

Logging en loganalyse wordt ook geschaard onder security monitoring. Logging is het schrijven van informatie in een logbestand naar aanleiding van een handeling of gebeurtenis. Een logbestand is een chronologische vastlegging van informatie, dat wil zeggen dat de tijdsvolgorde van handelingen of gebeurtenissen worden weerspiegeld in het logbestand. Het doel van het vastleggen van informatie is het traceerbaar maken van gebeurtenissen en handelingen. Er kan dan gereproduceerd worden wanneer wat gebeurd is en wie of wat een gebeurtenis heeft geïnitieerd.

Loginformatie kan worden vastgelegd voor verschillende doeleinden, namelijk voor beveiliging, auditing en voor beheer. In het kort bestaan er de volgende soorten log:

- Transactie log waarmee een transactie geregeneerd kan worden in geval van een storing;
- juridische log waarmee het mogelijk is te achterhalen wat er ontvangen en medegedeeld is aan relaties van de Belastingdienst.
- auditlog om vast te leggen wie wat gedaan heeft binnen een system (audittrail).
- applicatielog is een aanvulling op de auditlog om uitzonderingssituaties in de applicatielogica (bijzondere beslismomenten) te kunnen vastleggen (denk bijvoorbeeld aan uitval en uitworp).
- technische log om fouten te kunnen signaleren.

Het is denkbaar dat een handeling in meer soorten log opgenomen wordt.

Security monitoring is als volgt uitgewerkt:

- In welk logbestand wat hoelang vastgelegd moet worden, is uitgewerkt in richtlijn SM R-1;
- richtlijn SM R-2 gaat in op de detectie van onregelmatigheden in de log;
- het vaststellen of de beveiliging goed gefunctioneerd heeft wordt beschreven in SM R-3.

2.2.2 Welke informatie moet in een logbestand worden vastgelegd?

Richtlijn

SM R-1	<i>Het juist functioneren van ICT-systemen is controleerbaar en het gebruik van ICT-systemen is herleidbaar tot een natuurlijk persoon.</i>
--------	---

Risicoafweging

De verwevenheid van ICT-systemen tot een complex geheel maakt dat niet vanzelf duidelijk is waarom gebeurtenissen hebben plaats gevonden. Door het gedeeld gebruik van ICT-systemen is daarnaast niet zonder meer te achterhalen en wie bepaalde handelingen op het systeem heeft uitgevoerd. In een logbestand worden daarom gegevens over het functioneren en het gebruik van ICT-systemen vastgelegd. Deze gegevens zijn nodig om fouten in het systeem te achterhalen, misbruik van het systeem op te sporen en om personen aan te kunnen spreken op het voorwaardelijk gebruik van de ICT-systemen.

Norm

SM N-1-1	In de log wordt informatie vastgelegd waarmee reproduceerbaar is wie waar wanneer welke cruciale handelingen heeft verricht.
----------	--

Toelichting

Het is belangrijk de reproduceerbaarheid en de hoeveelheid te loggen gegevens te optimaliseren. Zo zal bijvoorbeeld het loggen van de syntax van een opgegeven query in omvang beperkter zijn dan het loggen van de output van een query. Wat exact gelogd moet worden is afhankelijk van de situatie. In de maatregelen kan dat niet uitputtend uitgewerkt worden, daarentegen worden wel een aantal indicaties aangereikt. Voorop staat in ieder geval dat fouten en misbruik opgespoord moeten kunnen worden.

Maatregelen

1. In het ontwerp is een overweging gemaakt welke fouten en misbruik binnen het systeem voor kunnen komen en hoe dit uit loginformatie kan blijken (zie ook SM N-2-2, waarin opgenomen is dat analyses en rapportages in het ontwerp gespecificeerd worden. Waar geen analyse en rapportage op plaats vindt, wordt in principe niet gelogd).

