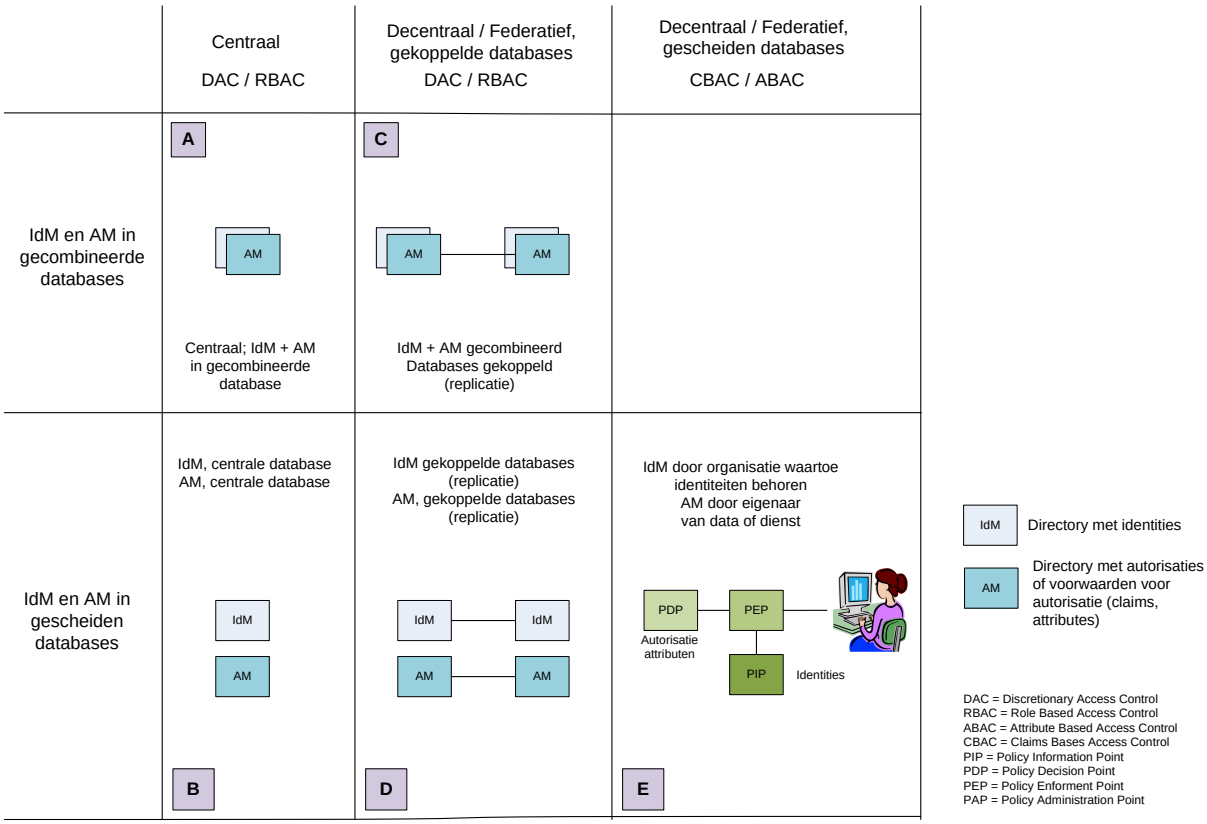


Figuur 15: Identificatie, authenticatie en autorisatie

Authenticatie en autorisatie hebben betrekking op objecten van alle niveaus (zie de situatieschets in figuur 15) zoals gebruikers, beheerders, werkplekken en servers. Authenticatie is het controleren of de identiteit die een object/persoon claimt te hebben ook klopt. Autorisaties zijn de rechten die aan die identiteit gekoppeld zijn. De beveiligingsfunctie die hiermee wordt gerealiseerd is die van Identificatie, Authenticatie, Autorisatie.

Authenticatie en autorisatie komen in verschillende vormen voor (zie figuur 16):

A. Identificatie/authenticatie gekoppeld met autorisatie in dezelfde centrale database (bijvoorbeeld Active Directory)
B. Identificatie/authenticatie gescheiden van autorisatie (bijvoorbeeld AD voor authenticatie en autorisatie in de applicatie zelf) met een centrale database voor identificatie en een aparte (centrale) database voor autorisatie.
C. Federatieve IAM (Identity en Access Management) met gekoppelde databases (replicatie van gegevens) die gebruikt worden voor identificatie en voor autorisatie.
D. Federatieve IAM met gekoppelde databases (replicatie van gegevens) waarbij er aparte databases voor identificatie en voor autorisatie zijn.
E. Federatieve IAM met gescheiden verantwoordelijkheden voor Identificatie/authenticatie en voor autorisatie. Authenticatie is de verantwoordelijkheid van organisatie van de identiteit en autorisatie wordt bepaald door eigenaar van de applicatie of de informatie.

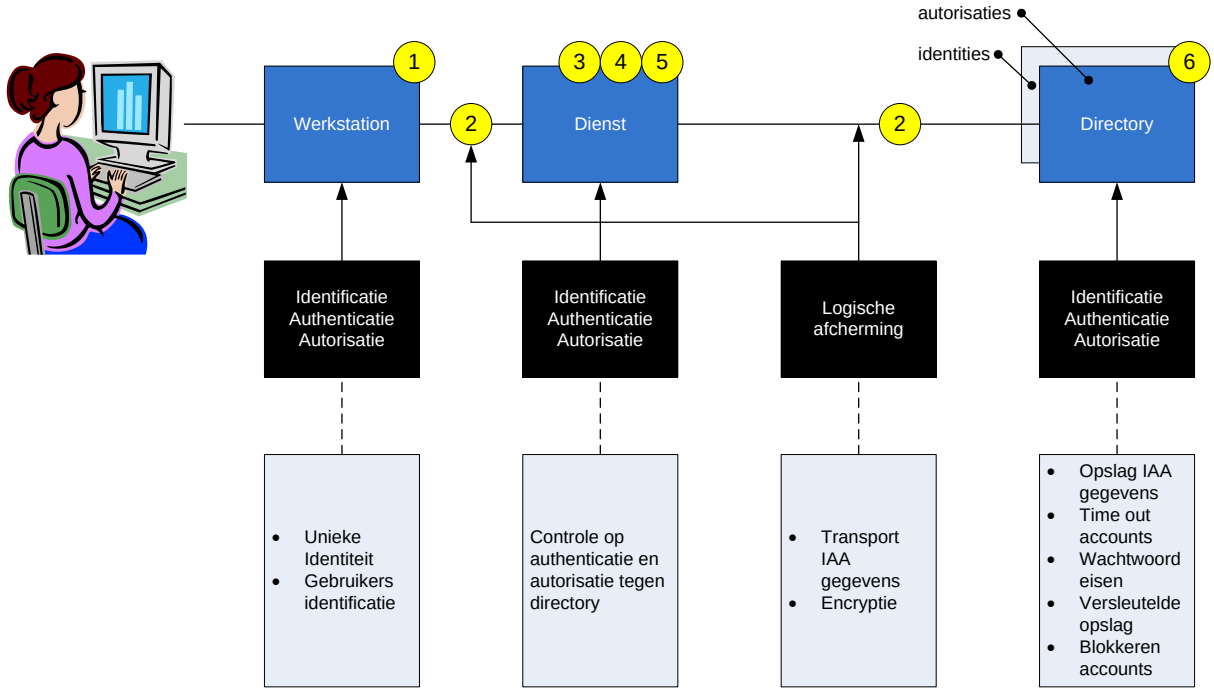


Figuur 16: Vormen van authenticatie en autorisatie

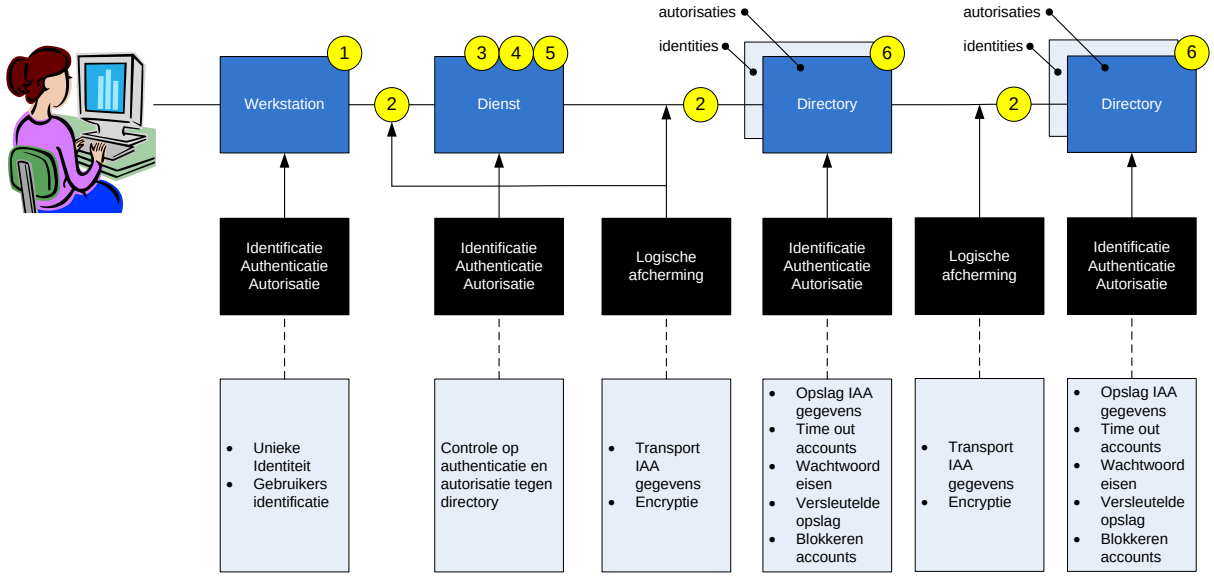
Voor de situaties A t/m D zijn de volgende access methoden gangbaar: DAC (Discretionary Access Control) en RBAC (Role Based Access Control). Voor situatie E is CBAC (Claims Based Access Control) ofwel ABAC (Attribute Based Access Control) van toepassing.

De bijbehorend patronen zijn in de figuren 17, 18 en 19 aangegeven. De situaties A en B zijn in één patroon samengevoegd (figuur 18). Dat geldt ook voor de situaties C en D (figuur 19).