2. Het moet mogelijk zijn om de handelingen van een bepaalde persoon of component in detail in een auditlog vast te leggen. ("In detail" wil zeggen dat op basis daarvan de exact verrichte handelingen zijn te reproduceren. Dat gaat dus verder dan alleen het aanmelden op een systeem. Moet mogelijk zijn" wil zeggen dat deze logging standaard uit staat en wanneer daar aanleiding toe is selectief aangezet kan worden).
3. De volgende uitgevoerde handelingen worden in ieder geval opgenomen in de logging:
 - a. Gebruik van technische beheerfuncties (zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, uitvoering van een back-up of restore);
 - b. gebruik van functioneel beheerfuncties (zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets waaronder databases);
 - c. handelingen van beveiligingsbeheer (zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoordreset, uitgifte en intrekken van cryptosleutels);
 - d. als door middel van een functioneel account handelingen op een ander systeem worden verricht;
 - e. beveiligingsovertredingen (zoals de constatering van een virus, worm, Trojaans paard of andere malware, een poortscan of testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, het gebruik van niet operationele systeemservices, het stoppen van security services);
 - f. verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen).
4. In een te schrijven logregel wordt in ieder geval weggeschreven:
 - a. De gebruikersnaam dat verzocht een handeling uit te voeren;
 - b. het soort handeling;
 - c. het object waarop de handeling werd uitgevoerd of waar een event optrad;
 - d. het resultaat van de handeling indien dit niet uit het soort handeling is af te leiden;
 - e. de datum en het tijdstip van een handeling of event.
5. Berichten die de Belastingdienst uitwisselt met relaties van de Belastingdienst (belastingplichtigen, aanvragers van toeslagen, leveranciers van rensignementen, enz) worden vastgelegd in een juridisch archief. Hierin wordt opgeslagen:
 - a. Alle berichten die de belastingdienst ontvangt of verstuurt;
 - b. de berichtinhoud (inclusief headers) die zo dicht mogelijk de vorm benaderd zoals berichten daadwerkelijk zijn ontvangen of verstuurd, dus waarop zo min mogelijk bewerkingen (conversies) zijn uitgevoerd;
 - c. de elektronische handtekening (indien het bericht elektronisch ondertekend is) en het resultaat van de handtekeningcontrole;
 - d. het kanaal, de datum en het tijdstip van ontvangst.
6. Systeemklokken worden tijdens openstelling gesynchroniseerd en worden gelijk gezet met een atoomklok de op basis van het Network Time Protocol (NTP), zodat de juiste tijd in het logbestand vastgelegd kan worden. Een indicatie voor de synchronisatiefrequentie is 4 uur. De maximale afwijking ten opzichte van de standaardtijd is 100 milliseconden.
7. In een te schrijven logregel worden in geen geval gegevens opgenomen waardoor de beveiliging doorbroken kan worden (zoals wachtwoorden; inbelnummers).

Norm

SM N-1-2	De integriteit van opgeslagen logbestanden moet gewaarborgd zijn.
----------	---

Toelichting

Het reproduceren van wat er zich binnen ICT-systemen heeft voorgedaan aan de hand van logging is alleen goed mogelijk indien de logging weergeeft wat er zich daadwerkelijk heeft voorgedaan. Daarom vergt het waarborgen van de juistheid en volledigheid van de opgeslagen logregels aandacht. Zo mag een aangelegd logbestand niet achteraf aangepast worden, waardoor handelingen achteraf alsnog verhuld kunnen worden.

Maatregelen

1. Bij het schrijven en opslaan van logregels wordt zoveel mogelijk gebruik gemaakt van de hiervoor ingerichte generieke beveiligingsvoorzieningen (momenteel SyslogNG voor Midrange-systemen en SMIV voor Mainframe-systemen).
2. Bij het aanleggen van logbestanden wordt zo mogelijk gebruik gemaakt van "write once"-technologie.
3. De volledigheid van de logging kan worden vastgesteld, bijvoorbeeld met behulp van opeenvolgende nummers per log-event.
4. Uitsluitend geautoriseerde processen (operationeel onder een functioneel account) mogen logregels schrijven (zie ook IAM N-1-1).
5. Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers, waarbij de toegang is beperkt tot leesrechten. Zo mogelijk hebben ook beheerders geen schrijfrechten op logbestanden (zie ook IAM N-3-2).
6. Beheerders zijn niet in staat de instellingen van de logging te wijzigen of logbestanden te verwijderen, tenzij het specifiek hiervoor bevoegde beheerders zijn. Wanneer een systeem een specifieke rol voor auditdoeleinden kent, dan wordt hiervan gebruik gemaakt (zie ook IAM N-4-1).

Norm

SM N-1-3	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht.
----------	--

Toelichting

Loginformatie wordt enkel vastgelegd indien er behoefte is achteraf na te gaan wat er zich op een systeem heeft plaats gevonden. Loginformatie kan verwijderd worden als deze behoefte vervallen is. De termijn dat loginformatie bewaard moet worden is afhankelijk van het soort log dat is aangelegd. In de maatregelen zijn hiervoor indicaties opgenomen.