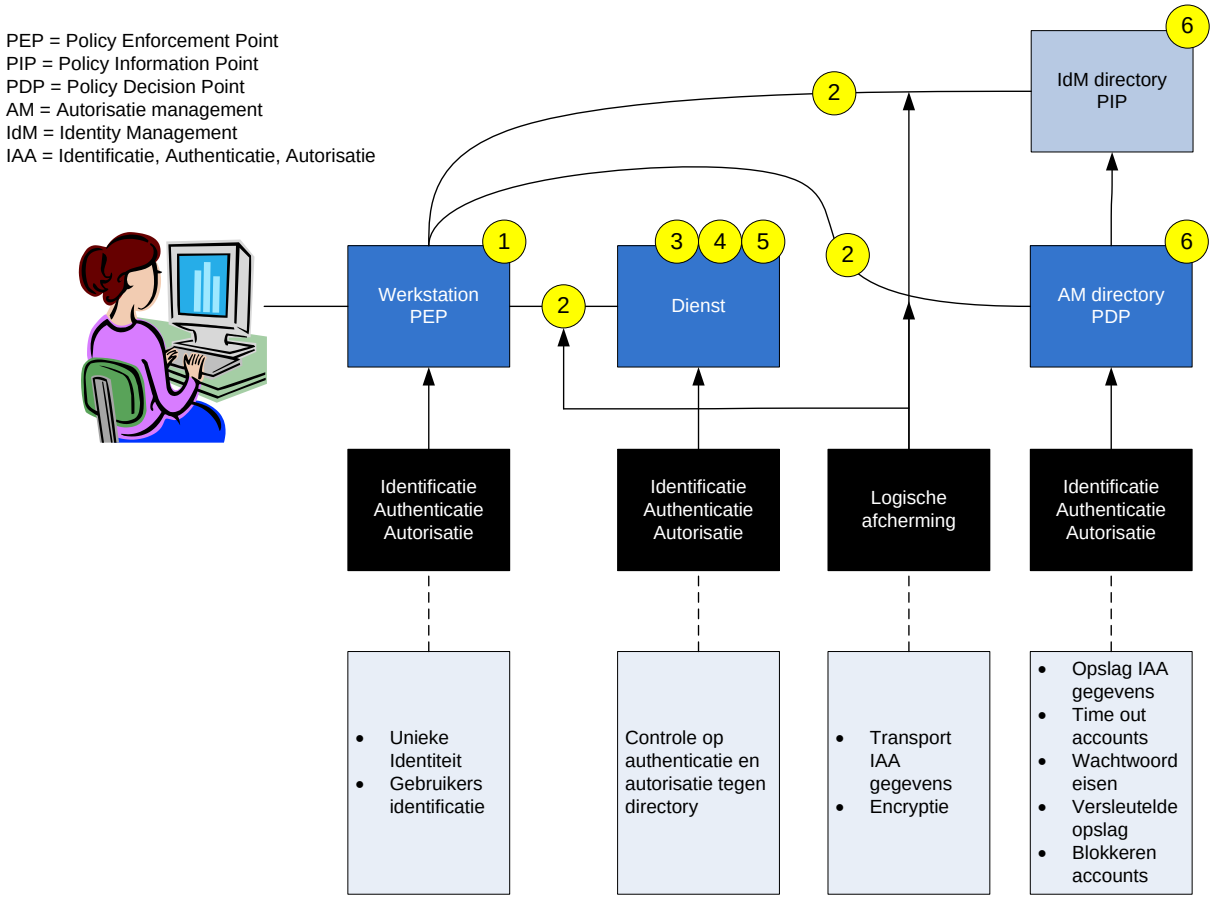
2.11.3 Oplossing



Figuur 17: DAC of RBAC (Centraal)



Figuur 18: DAC of RBAC (decentraal)



Figuur 19: CBAC of ABAC

De minimale vorm van authenticatie is die op basis van *gebruikersnaam* en *wachtwoord*. Het authenticatie mechanisme op basis van wachtwoord is kwetsbaar omdat een aanvaller wachtwoorden ongemerkt zou kunnen afluisteren of raden. Om te voorkomen dat een buitenstaander inzage heeft in het wachtwoord van een gebruiker mag een wachtwoord nooit in klare tekst worden opgeslagen of getransporteerd. Het risico van raden van een wachtwoord wordt beperkt door het aantal mogelijke inlogpogingen te beperken in tijd en in aantal. Bij voorkeur heeft het wachtwoord een zekere moeilijkheidsgraad, maar het afdwingen hiervan maakt het aantal mogelijke wachtwoorden alleen maar kleiner. Wachtwoorden dienen regelmatig te worden gewijzigd. Indien er meer zekerheid ten aanzien van de identiteit van een gebruiker is vereist (bijvoorbeeld bij authenticatie op afstand of ten behoeve van beheertaken) dient *sterke authenticatie* (twee factor) te worden gebruikt waarbij naast kennis van een wachtwoord of PIN ook het bezit van smartcard of token nodig is voor authenticatie.
Vaak wordt authenticatie gerealiseerd volgens een PKI (Public Key Infrastructure) gerealiseerd. Zie het betreffende patroon voor PKI.

2.11.4 Operationele maatregelen

Identificatie, authenticatie, autorisatie

1. Elke identiteit (persoon of object, b.v. een server) heeft een unieke gebruikersnaam/identifier.
2. De systeemprocessen draaien onder een eigen account.

3. Het is mogelijk om de rechten per identiteit of per rol te specificeren (Discretionary access control of role based access control) of de criteria waaraan de identiteit moet voldoen om toegang tot de applicatie te krijgen (attribute based access control of claims based access control).
4. Er is inzichtelijk vastgelegd welke identiteiten en rollen een bepaald recht hebben of welke attributen recht geven op toegang.
5. Gebruikers moeten zich minimaal op basis van gebruikersnaam en wachtwoord authenticeren.
6. Beheerders hebben een persoonsgebonden beheeraccount.
7. Systeem- en netwerkbeheer en functioneel beheer accounts worden altijd geauthenticeerd door middel van 2-factor authenticatie.
8. Voor alle accounts moet een screensaver met wachtwoord worden ingeschakeld na een periode van inactiviteit zoals bepaald in het SLA (zie bijlage 1).
9. Wachtwoorden worden eenzijdig vercijferd opgeslagen volgens een algoritme bepaald in het SLA en beschreven in bijlage 2.
10. accounts die een periode bepaald in het SLA niet worden gebruikt worden onderzocht om te bepalen of het account verwijderd kan worden.
11. De expiratiedatum van een account is gekoppeld aan de uitdiensttreding van een medewerker.
12. Een wachtwoord is maximaal geldig gedurende de periode bepaald in het SLA en dient binnen die tijd te worden aangepast waarna opnieuw de genoemde termijn ingaat.
13. Na expiratie moet een account automatisch geblokkeerd worden, waarbij via vastgelegde procedures het account eventueel weer ontsloten kan worden.
14. Standaard wachtwoorden worden tijdens of direct na de installatie gewijzigd.
15. Initiële wachtwoorden moeten bij het eerste gebruik door de gebruiker worden gewijzigd.
16. Initiële wachtwoorden zijn maximaal geldig gedurende de periode genoemd in het SLA, na deze periode wordt het account automatisch geblokkeerd.
17. Initiële wachtwoorden voldoen aan de standaard normen (zie bijlage 1) en mogen eenmalig, uniek per gebruiker, gebruikt worden.
18. Wanneer een inlogingpoging meerdere keren (zie bijlage 1 voor maximum) mislukt, wordt het account tijdelijk (zie bijlage 1 voor minimum) geblokkeerd. Betreft het een beheeraccount, dan wordt dat account geblokkeerd en pas na verificatie van rechtmatigheid handmatig gereset.
19. Een wachtwoord mag niet getoond worden.
20. Bij het login scherm wordt een melding getoond waarin genoemd wordt dat ongeautoriseerd inloggen en misbruik strafbaar is.
21. Na inloggen wordt een melding met de laatste succesvolle login en bijbehorende datum en tijd getoond.
22. Het tonen van het laatst ingelogde account is niet toegestaan.
23. Automatisch onder een gebruikersaccount inloggen na het opstarten is niet toegestaan. (Single sign on is wel mogelijk, deze eis geldt alleen voor initiële werkplekauthenticatie)
24. Het BIOS/Firmware is door middel van een wachtwoord afgeschermd voor inzage en wijzigingen. Alleen werkplekbeheerders bezitten de BIOS/Firmware wachtwoorden.
25. Authenticatie is altijd herleidbaar tot één persoon. Indien groepsaccounts nodig zijn worden aanvullende maatregelen genomen om herleidbaarheid tot één persoon te garanderen.
26. Bij werken op afstand is 2-factor authenticatie vereist, in combinatie met een veilige toegangsmethode zoals genoemd in bijlage 2.
27. Voor autorisaties wordt zoveel mogelijk gebruik gemaakt van standaard autorisatievoorzieningen.
28. Een identiteit mag alleen de rechten bezitten die nodig zijn voor het uitvoeren van een bepaalde taak. Voorbeelden zijn lees- en schrijfrechten, toegangsrechten.

Logische afscherming

29. Wachtwoorden, en bij voorkeur ook gebruikersnamen, worden altijd vercijferd verzonden.
30. Er wordt gebruik gemaakt van standaard vercijfer algoritmen voor wachtwoorden zoals beschreven in bijlage 2.

2.11.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.11.4.1	11.2.1.1	Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
2.11.4.2	11.2.2.2	Systeemprocessen draaien onder een eigen gebruikersnaam (een functioneel account), voor zover deze processen handelingen verrichten voor andere systemen of gebruikers.
2.11.4.3	11.2.2.1	Gebruikers hebben toegang tot speciale bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is (need to know, need to use).
2.11.4.4	11.2.1.2	Authenticatiegegevens worden bijgehouden in één bronbestand) zodat consistentie is gegarandeerd.
2.11.4.5	11.2.1.1	Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden. Opm.: dit geeft nog niet aan dat het minimaal met een gebruikersnaam en wachtwoord moet.
2.11.4.6	11.2.2.1	Precisering van TNK 11.2.2.1: 11.2.2.1: Gebruikers hebben toegang tot speciale bevoegdheden voor zover dat voor de uitoefening van hun taak noodzakelijk is (need to know, need to use).
2.11.4.7	11.5.1.1	Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van two-factor authenticatie.
2.11.4.8	11.3.3.3	Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van inactiviteit van maximaal 15 minuten alle informatie op het beeldscherm onleesbaar en ontoegankelijk.
2.11.4.9	11.2.3.1	Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt bijvoorbeeld de hashwaarde van het wachtwoord opgeslagen.
2.11.4.10	11.5.3.2	Wachtwoorden hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
2.11.4.11	11.5.3.2	Wachtwoorden hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
2.11.4.12	11.5.3.2	Wachtwoorden hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
2.11.4.13	11.5.3.2	Wachtwoorden hebben een geldigheidsduur van maximaal 3 maanden. Daarbinnen dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
2.11.4.14	11.5.3.3	Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.

Operationele norm	TNK referentie	TNK norm
2.11.4.15	11.5.3.3	Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.
2.11.4.16	11.5.3.3	Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een zeer beperkte geldigheidsduur en moeten bij het eerste gebruik worden gewijzigd.
2.11.4.17	geen	Opm.: precisering van TNK 11.5.3.3
2.11.4.18	11.5.1.5	Nadat voor een gebruikersnaam 5 keer een foutief wachtwoord gegeven is, wordt het account minimaal 10 minuten geblokkeerd. Indien er geen lockout periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker verzoekt deze lockout op te heffen of het wachtwoord te resetten.
2.11.4.19	11.5.1.2	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
2.11.4.20	11.5.1.3	Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
2.11.4.21	11.5.1.4	Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
2.11.4.22	geen	Opm.: dit is een precisering van TNK 11.5.1.4
2.11.4.23	11.3.1.1	Aan de gebruikers is een set gedragsregels aangereikt met daarin minimaal het volgende: • Wachtwoorden worden niet opgeschreven. • Gebruikers delen hun wachtwoord nooit met anderen. • Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde. • ***Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).***
2.11.4.24	geen	
2.11.4.25	10.10.1.2	Een logregel bevat minimaal: • ***een tot een natuurlijk persoon herleidbare gebruikersnaam of ID*** • de gebeurtenis (zie 10.10.2.1) • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis
2.11.4.26	11.6.1.3	Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
2.11.4.27	11.4.2	Opm.: dit is een precisering van TNK 11.4.2 11.4.2: Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.

Operationele norm	TNK referentie	TNK norm
2.11.4.28	11.6.1.1	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
2.11.4.29	11.2.3.1	Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt bijvoorbeeld de hashwaarde van het wachtwoord opgeslagen.
2.11.4.30	geen	Opm.: dit is een nadere precisering van TNK 11.2.3.1

2.12 Public Key Infrastructure (PKI)

2.12.1 Rationale

Communicatie tussen zender en ontvanger (persoon of object) vindt veelal plaats over elektronische netwerken, waarvan de vertrouwelijkheid niet altijd gegarandeerd is. De gebruikers rekenen op een betrouwbare, getrouwe en vertrouwelijke elektronische berichtuitwisseling waarbij de afzender met zekerheid bekend is en het bericht terecht komt bij de goede geadresseerde.

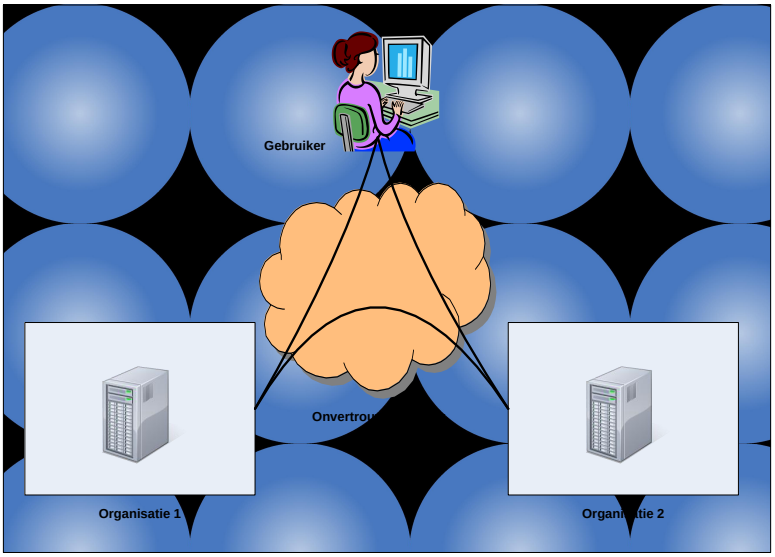
De belangrijkste problemen die voor een betrouwbare elektronische communicatie opgelost moeten worden zijn:

- **Identiteit:** Hoe kun je vaststellen met wie je communiceert en hoe weet de ontvanger zeker dat jij de verzender bent en niet iemand anders?
- **Vertrouwelijkheid**: Hoe zorg je ervoor, dat de inhoud onleesbaar is voor derden?
- **Integriteit**: Hoe kunnen wijzigingen van gegevens tijdens transport worden opgemerkt?
- **Onweerlegbaarheid:** Waarmee wordt voorkomen dat een ontvangen bericht wordt ontkend?
- **Sleuteldistributie en beheer**: Bij grote aantallen gebruikers van symmetrische[7] versleuteling neemt de beheerlast exponentieel toe. Een dilemma bij encryptie is tevens dat er eerst geheime sleutels uitgewisseld moeten worden voordat 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?

2.12.2 Context

Figuur 20 schetst de situatie waarin bedrijven en personen met elkaar via een onvertrouwd netwerk willen communiceren. Daarbij gelden de vereisten van identiteitsvaststelling, vertrouwelijkheid, integriteit, en onweerlegbaarheid.

[7] Symmetrische encryptie werkt met één geheime sleutel die zowel bij de zender als de ontvanger bekend moet zijn.

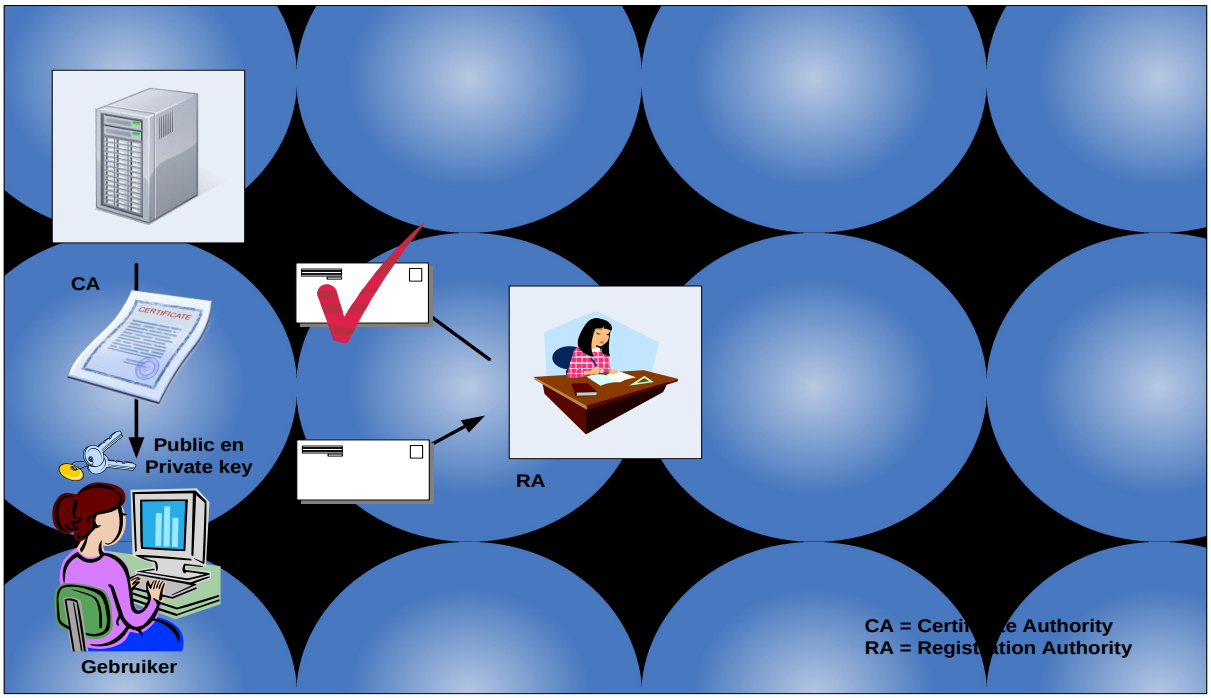


Figuur 20: communicatie via onvertrouwde netwerken waarbij authenticatie, vertrouwelijkheid, integriteit van gegevens en onweerlegbaarheid vereist is.

2.12.3 Oplossing

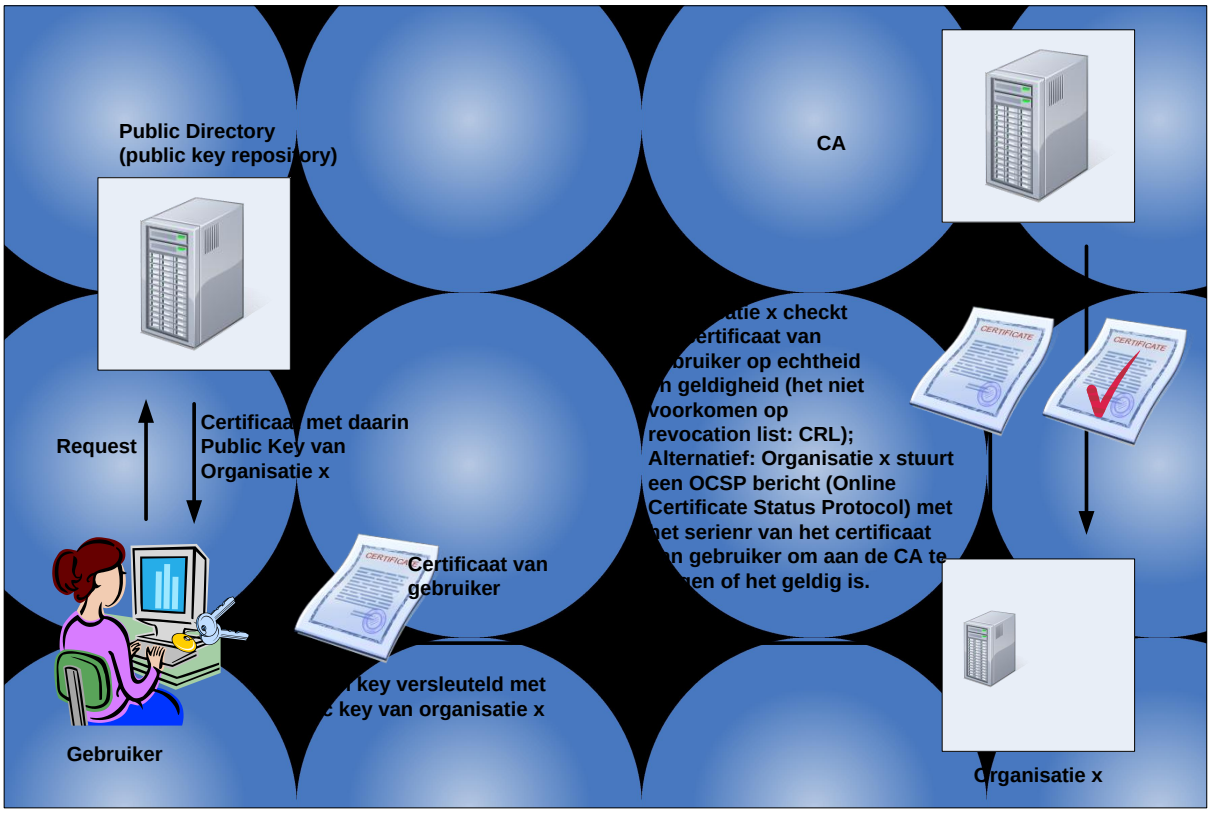
Een Public Key Infrastructure (PKI) is een set van technische en organisatorische voorzieningen, die een oplossing biedt voor bovengenoemde probleemstelling. De basis van een PKI is asymmetrische versleuteling en elektronische certificaten.
Om publieke sleutels voor een ieder toegankelijk en vindbaar te maken op het internet, zijn er 'public key repositories' 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 gebruik van certificaten. Van hetzelfde sleutelpaar wordt nu de publieke sleutel opgenomen in een zogeheten PKI-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 onvertrouwd netwerk.
Certificaten worden door een (derde) vertrouwde partij uitgegeven; een CA (Certificate Authority) op gezag van een RA (Registration Authority). De CA garandeert de echtheid en de oorsprong van de certificaten. Certificaten kunnen in allerlei vormen worden uitgegeven. De bijbehorende private sleutels moeten beschermd zijn tegen kopiëren en worden bij voorkeur uitgegeven / opgeslagen op afzonderlijk te beveiligen objecten als smartcards, usb-tokens, en HSM's (Hardware Security Module.)

De uitgifte van een certificaat is in figuur 21 weergegeven.



Figuur 21: Certificaatuitgifte.

Figuur 21 schetst het uitgifteproces. Een gebruiker vraagt een certificaat aan bij de Registration Authority (RA), die opdracht verstrekt aan de Certificate Authority (CA). De CA zendt (via een veilige weg) een certificaat naar de gebruiker. Er bestaan meerdere RA's en CA's. De CA's wisselen onderling de certificaten uit.



Figuur 22: Certificaatgebruik

In figuur 22 is een voorbeeld gegeven van veilige communicatie tussen een persoon (gebruiker) en organisatie x met behulp van certificaten. Een gebruiker, die veilig wil communiceren met een organisatie x, zendt zijn certificaat, gelijktijdig met de session key, versleuteld met de public key van organisatie x, naar organisatie x. Organisatie x, verifieert het certificaat bij zijn CA, die kan bevestigen dat of certificaat echt is. Na die bevestiging kunnen de gebruiker en organisatie x veilig communiceren: vertrouwelijk door versleuteling met de session key, geauthenticeerd door het certificaat en verificatie daarvan, data-integer doortoevoeging van een hashcode en onweerlegbaar doordat het bericht is versleuteld met de publieke sleutels van de gebruiker en organisatie x. De CA's garanderen dat die publieke sleutels echt horen bij de eigenaar (gebruiker en organisatie x).Het gebruik van certificaten is ruimer dan dit voorbeeld. Er kan op deze manier ook gecommuniceerd worden tussen organisaties (waaronder machine-machine communicatie).

Een PKI infrastructuur bestaat uit verschillende componenten en taken. De belangrijkste zijn:

- Een certificaatautoriteit (of *Certificate Authority*, CA) — beheert de certificaten.
- Een registratieautoriteit (of *Registration Authority*, RA) — stelt vast aan wie een certificaat kan worden verstrekt en controleert de uitgifte ervan.
- Een lijst met ingetrokken en vervallen certificaten; de Certificate Revocation List of CRL
- De algemene (verkoop)voorwaarden van de PKI; het Certificate Practice Statement of CPS.

- Een of meer CSP's (Certificate Service Provider) die als taak hebben het verstrekken en beheren van certificaten en sleutelinformatie. Een CSP levert dus CA diensten.