Maatregelen

1. Loginformatie wordt bewaard totdat de bewaartermijnen verstreken zijn. Een indicatie voor de bewaartermijn is:
 - a. Een transactie log wordt bewaard totdat is vastgesteld dat de juiste en volledige verwerking van een (batch) transactie(s) heeft plaats gevonden of totdat de mogelijkheid om een roll back uit te voeren is verstreken, veelal maximaal één dag;
 - b. een technische log wordt bewaard totdat is vastgesteld dat er zich geen verstoring in het systeem heeft voorgedaan, veelal maximaal enkele dagen tot een week;
 - c. een applicatielog wordt bewaard totdat is vastgesteld dat beslissingen op juiste gronden genomen zijn, mogelijk tot een half jaar gezien deze controles vaak handmatig worden uitgevoerd;
 - d. een auditlog wordt bewaard totdat de jaarverslaggeving is goedgekeurd en alle controles daarvoor hebben plaats gevonden, veelal tot 2 jaar;
 - e. een Juridische archief wordt bewaard totdat de termijn verstreken is dat partijen juridisch het nakomen van fiscale rechten en plichten kunnen laten vorderen. Voor informatieverstrekking is dat 5 jaar, voor de doorsnee handelingen voor heffen en innen 7 jaar en bij beroepsprocedures kan deze termijn oplopen tot 10 jaar na een gerechtelijke uitspraak.
2. Een juridisch archief mag niet vooruit gepland geautomatiseerd geschoond worden. Voor het schonen van het archief wordt een opdracht verstrekt. De hiervoor genoemde bewaartermijn van een juridisch archief is louter bedoeld als indicatie bij dimensionering van opslagruimte.
3. Het overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
4. Het vollopen van het opslagmedium voor de logbestanden wordt gelogd (zie SM N-1-1-3f) en leidt tot automatische alarmering van de beheerorganisatie (zie SM N-2-1).
5. Bij onderhoud op analyse- en raadpleegvoorzieningen voor een applicatielog, auditlog of een juridisch archief, wordt achterwaartse compatibiliteit afgedwongen. Dit wil zeggen dat ook de eerder aangelegde logbestanden binnen de bewaartermijn van het logbestand met de nieuwe of gewijzigde voorziening ontsloten kan worden.

2.2.3 Hoe moeten onregelmatigheden in het logbestand worden vastgesteld?

Richtlijn

SM R-2	<i>Verdachte handelingen in de loginformatie worden tijdigesignaleerd</i>
--------	---

Risicoafweging

Door loginformatie te analyseren kunnen fouten en misbruik gedetecteerd worden, die anders mogelijk niet ontdekt waren. Vervolgens kunnen dan tijdig passende tegenmaatregelen genomen worden, waardoor de ontstane schade beperkt wordt. Daarnaast werkt het op orde hebben van een detectief systeem ook preventief. Potentiële plegers van misbruik zijn namelijk minder geneigd tot misbruik over te gaan naarmate de kans op ontdekking groter is.

Norm

SM N-2-1	Er worden log-events onderkend die leiden tot automatische alarmering van de beheerorganisatie.
----------	---

Toelichting

Sommige beveiligingsincidenten zijn zo ernstig en urgent dat zo snel mogelijk schadebeperkende of herstelmaatregelen genomen moeten worden. ICT-systemen moeten dit ondersteunen. Tijdens het ontwerp van het ICT-systeem dient reeds gespecificeerd te worden welke beveiligingsincidenten op kunnen treden. De ernst van een incident is te ontleen aan de potentiële gevolgschade. De urgentie van een incident wordt bepaald door de snelheid waarmee tegenmaatregelen nodig zijn. Bij urgente beveiligingsincidenten zal de gevolgschade relatief snel toenemen naarmate langer wordt gewacht met het nemen van tegenmaatregelen.