PKI Overheid

PKI Overheid is de Public Key Infrastructure van de Nederlandse overheid. Net als elke andere PKI is het een systeem waarmee uitgifte en beheer van digitale certificaten kan worden gerealiseerd. PKI Overheid wordt beheerd door Logius.

Het verschil met commerciele versies is dat de technisch hoogste autoriteit (root CA) de overheid is. De Nederlandse overheid is verantwoordelijk voor het stamcertificaat op de root CA, waardoor PKI Overheid niet afhankelijk is van (buitenlandse) commerciële partijen. PKI Overheid is een stelsel van voorwaarden voor het uitgeven van certificaten. Commerciële CA's (Certificate Services Providers genoemd) kunnen aansluiten bij PKI Overheid. De CA van deze CSP wordt dan opgenomen in de hierarchie van PKI Overheid. PKI Overheid geeft zelf geen eindgebruikerscertificaten uit, alleen certificaten aan de CSP's. PKI Overheid stelt voorwaarden voor uitgifte van certificaten. Deze zijn overeenkomstig aan de voorwaarden voor gekwalificeerde certificaten. Eén van die voorwaarden is dat de aanvrager zich moet melden en identificeren bij bijvoorbeeld een notaris. Deze voorwaarden gelden niet alleen voor de persoonsgebonden certificaten, maar ook voor de certificaten op organisatie niveau. PKI Overheid streeft naar één hoog betrouwbaarheidsniveau voor alle certificaattypen.

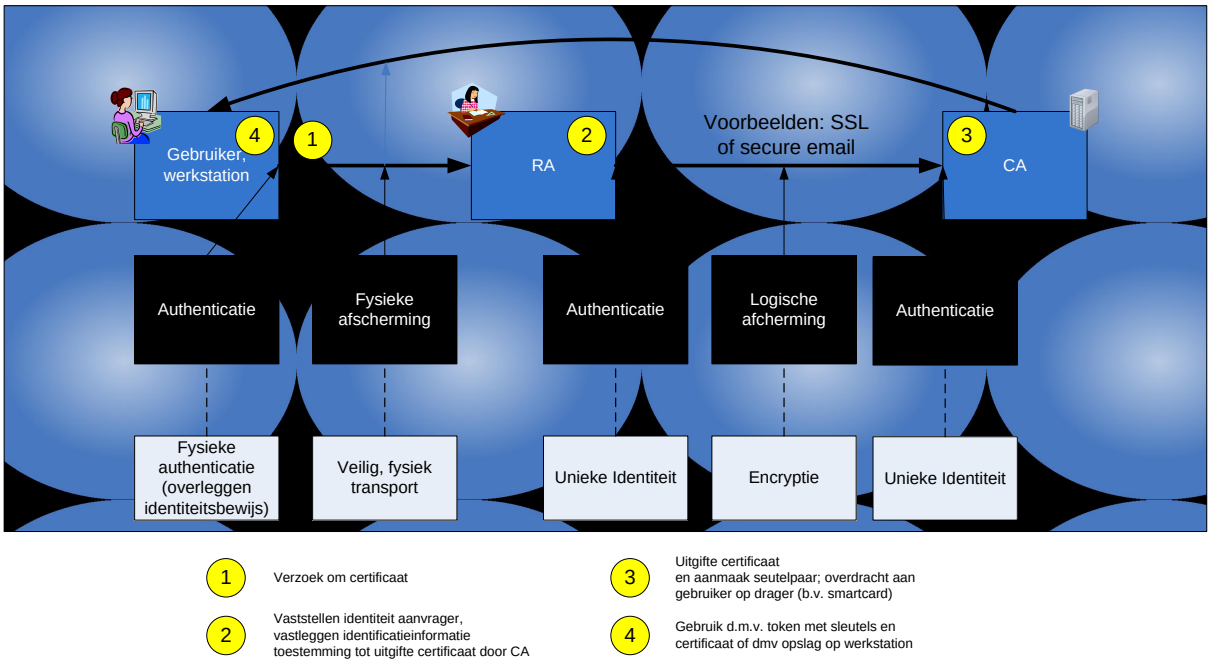
PKI Overheid stelt onder de Staat der Nederlanden de volgende Certificatenhiërarchie beschikbaar:

1. Programma van eisen van PKI Overheid
2. Uitgevers van certificaten
3. Gekwalificeerde elektronische handtekening
4. Uitgifte van certificaten

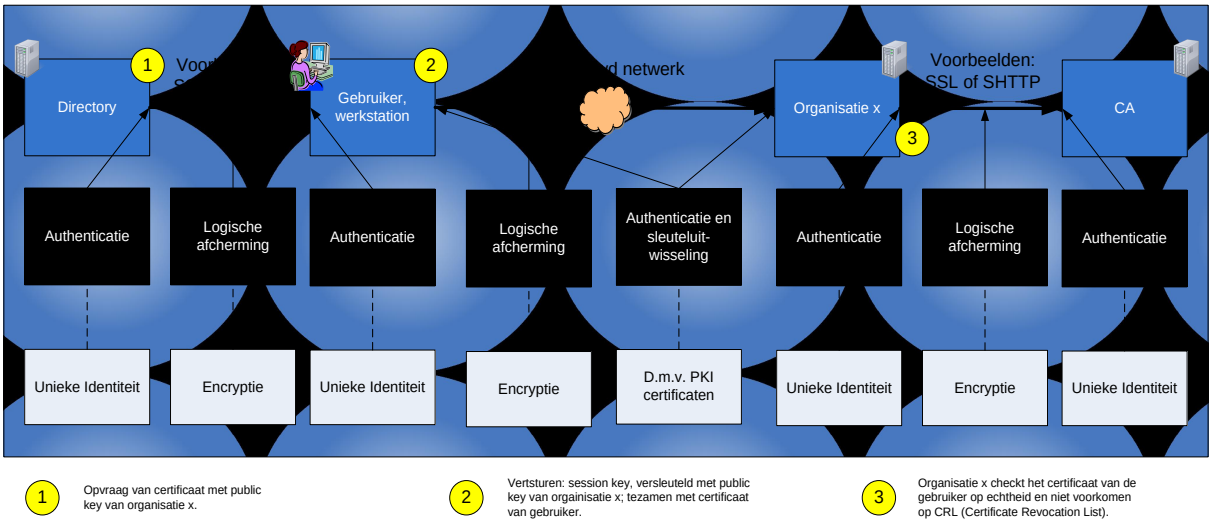
Zie voor nadere informatie: **www.pkioverheid.nl**

Architectuurpatroon

De IB functies van het patroon PKI zijn gegeven in de figuren 23 en 24.



Figuur 23: Certificaatuitgifte



Figuur 24: Certificaatgebruik en vertrouwde communicatie

2.12.4 Operationele Maatregelen

Zonering

1. Bij gebruik van PKI communicatie door een gebruiker op een werkstation, dienen de geheime sleutels veilig te worden bewaard op een apart beveiligd medium (usb-token, smart card o.i.d.). Niet op het werkstation van een gebruiker.

2. Bij computer-computercommunicatie dienen de geheime sleutels op de communicerende machines te worden bewaard maar dan moeten aantoonbare voldoende fysieke en logische beveiligingsmaatregelen zijn toegepast.

Logische afscherming

3. Certificaten moeten voorzien zijn van een voldoend sterke hash zoals beschreven in bijlage 2.

Identificatie, authenticatie, autorisatie

4. Bij gebruik van PKI door een menselijke gebruiker (b.v. voor telewerken) is 2-factor authenticatie vereist: username/password of pincode in combinatie met een token met de geheime sleutel (b.v. smartcard).
5. Tokens dienen te voldoen aan de eisen van PKI Overheid.

Interoperabiliteit/beheer

6. Certificaten dienen te voldoen aan de eisen in bijlage 1.
7. Voor alle gegevensdragers geldt dat:
    - een betrouwbare registratie moet worden gevoerd
    - gebruik en toegang plaats vind op basis van need to know
    - afvoer en schoning gebeurt volgens de geldende richtlijnen (VIR-BI)
8. Personeel dat in aanraking komt met sleutels en tokens van een CA dient in het bezit van een geldige verklaring van geen bezwaar (zoals bedoeld in de wet veiligheidsonderzoeken) te zijn.
9. Publieke sleutels worden direct na uitgifte (binnen 60 seconden) door een CA verspreid naar andere CA's en Public Key Directories.
10. Het intrekken van certificaten gebeurt uitsluitend op aanvraag van een geautoriseerde RA medewerker of op aanvraag van de gebruiker of functioneel beheerder.

Continuïteitsvoorzieningen / filtering

11. De beveiligingsmiddelen die worden ingezet voor de toegangsbeveiliging (o.a. sleutels, codes, biometrie en smartcards) dienen:
    - vrij te zijn van bekende zwaktes dan wel dienen er aanvullende maatregelen te worden getroffen zodat bekende zwaktes niet misbruikt kunnen worden.
    - waarborgen te bieden tegen ongeautoriseerd kopiëren
    - alleen overhandigd te worden aan geregistreerde personen.
    - geheime sleutels worden alleen op veilige media opgeslagen bij de CA.

Controle, alarmering, rapportering

12. De geldigheid van certificaten wordt bijgehouden in een CRL. De CA zorgt voor een up-to-date CRL en voor uitwisseling daarvan met andere CA's.

2.12.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.12.4.1	geen	
2.12.4.2	12.3.2.3	De vertrouwelijkheid van cryptografische sleutels dient te zijn gewaarborgd tijdens generatie, gebruik, transport en opslag van de sleutels.
2.12.4.3	geen	

Operationele norm	TNK referentie	TNK norm
2.12.4.4	11.6.1.3	Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
2.12.4.5	12.3.2.5	Bij voorkeur is sleutelmanagement ingericht volgens PKI Overheid
2.12.4.6	geen	
2.12.4.7	10.7.1	Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.
2.12.4.8	geen	
2.12.4.9	geen	
2.12.4.10	geen	
2.12.4.11	geen	
2.12.4.12	geen	

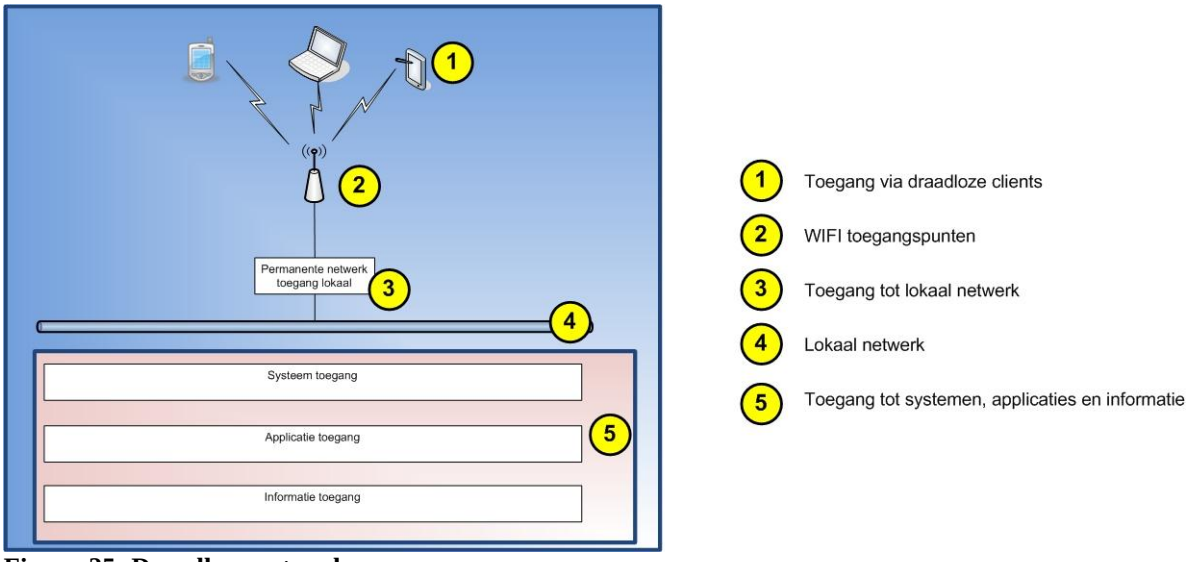
2.13 Draadloze netwerken

2.13.1 Rationale

Veel organisaties binnen de overheid maken gebruik van draadloze netwerken (bijvoorbeeld WIFI). Omdat de netwerksignalen niet kabelgebonden zijn is het mogelijk om het draadloze netwerkverkeer (op afstand) af te luisteren, te manipuleren en weer uit te zenden. Om deze reden zijn er aanvullende maatregelen nodig om de vertrouwelijkheid en de integriteit te kunnen garanderen. Een draadloos netwerk zelf (zonder deze aanvullende maatregelen) wordt als onvertrouwd beschouwd. Draadloze netwerken zijn inherent kwetsbaarder op het gebied van beschikbaarheid, een stoorzender is snel geplaatst en zeer effectief.