Maatregelen

1. In het ontwerp is gespecificeerd welke beveiligingsincidenten kunnen optreden. Deze beveiligingsincidenten zijn geënclassificeerd naar ernst en urgentie.
2. Instelbaar is bij welke drempelwaarden (gebaseerd op de ernst en urgentie van een log-event daarbij rekeninghoudend met hoe vaak een log-event voorkomt) een melding wordt gegeven die zichtbaar is voor de beheerorganisatie.
3. Instelbaar is bij welke drempelwaarden de beheerorganisatie wordt gealarmeerd, zonodig ook buiten kantooruren.
4. In het ontwerp zijn de default instellingen (de drempelwaarden) opgenomen voor signalering en alarmering van de beheerorganisatie.
5. De ICT-systemen dienen aan te sluiten op de generieke beveiligingsvoorziening voor Security Event Management (SEM) waarmee meldingen en alarmoproepen aan de beheerorganisatie gegeven kunnen worden.

Norm

SM N-2-2	Logbestanden worden periodiek geanalyseerd en gecorreleerd ten einde beveiligingsincidenten te detecteren.
----------	--

Toelichting

De reden om deze norm in het VBI op te nemen is dat de loganalyse bij voorkeur geautomatiseerd plaats vindt en dat in het ontwerp deze analyserapporten gespecificeerd dienen te worden. Het interpreteren van loganalyserapporten en het nemen van passende maatregelen is een verantwoordelijkheid binnen het exploitatieproces (zie ook HIB CICT Ex N-1-3). Daar wordt hier verder niet op ingegaan.

Maatregelen

1. Voor rapportage en analyse van logbestanden wordt zoveel mogelijk gebruik gemaakt van generieke beveiligingsvoorzieningen voor loganalyse.
2. De correlatie en analyse van logbestanden is zoveel mogelijk geautomatiseerd.

3. De rapportages zijn gespecificeerd in het ontwerp.
4. Rapportages worden gespecificeerd in overleg met de opdrachtgever/afnemer van de rapportage.
5. Naast rapportages kunnen (met name) de auditlog en het juridisch archief middels een query mogelijkheid bevraagd worden.

2.2.4 Hoe moet vastgesteld worden dat de beveiliging juist gefunctioneerd heeft?

Richtlijn

SM R-3	<i>De goede werking van beveiligingsmaatregelen kan worden vastgesteld.</i>
--------	---

Risicoafweging

Zonder inzicht in restrisico's kunnen zwakheden in de beveiliging ongezien uitgebuit worden, waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van informatievoorziening in gevaar komt.

De verantwoordelijkheid voor de beheersing van de beveiliging is uitgewerkt in de processen van de Belastingdienst. Voor het technisch beveiligingsbeheer van de ICT-systemen is dit belegd binnen de processen van B/CICT. In het VBI wordt niet ingegaan op deze processen. Wel gaat het VBI in op de ICT-hulpmiddelen die binnen deze processen nodig zijn. In een complex geheel van ICT-systemen kunnen beveiligingsincidenten zich relatief eenvoudig aan het oog onttrekken. Hulpmiddelen om vast te stellen of de beveiliging van een systeem goed heeft gefunctioneerd, zijn dan onmisbaar. Het gaat daarbij om hulpmiddelen voor het vaststellen van:

- overtredingen van gebruiksvoorschriften (zie SM N-3-1);
- wijzigingen in statische bestanden (zie SM N-3-2);
- zwakheden in de beveiliging (zie SM N-3-3).

Norm

SM N-3-1	Het overtreden van gebruiksvoorschriften van ICT-middelen kan geautomatiseerd worden vastgesteld.
----------	---

Toelichting

Dat gebruiksvoorschriften worden nageleefd en dat ICT-middelen overeenkomstig goed huisvaderschap worden aangewend is de verantwoordelijkheid van het management van de Belastingdienstkantoor (zie HIB-BBN P&O N-8-1). Het management zal dan wel inzicht in het gebruik van deze ICT-middelen moeten hebben. Het ICT-systeem of aanvullende hulpmiddelen zal dat moeten verzorgen. Bij een meer geavanceerde rapportage kan daarbij selectie of filtering toegepast worden, zodat een rapportage meer bruikbaar is.

Maatregelen

1. In een definitiestudie wordt aangegeven welke geautomatiseerde rapportage of controle mogelijk is. Alleen indien er een concrete klantvraag voor is, worden hiervoor hulpmiddelen ingericht. Belangrijk is daarbij dat een geautomatiseerd vervaardigde rapportage daadwerkelijk door een functionaris gebruikt gaat worden.
2. Zo mogelijk wordt aangesloten bij huidige rapportages en generieke hulpmiddelen.