2.13.2 Context

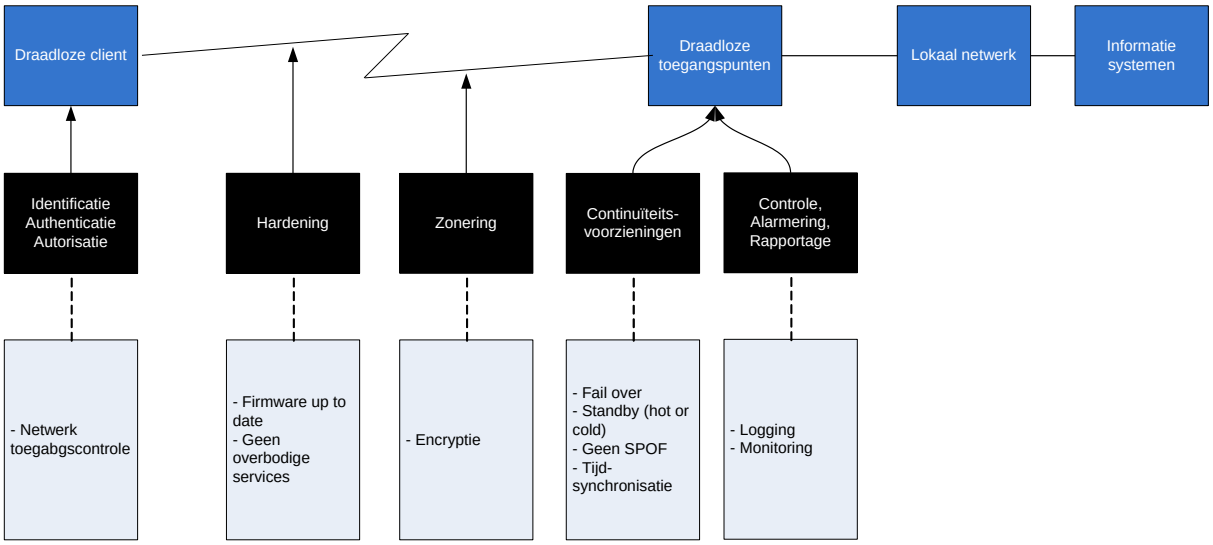
Dit patroon is gericht op de beveiliging van draadloze netwerken en de koppeling naar het lokale netwerk. Er wordt vanuit gegaan dat het lokale netwerk is opgebouwd zoals dat is beschreven in het patroon Generieke netwerk configuratie. De omgeving is geschetst in onderstaande figuur.



Figuur 25: Draadloos netwerk

2.13.3 Oplossing

Het versturen van de netwerksignalen door de lucht vormt het grootste risico. Onderstaande figuur beschrijft de noodzakelijk IB functies en beveiligingsmaatregelen om dit risico zo klein mogelijk te maken.



figuur 26: Beveiligingsfuncties draadloos netwerk (voor verklaring van gele nummers, zie figuur 29)

2.13.4 Operationele maatregelen

Identificatie, Authenticatie, Autorisatie

1. Ongeautoriseerde toegang tot het draadloze netwerk is niet mogelijk.
2. Iedere gebruiker meldt zich aan op het netwerk met een unieke identiteit.

Hardening

3. Op de netwerkcomponenten voor het draadloze netwerk draaien geen overbodige diensten.
4. Daar waar mogelijk zijn producten gebruikt die volgens een internationaal geaccepteerde standaard/organisatie (zie bijlage 2) geëvalueerd zijn.

Zonering

5. Draadloze netwerken voor verschillende doeleinden zijn minimaal logisch van elkaar gescheiden.
6. Het draadloze netwerkverkeer is volgens een voldoende veilige standaard (bijlage 2) versleuteld.

Continuïteitsvoorzieningen

7. De draadloze toegangspunten zijn dusdanig gepositioneerd dat men op de daarvoor bestemde plaatsen betrouwbaar gebruik kan maken van het draadloze netwerk.
8. De draadloze toegangspunten zijn dusdanig gepositioneerd dat er onderling geen interferentie optreed.
9. De draadloze toegangspunten zijn fysiek onbereikbaar voor onbevoegden zodat onbeschikbaarheid door fysiek ingrijpen voorkomen wordt.

Controle, Alarmering, Rapportage

10. Informatie over de inkomende en uitgaande datastromen wordt minimaal 3[8] maanden bewaard (niet de inhoud van de datastroom maar o.a. timestamp, bron IP/poort, doel IP/poort, protocol).
11. Informatie over de datastromen is alleen inzichtelijk voor geautoriseerde personen.

[8] Deze termijn is de minimaal bewaartermijn voor logs volgens het Voorschrift Informatiebeveiliging Rijksdienst – Gerubriceerde Informatie.

2.13.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.13.4.1	11.4.2.2 en 11.6.1.3	Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen. Opm.: Een draadloos netwerk (standaard WiFi) is een onvertrouwd netwerk. TNK 11.6.1.3 zegt daarover: Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
2.13.4.2	11.2.1.1	Gebruikers worden vooraf geïdentificeerd en geautoriseerd. Van de registratie wordt een administratie bijgehouden.
2.13.4.3	11.4.4.1	Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten.
2.13.4.3	11.4.5.5	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
2.13.4.4	12.1.1.5	Voor beveiliging worden componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals NBV[9] goedkeuring of certificering volgens ISO/IEC 15408 (common criteria)[10].
2.13.4.4	12.3.1.3	De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
2.13.4.5	11.4.5.2	De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.
2.13.4.6	12.3.1.3	De cryptografische beveiligingsvoorzieningen en componenten voldoen aan algemeen gangbare beveiligingscriteria (zoals FIPS 140-2 en waar mogelijk NBV).
2.13.4.7	9.2.1.1	Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningbeveiliging.
2.13.4.8	9.2.1.1	Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningbeveiliging.
2.13.4.9	9.2.1	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

[9] NBV: Nationaal Bureau voor Verbindingsbeveiliging, onderdeel van het ministerie van BZK.

[10] Voor een common criteria beoordeling moet een bewuste keuze worden gedaan voor een EAL niveau en een protection profoile dat voldoende is voor de toepassing.

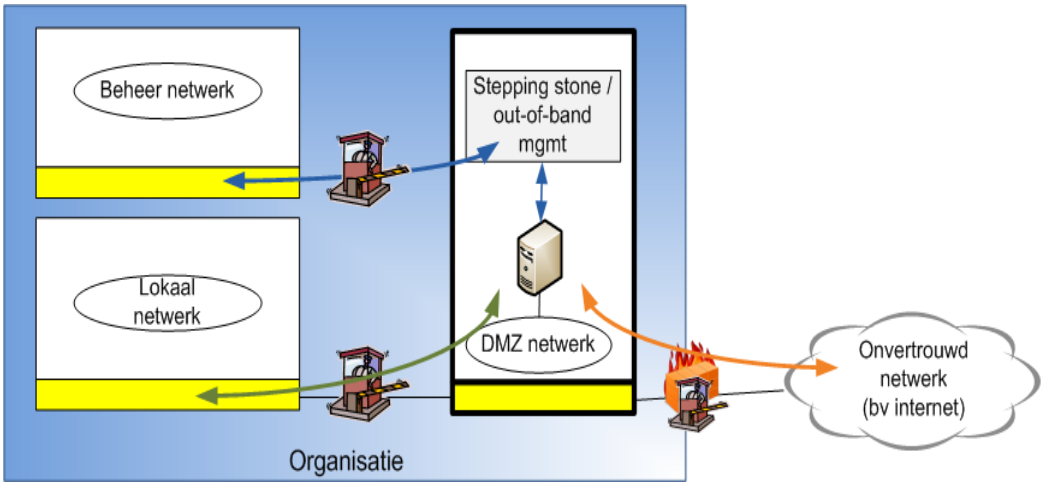
Operationele norm	TNK referentie	TNK norm
2.12.4.10	10.10.3.5	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
2.12.4.11	10.10.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.

2.14 Patroon Demilitarised Zone

2.14.1 Rationale

Informatie systemen die vanuit onvertrouwde omgevingen worden benaderd kennen een hoger risicoprofiel. Deze systemen kunnen zelf aangevallen worden of ongeautoriseerd gebruikt worden voor het aanvallen van andere interne systemen. Het is het belangrijk dat de betrokken organisaties onderling er van kunnen uitgaan dat deze systemen goed beveiligd zijn.

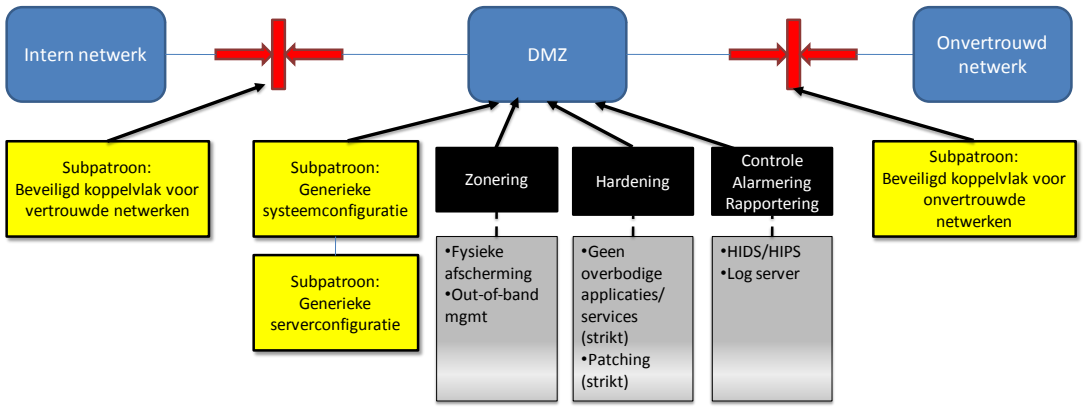
2.14.2 Context



Figuur 27: Demilitarised Zone

Figuur 27 schetst hoe toegang vanuit onvertrouwde netwerken tot interne systemen is geregeld. Het lokale netwerk is gescheiden van het onvertrouwde netwerk. Beide netwerken hebben toegang tot een 'demilitarised' zone (DMZ). Alleen de systemen binnen deze zone zijn dus toegankelijk vanuit het onvertrouwde netwerk. Het interne netwerk is afgeschermd voor toegang vanuit de DMZ.

2.14.3 Oplossing



Figuur 28: Beveiligingsfuncties DMZ

Figuur 28 schetst de IB-functies en mechanismen voor het patroon Demilitarised Zone. Binnen dit patroon worden de subpatronen "Beveiligd koppelvlak voor vertrouwde netwerken", "Beveiligd koppelvlak voor onvertrouwde netwerken" en "Generieke systeem configuratie" hergebruikt en niet opnieuw beschreven. Het eerste genoemde

koppelvlak schermt het interne netwerk af van de DMZ. De DMZ is als een vertrouwd netwerk te beschouwen: Het wordt van het onvertrouwde netwerk afgescheiden door het “Beveiligd koppelvlak voor onvertrouwde netwerken” en valt binnen het domein waarover de betreffende beheerorganisatie zelf de controle heeft. Zoals voor alle maatregelen in dit document, geldt dat beide koppelvlakken zwaardere maatregelen mogen bevatten dan hier beschreven zolang de interoperabiliteit niet wordt geschaad. Via de koppelvlakken ontstaat dus een zone, de DMZ. De zone zelf dient fysiek gescheiden te zijn van het interne netwerk. Dat betekent dat het DMZ LAN geen logische LAN kan zijn op dezelfde apparatuur als het interne netwerk.