Norm

SM N-3-2	Wijzigingen in static content van ICT-systemen kunnen geautomatiseerd worden gedetecteerd.
----------	--

Toelichting

Static content zijn bestanden en instellingen van een ICT-systeem die statisch zijn, dat wil zeggen dat deze bestanden en instellingen bij normaal functioneren niet zullen wijzigen. Voorbeelden zijn configuratiebestanden, programmatuur, conversietabellen, parameters, etc.

Ongeautoriseerde wijzigingen kunnen de werking van het systeem drastisch beïnvloeden. Uitsluitend beheerders of speciale gebruikers mogen daarom wijzigingen doorvoeren, middels een account waaraan de benodigde beheerrollen zijn toegekend (zie IAM N-4-2) en waarvan het gebruik wordt gelogd (zie SM N-1-1-3a/b). Wijzigingen mogen bovendien uitsluitend doorgevoerd worden indien er een wijzigingsverzoek voor is (zie HIB CICT Ex N-3-2). De verantwoordelijk functionaris binnen de sector Exploitatie correleert een geautomatiseerd vervaardigde wijzigingsrapportage met de loginformatie en de wijzigingsverzoeken (zie HIB CICT Ex N-1-4). De maatregelen bij deze norm geven aan wat er binnen het ontwerp gedaan moet worden om deze geautomatiseerde wijzigingsrapportage mogelijk te maken.

Maatregelen

1. In het ontwerp wordt aangegeven welke bestanden een statisch karakter hebben (dat wil zeggen, bestanden die uitsluitend na een wijzigingsverzoek en uitsluitend door een beheerder of speciale gebruiker gewijzigd mogen worden).
2. Dynamische gegevens (zoals database bestanden en gebruikers bestanden) worden gescheiden opgeslagen van statische gegevens (zoals systeembestanden en programmatuur). Gescheiden wil zeggen in een separate directory of zo mogelijk een separate partitie.
3. In het ontwerp wordt aangegeven welke wijzigingen in de configuratie gesignaleerd moeten worden. Deze signalering is momenteel alleen ingericht voor systemen binnen het e-fundament en wel met behulp van de tool Tripwire.

Norm

SM N-3-3	ICT-systemen worden gecontroleerd op zwakheden in de beveiliging.
----------	---

Toelichting

Binnen CICT zijn hulpmiddelen ingericht om te controleren of de laatste patches zijn aangebracht en of zwakheden in de configuratie van het systeem voorkomen. Daarnaast zijn er diensten met externe partijen overeengekomen voor het doorgeven aan de Belastingdienst van waarschuwingen in het geval er in Nederland of wereldwijd beveiligingsincidenten gesignaleerd worden. Hiertoe beschikken deze externe partijen over een lijst van de bij de Belastingdienst in gebruik zijnde componenten. Willen deze hulpmiddelen en diensten effect hebben, dan moet bekend zijn wat gecontroleerd moet worden. In het ontwerp van een ICT-systeem wordt dit uitgewerkt. Aan de hand van het ontwerp beoordeelt het serviceteam beveiliging of de afspraken met waarschuwingdiensten aangepast moeten worden.

Maatregelen

1. ICT-Systemen die gekoppeld zijn met externe netwerken dienen gebruik te maken van de waarschuwingsdienst van het serviceteam Beveiliging (momenteel zijn hiervoor contracten afgesloten met Symantec en GovCert). Voor overige ICT-Systemen wordt gebruik hiervan aangeraden.
2. Van componenten binnen ICT-systemen kan bij voorkeur geautomatiseerd gecontroleerd worden of de laatste updates (patches) in systeemprogrammatuur of standaardpakket programmatuur zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de systeemeigenaar.
3. Componenten binnen ICT-systemen kunnen geautomatiseerd gecontroleerd worden op het voorkomen van bekende zwakheden in de configuratie van de componenten. De componenten die hiervoor in ieder geval voor in aanmerking komen zijn besturingssystemen (operating systemen van platformen) en netwerkcomponenten. Voor database managementsystemen en standaardapplicaties is dit wenselijk. Bij het introduceren van nieuwe componenten wordt gelijktijdig tooling geselecteerd die dit mogelijk maakt.