Een andere pijler van de beveiliging van de DMZ is de bescherming van de systemen daarin. De systemen lopen meer gevaar, omdat ze ook vanuit onvertrouwde compartimenten te bereiken zijn. Ook dient extra aandacht te worden besteed aan logging en monitoring. Systemen dienen niet ongemerkt te kunnen worden aangevallen.

Tot slot is het beheer van de DMZ zelf en de systemen daarin een aandachtsgebied. Het mag niet mogelijk zijn dat via aangevallen systemen het beheerdomein gecompromitteerd wordt. Daarnaast is het onwenselijk dat door aanvallen beheervoorzieningen onbereikbaar worden. Beheer van systemen, netwerk componenten vindt daarom plaats out-of-band (dat wil zeggen niet via het productie netwerk, ook niet logisch gescheiden daarbinnen). Bijvoorbeeld door toepassing van ‘console servers’ welke zijn aangesloten op een fysiek gescheiden beheer segment binnen de DMZ.

2.14.4 Operationele maatregelen

Zonering

1. De DMZ is ontkoppeld van het onvertrouwde netwerk door toepassing van het patroon “Beveiligd koppelvlak voor onvertrouwde netwerken”.
2. De DMZ is ontkoppeld van het interne netwerk door minimaal toepassing van het patroon “Beveiligd koppelvlak voor vertrouwde netwerken”.
3. Het netwerk van de DMZ is fysieke gescheiden van andere netwerken.
4. Het beheernetwerk is fysiek gescheiden van het beheer segment in de DMZ. Het beheer verloopt via out-of-band voorzieningen.

Hardening

5. Alle systemen binnen de DMZ zijn ‘gehardend’ waarbij rekening gehouden is met het hogere dreigingsprofiel.

Controle, Alarmering, Rapportering

6. Alle aanvallen op systemen worden gedetecteerd en waar mogelijk ook op systeem niveau tegengehouden.

2.14.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.14.4.1	11.4.5.3	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie. Opm.: specifiek gemaakt adhv het OB

Operationele norm	TNK referentie	TNK norm
2.14.4.2	11.4.5.3	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie. Opm.: specifiek gemaakt adhv het OB
2.14.4.3	11.4.5.3	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie. Opm. 1: specifiek gemaakt adhv het OB **Opm. 2: operationele norm 2.14.4.3 geeft aan dat de scheiding fysiek moet zijn. Heroverwegen of logische scheiding ook voldoende is.**
2.14.4.4	11.4.5.4	Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
2.14.4.5	11.4.5.5	Zonering wordt ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).
2.14.4.6	10.4.1.4	Er zijn maatregelen om verspreiding van virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering).

2.15 Logging & monitoring

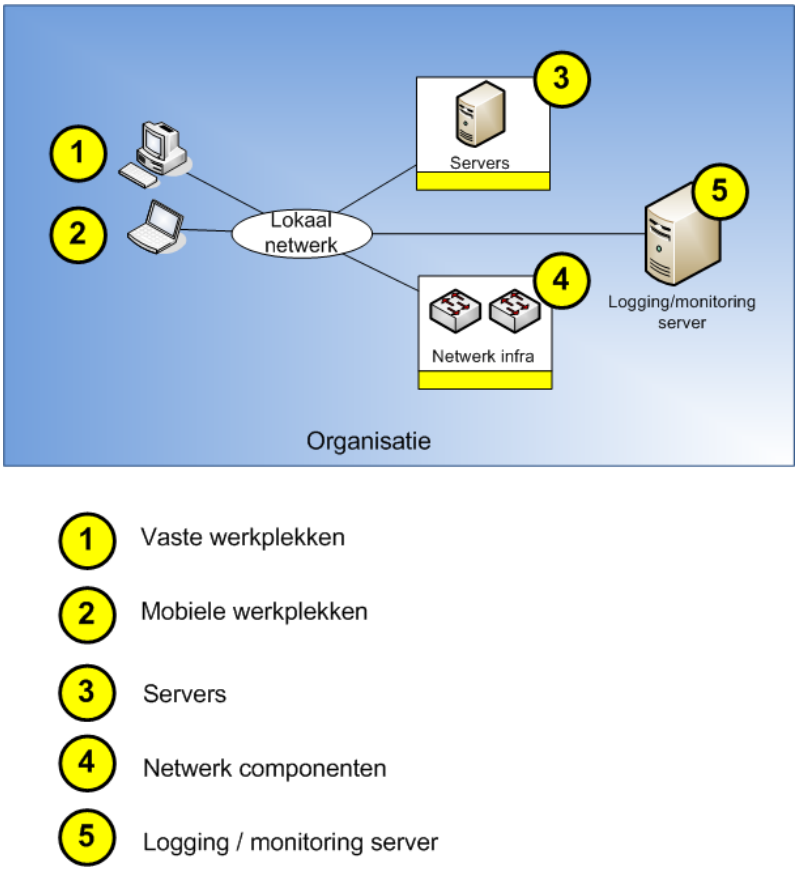
2.15.1 Rationale

Om beveiligingsincidenten te kunnen detecteren en analyseren is het toepassen van logging en monitoring noodzakelijk. Monitoring dient in het bijzonder voor het tijdig detecteren van incidenten, zodat er tijdig actie op kan worden ondernomen (alerting). De logging is van belang bij het analyseren van incidenten; als de detectie pas in een laat stadium plaatsvindt kan met behulp van de logging worden achterhaald welke gebeurtenissen eraan vooraf gingen.

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

2.15.2 Context

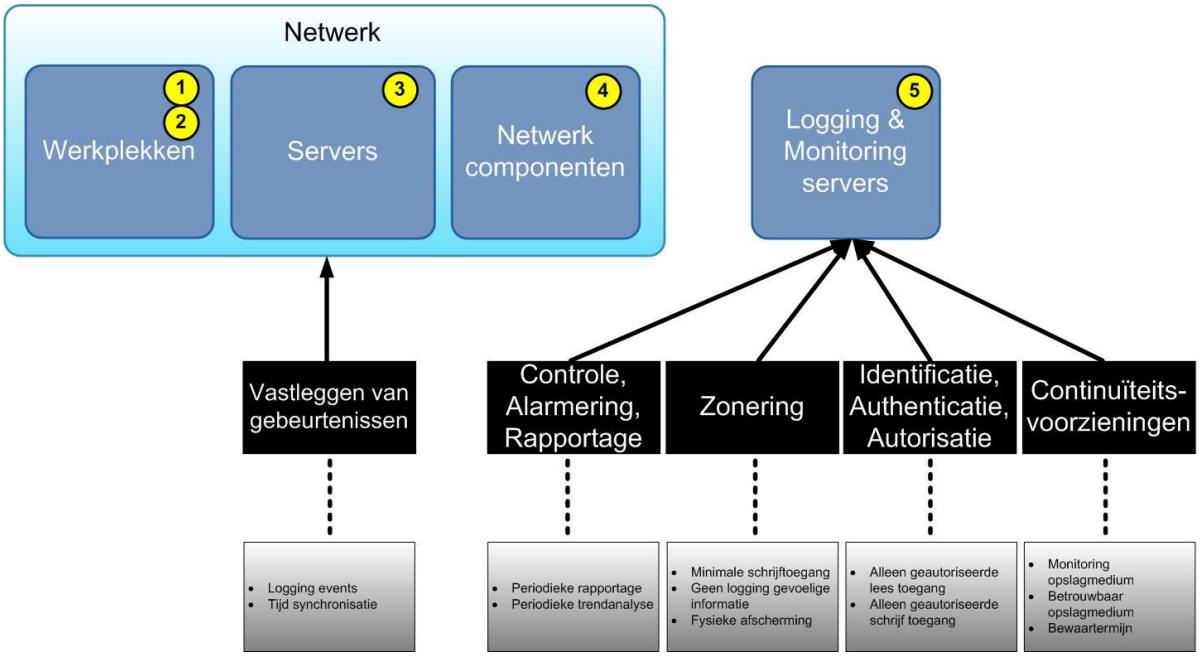
Dit patroon is gericht op logging, monitoring en analyse van afwijkend gedrag in IT voorzieningen. Logging & monitoring is op verschillende manieren in te richten. Dit patroon bevat de basis functionaliteiten van logging & monitoring, maar ook een systeem om dit op effectieve wijze te faciliteren. Dit systeem van maatregelen wat overkoepelend de logging & monitoringfunctie vervult wordt *Security Information Event Management*, hierna SIEM genoemd. Dit systeem is gepositioneerd in het beheerdomein. De basis functionaliteiten zijn noodzakelijk om aan het TNK te voldoen. SIEM is optioneel, maar sterk aanbevolen. De omgeving is geschetst in figuur 29.



Figuur 29: Logging en monitoring

2.15.3 Oplossing

Figuur 30 schetst de IB-functies en mechanismen voor het patroon logging/monitoring. Bij logging voor analyse van incidenten zijn de integriteit en beschikbaarheid belangrijk. De gewenste loggegevens dienen altijd te kunnen worden opgeslagen en daarna geraadpleegd te kunnen worden een zekere tijdsperiode na de logging. Inzage in de loggevens dient beperkt te zijn tot geautoriseerde personen en de loggegevens zelf dienen voldoende informatie te verschaffen voor analyse maar niet voor doorbreken van beveiliging (denk aan opslag van wachtwoorden).



Figuur 30: Beveiligingsfuncties logging en monitoring

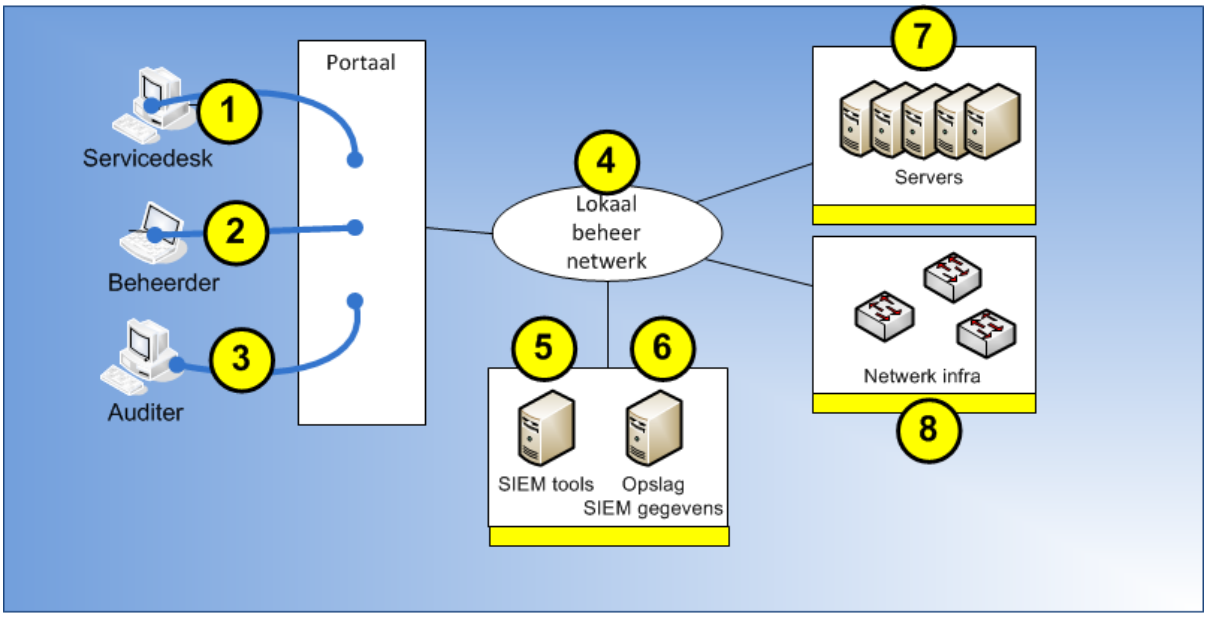
SIEM

Een systeem van voorzieningen, die voorziet in het continu loggen en (near-) realtime monitoren van beveiligingsmaatregelen en afwijkend gedrag in infrastructuren, wordt vaak aangeduid met SIEM. Het voorziet in lange-termijn opslag van verzamelde gegevens en in historische- en trendanalyse van die gegevens en biedt functies voor forensisch onderzoek.

Figuur 31 geeft in een donkere (blauw) kleur aan uit welke onderdelen SIEM is opgebouwd. Vanuit de bronsystemen word informatie verzameld door de Security Event en Information Monitoring module. Die module bestaat de subprocessen die de volgende bewerking op de informatie uitvoeren:

- Verzamelen
- Normaliseren
- Verrijken
- Aggregeren
- Correleren

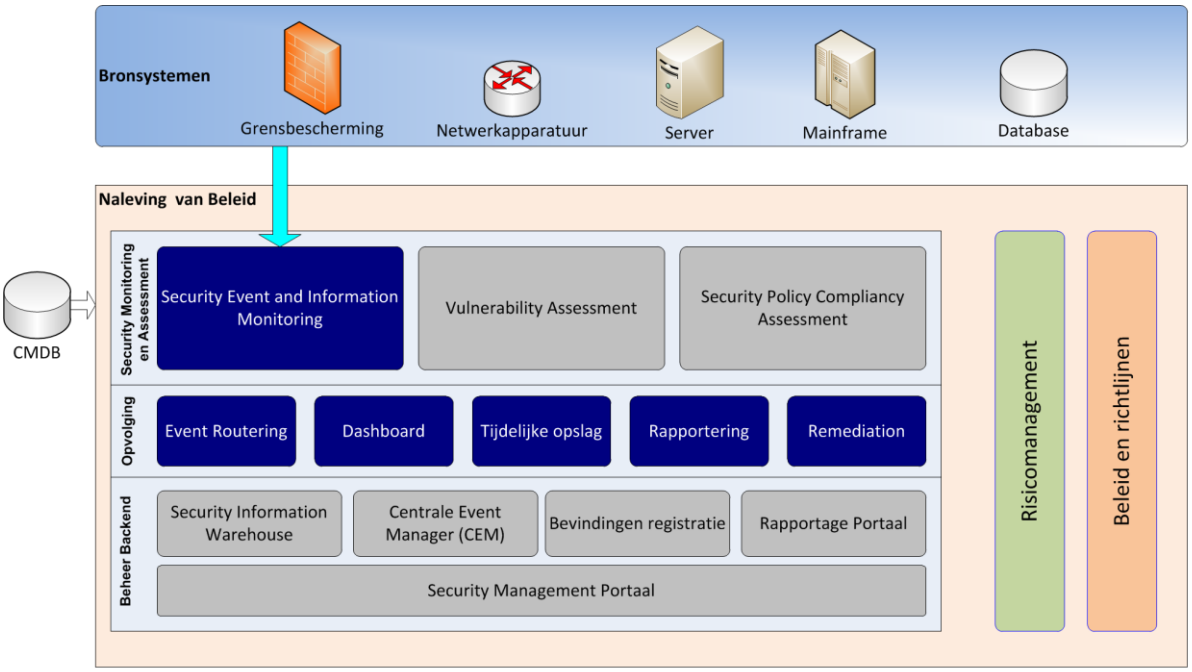
Vervolgens wordt deze informatie met de originele melding opgeslagen en voor weergave op een dashboard en rapportagefunctie geschikt gemaakt. De Security Information Datawarehouse functioneert als een ‘verzamelbak’ van beveiligingsgerelateerde informatie voor lange termijn opslag.



1 Koppeling met Servicedesk
2 Toegang Beheerders
3 Toegang Auditer
4 Beheernetwerk
5 SIEM tooling, die z'n gegevens over afwijkend logisch gedrag verkrijgt vanuit de IT-infrastructuur
6 Opslag voor SIEM- gegevens, b.v. in een datawarehouse
7 Servers en applicaties die afwijkingen rapporteren aan SIEM
8 Netwerkapparatuur die afwijkingen rapporteert aan SIEM

Figuur 31: SIEM

In SIEM systemen wordt gebruik gemaakt van Network Behavior Anomalies (NBA) technieken. Op basis van baselines wordt afwijkend gedrag in netwerk-gebruik gedetecteerd en eventueel gecorreleerd met andere gebeurtenissen. Figuur 32 laat de SIEM componenten zien.



Figuur 32: Componenten SIEM

Afwegingen voor de toepassing van SIEM

- Monitoring is een belangrijk onderdeel voor de toetsing op naleving van beveiligingsbeleid, maar is daarin slechts één van de drie belangrijkste securitymanagement services. Controle op de naleving van het beleid steunt daarom evenzeer op Vulnerability Management en Policy Compliance Management.
- Bij de keuze en implementatie van SIEM-tooling 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 securitymanagement. Voor kleinschaliger toepassing van monitoring kan de toepassing van individuele of platformgebonden rapportagetools al voldoende zijn.

2.15.4 Operationele maatregelen

Vastleggen van gebeurtenissen

1. De volgende typen informatie moeten gelogd worden:
    - authenticatie pogingen (al dan niet succesvol)
    - gedetecteerde malware (wormen/virussen/spyware e.d.)
    - toegang tot gedeelde bestanden/informatie
    - beheeracties van beheerders
    - storingen in de dienstverlening
    - significante gebruikershandelingen (zie bijlage 1)
2. Een logregel moet de volgende informatie bevatten:
    - Datum, tijdstip en tijdzone, minimaal tot op secondeniveau
    - gebruikersnaam/identificatie
    - werkstation/locatie informatie
    - activiteit
    - het object waarop de activiteit werd uitgevoerd

- indien relevant, het resultaat van de activiteit

3. Logregels hebben een volgnummer en een timestamp, waardoor verwijderde regels gedetecteerd kunnen worden.
4. Om een goede analyse van incidenten mogelijk te maken moeten de systemen die loginformatie versturen een gesynchroniseerde klok hebben, met een maximale afwijking zoals genoemd in bijlage 1.

Controle, Alarmering, Rapportering

5. Op het mogelijk vollopen van het opslagmedium van logging-informatie dient actief gemonitord te worden. Indien het opslagmedium toch vol is wordt op een veilige manier gefaald.
6. Aanpassingen in de logging worden op een separaat systeem gelogd worden om fraude te detecteren.
7. Beveiligingsinstellingen dienen te worden gemonitord, en wijzigingen van beveiligingsinstellingen gelogd.
8. Het moet mogelijk zijn om wijzigingen ingedeeld naar (functionele) rol in te zien van gebruikersaccounts (van systemen/werkplekken).
9. De belasting van serversystemen wordt automatisch gemeten en kan worden uitgelezen via bijvoorbeeld snmp, minimaal versie 3.
10. Wijzigingen in firewall instellingen en firewall acties worden gelogd.
11. Rapportage over logging-informatie met betrekking tot beveiliging dient regulier (zie bijlage 1 voor minimum) te worden opgeleverd aan de beveiligingsfunctionaris/security officer.
12. Trendanalyses over beveiligingsgebeurtenissen dienen maandelijks te worden opgeleverd aan de beveiligingsfunctionaris/security officer.
13. Beveiligingsincidenten worden meteen (volgens een vooraf opgestelde procedure) aan de beveiligingsfunctionaris/security officer gemeld. Bewijsmateriaal wordt hierbij aan de beveiligingsfunctionaris/security officer overhandigd.
14. De configuratie van systemen moet zijn vastgelegd en moet inzichtelijk zijn voor beheerders en ander geautoriseerd personeel.

Zonering

15. De integriteit van logbestanden moet worden gewaarborgd, schrijftoegang moet zoveel mogelijk worden beperkt (write-once).
16. Een logregel bevat geen wachtwoorden of andere informatie die tot beveiligingsincidenten kan leiden.

Identificatie, authenticatie, autorisatie

17. Logging informatie mag alleen door geautoriseerde personen benaderd worden.
18. Alleen geautoriseerde systemen kunnen in de centrale log-database schrijven.
19. Alleen geautoriseerde beheerders hebben de mogelijkheid om de log-instellingen te wijzigen of logbestanden aan te passen.

Continuïteitsvoorzieningen

20. Het overschrijven of verwijderen van logbestanden wordt in het nieuwe logbestand gelogd.
21. Bewaartermijn: alle logging-informatie moet minimaal 3 maanden bewaard blijven, en gedurende die tijd kunnen worden ingezien. Logging-informatie over een vermoed incident moet 5 jaar bewaard blijven. (bepaling VIR-BI)
22. Voor archivering van (centrale) logbestanden dient een hash van het logbestand gemaakt te worden, die apart wordt gearchiveerd.

2.15.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.15.4.1	10.10.1.2	Een logregel bevat minimaal: • een tot een natuurlijk persoon herleidbare gebruikersnaam of ID • de gebeurtenis (zie 10.10.2.1) • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis
2.15.4.1	10.10.2.1	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore • gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases) • handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels • beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services) • verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen) • handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.
2.15.4.2	10.10.1.2 en 10.10.2.1	**Zie hierboven**
2.15.4.3	10.10.1.2	Een logregel bevat minimaal: • een tot een natuurlijk persoon herleidbare gebruikersnaam of ID • de gebeurtenis (zie 10.10.2.1) • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis
2.15.4.4	10.10.6.1	Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is.

Operationele norm	TNK referentie	TNK norm
2.15.4.5	10.10.1.5	Controle op opslag van logging: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is).
2.15.4.6	10.10.3.3	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
2.15.4.7	10.10.2.1	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore • gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases) • handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels • beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services) • verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen) • handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.
2.15.4.8	10.10.1.4	Logberichten worden overzichtelijk samengevat. Daartoe zijn systemen die logberichten genereren aangesloten op een Security Information and Event Management systeem (SIEM[11]) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven worden. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden.

[11] Een SIEM systeem kan, afhankelijk van de context, meer of minder uitgebreid zijn. Essentieel is dat de loggegevens van beveiligingscomponenten en authenticatiemiddelen dusdanig overzichtelijk worden gepresenteerd dat belangrijke meldingen niet gemist worden.

Operationele norm	TNK referentie	TNK norm
2.15.4.9	10.3.13	De ICT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheideis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
2.15.4.10	10.10.2.1	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore • gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases) • handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels • beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services) • verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen) • handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden.
2.15.4.11	10.10.1.1	Van logbestanden worden rapportages gemaakt die periodiek, minimaal maandelijks, worden beoordeeld.
2.15.4.11	13.2.3.1	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
2.15.4.12	13.1.1.4	Informatie over de beveiligingsrelevante handelingen van de gebruiker wordt regelmatig nagekeken. De BVA bekijkt maandelijks een samenvatting van de informatie.
2.15.4.13	10.8.2.2	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, alsmede procedures over melding van incidenten.

Operationele norm	TNK referentie	TNK norm
2.15.4.13	13.1.1.2	Er is een contactpersoon aangewezen voor het rapporteren van beveiligingsincidenten. Voor integriteitsschendingen is ook een vertrouwenspersoon aangewezen die meldingen in ontvangst neemt.
2.15.4.14	12.4.1.3	Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.
2.15.4.15	10.10.3.3	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
2.15.4.16	10.10.1.3	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit Betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, enz.).
2.15.4.17	10.10.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
2.15.4.18	10.10.3.3	Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
2.15.4.19	10.10.3.4	De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten te worden zal daarbij altijd het vier ogen principe toegepast worden.
2.15.4.20	10.10.3.1	Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
2.15.4.21	10.10.3.5	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
2.15.4.22	10.10.3.5	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

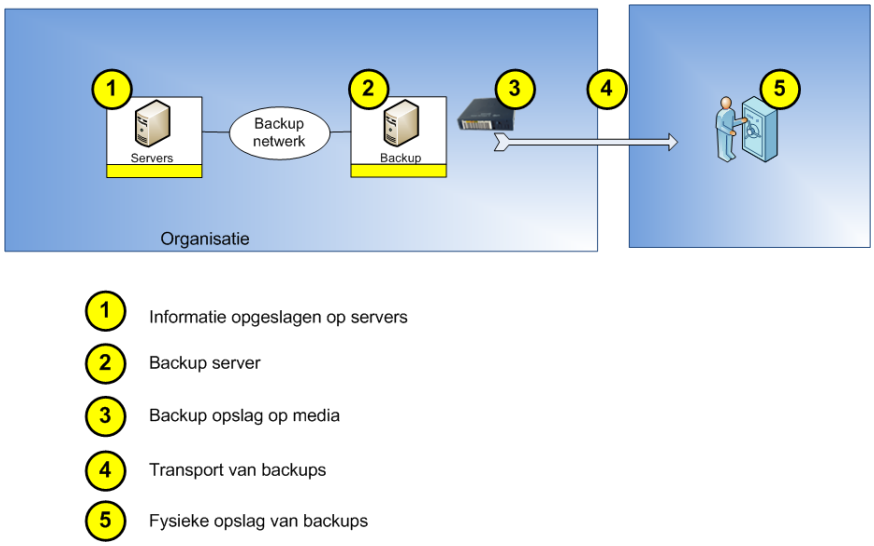
2.16 Patroon data recovery

2.16.1 Rationale

Omdat diensten een vastgesteld beschikbaarheidsniveau moet halen is het hebben van de mogelijkheid tot restoren van de veiliggestelde data noodzakelijk. Als data op een informatiesysteem onverhoopt beschadigd raakt moet het mogelijk zijn om terug te gaan naar een integere situatie.

In dit patroon worden de maatregelen genoemd om op een veilige wijze de data recovery (backup & restore) cyclus in te richten.

2.16.2 Context

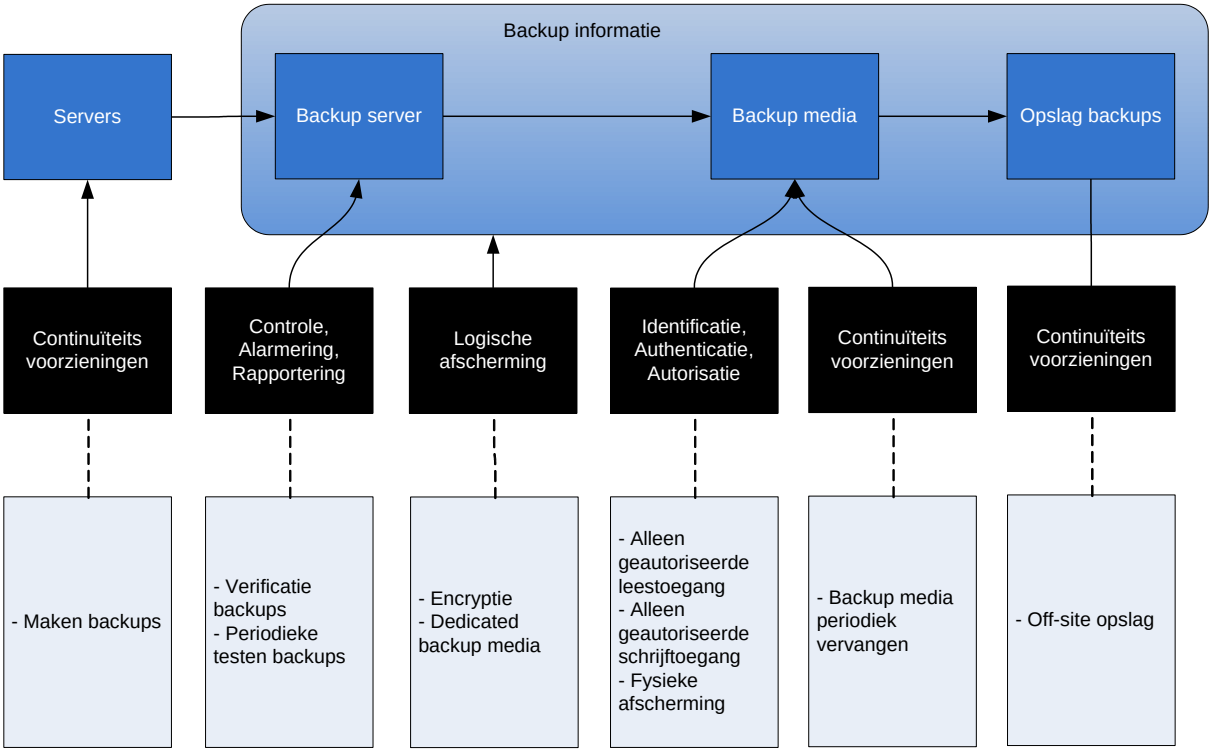


Figuur 33: Data recovery

Figuur 33 schetst de situatie rondom data recovery. Als maatregel voor het realiseren van een hoge beschikbaarheid wordt de data die in de informatiesystemen is opgeslagen gebackupt (Continuïteitsvoorziening). Of dit succesvol is gebeurd moet worden gecontroleerd en vastgelegd (Vastleggen van gebeurtenissen). Een onmisbare methode van controle is het uitvoeren van proef-restores.

Toegang tot de backup-informatie moet worden afgeschermd; alleen de noodzakelijke beheerders mogen toegang hebben. Dit kan door het gebruik van encryptie worden gerealiseerd (Zonering). De backups worden zowel on-site als off-site opgeslagen, wat weer een vorm van continuïteitsvoorziening is, en daar moet ook de fysieke toegang tot de backups worden afgeschermd tot alleen geautoriseerde personen (IAA). Ongeautoriseerde toegang moet worden gemeld, zodat er maatregelen getroffen kunnen worden (Controle, alarmering, rapportering).

2.16.3 Oplossing



Figuur 34: Beveiligingsfuncties data recovery

Figuur 34 schetst de IB-functies en mechanismen voor het patroon data recovery. Het maken van backups is een taak van beheer en de toegang (*autorisatie*) tot gemaakte backups dient beperkt te zijn tot de daarvoor verantwoordelijke beheerders om zo de *beschikbaarheid*, *integriteit* en *vertrouwelijkheid* van de op de backups opgeslagen data te kunnen waarborgen. Om dit te waarborgen dient ook zorgvuldig omgegaan te worden met de datadragers voor de backups en de procedures voor het maken van backups. De correcte werking van de datadrager zelf dient te worden gewaarborgd en bij opslag dient te worden gecontroleerd of de data correct is opgeslagen.

2.16.4 Operationele maatregelen

Continuïteitsvoorzieningen

1. Dagelijks wordt een incrementele backup gemaakt van de data.
2. Wekelijks wordt een full backup gemaakt van de data
3. Dagelijkse backups worden 1 maand bewaard
4. Wekelijkse backups worden 3 maanden bewaard
5. Iedere 3 maanden wordt er een restore-test uitgevoerd om te controleren of de opgeslagen data ook echt terug gehaald kan worden
6. Backups van oneven weken worden off-site bewaard, in een locatie waarvan het onwaarschijnlijk is dat die door eenzelfde calamiteit getroffen kan worden als de operationele locatie. De minimale afstand tussen de locaties is vastgelegd in het SLA (zie bijlage 1).

Controle, Alarmering, Rapportering

7. Er wordt gecontroleerd of een backup proces succesvol is geweest

Identificatie, authenticatie, autorisatie

8. Toegang tot backups is afgeschermd tot alleen de noodzakelijke beheerders

Logische afscherming

9. Backups worden versleuteld bij transport door onvertrouwd gebied (zowel fysiek als digitaal transport)
10. Backup media worden pas na vernietiging van de data erop hergebruikt voor andere systemen.

2.16.5 Relatie tactische normen

Operationele norm	TNK referentie	TNK norm
2.16.4.1	10.5.1.1	Opm.: nadere invulling van TNK 10.5.1.1 TNK 10.5.1.1: Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
2.16.4.2	10.5.1.1	Opm.: nadere invulling van TNK 10.5.1.1 TNK 10.5.1.1: Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen..
2.16.4.3	10.5.1.1	Opm.: nadere invulling van TNK 10.5.1.1 TNK 10.5.1.1: Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
2.16.4.4	10.5.1.1	Opm.: nadere invulling van TNK 10.5.1.1 TNK 10.5.1.1: Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
2.16.4.5	10.5.1.1	Opm.: nadere invulling van TNK 10.5.1.1 TNK 10.5.1.1: Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
2.16.4.6	10.5.1.4	Back-ups worden bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.
2.16.4.7	10.5.1.1	Opm.: nadere invulling van TNK 10.5.1.1 TNK 10.5.1.1: Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen.
2.16.4.8	10.5.1.5	De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.
2.16.4.9	11.6.1.3	Bij transport van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast
2.16.4.10	10.7.2.1	Er zijn procedures vastgesteld en in werking voor verwijderen van vertrouwelijke data en de vernietiging van verwijderbare media. Verwijderen van data wordt gedaan met een Secure Erase voor apparaten waar dit mogelijk is. In overige gevallen wordt de data twee keer overschreven met vaste data, één keer met random data en vervolgens wordt geverifieerd of het overschrijven is gelukt.

3 Bijlage 1: Norm met minimale waarden voor SLA

Beschikbaarheidseisen

Netwerk	99%
Kritische applicaties	99%
Koppelvlakken	99%

Maximale periode waar binnen geupdate wordt

IDS signatures	1 dag
Software updates	7 dagen
Kritische patches	1 dag
Security updates	1 dag
Virus definities	1 dag

Maximaal interval

Virusscan van opgeslagen data op server	7 dagen
Virusscan van opgeslagen date op mobiele werkplek	7 dagen
Controleren consistentie gerepliceerde informatie	7 dagen
Controle of inactief account verwijderd kan worden	90 dagen
Wijzigen van het wachtwoord	60 dagen
Ongeldig maken van initïele wachtwoord	1 dag
Inschakelen screensaver na inactiviteit	15 minuten

Cryptografie

Minimale encryptiestandaard	AES 256
Minimale hash algoritme	SHA2
Beveiligingscertificaten	X.509 versie 3

Maximale en minimale waarden

Minimale afstand tussen redundante systemen	500 meter
Minimale afstand tussen off-line backupmedia	501 meter
Maximale afwijking van UTC van systeemklok	200 ms
Maximale afwijking van datum en tijd in logregel	500 ms
Minimale versie SNMP	versie 3
Maximaal aantal inlogpogingen	5
Minimale blokkade na mislukte inlogpogingen	10 minuten
Minimale periode rapportage over logging-informatie	maandelijks

Significante gebruikershandelingen die gelogd worden

Zie tactisch normenkader 10.10.1.2 en 10.10.1.3.

4 Bijlage 2: Cryptografie

Daar waar cryptografische producten gebruikt worden wordt aanbevolen zoveel mogelijk gebruik te maken van de producten die het Nationaal Bureau Verbindingsbeveiliging heeft goedgekeurd voor het rubriceringsniveau “Dep. VERTROUWELIJK” of hoger. Het NBV is een onderdeel van de AIVD en de lijst met goedgekeurde producten is op de website van de AIVD te vinden.

Waar het niet mogelijk is met goedgekeurde producten te werken wordt gebruik gemaakt van robuuste algoritmen met een voldoende lange sleutel. Voor verbindings- en dataencryptie is dit minimaal AES met een sleutellengte van 128 bits of gelijkwaardig. Voor hash algoritmen is dit minimaal SHA2 of gelijkwaardig.