2.3 Encryption

2.3.1 Wat is encryption?

Encrypt/Decrypt

Encryption is een wiskundige techniek waarbij gegevens volgens een vast patroon (algoritme) worden vercijferd (encrypt) met een bepaalde waarde (de cryptografische sleutel). Het doel hiervan is om gegevens tijdens communicatie en de opslag te beschermen tegen kennisname door onbevoegden (het waarborgen van de vertrouwelijkheid van gegevens). Het berust op het principe dat encrypte boodschappen door iedereen gezien mogen worden, omdat uitsluitend met een cryptografische sleutel de boodschap ontcijferd (decrypt) kan worden.

Sign/Verify

Naast het waarborgen van de vertrouwelijkheid kan encryptie ook gebruikt worden om onweerlegbaarheid (in het Engels: non-repudiation) en integriteit te waarborgen. Dit wordt gedaan door een reeks controlegetallen (hash) voor het te verzenden bericht te berekenen. Aan de hand van de hash kan vastgesteld worden dat een bericht tijdens communicatie en opslag ongewijzigd is. Het plaatsen van een elektronische handtekening (sign) bestaat uit het encrypten van de hash. Het controleren van een elektronische handtekening wordt verify genoemd.

Soorten algoritmen

Er zijn veel encryptietechnieken (algoritmen). Er zijn onder meer verschillende technieken voor de verschillende waarborgen (vertrouwelijkheid, integriteit, onweerlegbaarheid, authenticatie) die encryptie moet bieden. Daarnaast is er een onderscheid in symmetrische algoritmen en asymmetrische algoritmen. Symmetrische algoritmen gebruiken dezelfde cryptografische sleutel voor encryptie en decryptie. Bij asymmetrische algoritmen wordt een sleutelpaar gebruikt. Dit sleutelpaar bestaat uit een openbare sleutel en een persoonlijke sleutel. Als aanduiding van deze sleutels worden de engelse termen public key respectievelijk private key gehanteerd. De public key is openbaar en wordt gepubliceerd. De private key is strikt persoonlijk en vertrouwelijk. De sleutels van een sleutelpaar zijn op een wiskundige wijze met elkaar verbonden. Symmetrische en asymmetrische algoritmen hebben ieder eigen voor- en nadelen. Kortweg bieden symmetrische algoritmen een betere performance en asymmetrische algoritmen een eenvoudiger sleutelbeheer. Daarom wordt vaak een mengvorm gebruikt: hybride encryptie. Hierbij wordt een bericht symmetrisch encrypt en de gebruikte symmetrische sleutel met een asymmetrisch algoritme uitgewisseld.

PKI en certificaten

PKI staat voor Public Key Infrastructure. Deze infrastructuur wordt gebruikt bij het sleutelbeheer voor encryptiesystemen die gebruik maken van asymmetrische encryptie. Kenmerkend hierbij is dat er gebruik wordt gemaakt van certificaten. In een certificaat verklaart een derde partij dat volgens bepaalde voorwaarden vastgesteld is (bijvoorbeeld gegevens van de certificaathouder zijn gecontroleerd of de certificaathouder heeft zich geïdentificeerd met een identiteitsbewijs) dat een in het certificaat opgenomen publieke sleutel tot de houder van het certificaat behoort. De certificerende partij wordt Certification Authority (CA) genoemd. In de wet Elektronische handtekening wordt een elektronische handtekening juridisch als gelijkwaardig beschouwd aan de traditionele handtekening, indien de elektronische handtekening een gekwalificeerde handtekening is. Eén van de voorwaarden voor een gekwalificeerde handtekening is dat de CA een volgens wettelijke voorwaarden geaccrediteerde partij is.

Structuur van richtlijnen voor encryptie

Bij de richtlijnen en normen worden zonodig verdere toelichtingen gegeven. Er wordt daarbij achtereenvolgens ingegaan op:

- Wanneer encryptie toegepast moet worden (ENC R-1);
- hoe sterk de encryptie moet zijn (ENC R-2);
- hoe het sleutelbeheer geregeld moet worden (ENC R-3).

2.3.2 Wanneer moet encryptie worden toegepast?

Richtlijn

ENC R-1	<i>De beperkingen van toegangsbeveiliging worden gecompenseerd door het toepassen van encryptie.</i>
---------	--

Risicoafweging

Indien gegevens van de Belastingdienst worden gecommuniceerd met ICT-systemen die niet van de Belastingdienst zijn of indien de gegevens op gegevensdragers buiten de Belastingdienst worden opgeslagen, dan heeft de logische en fysieke toegangsbeveiliging van de Belastingdienst hier geen controle over. Door encryptie toe te passen en de cryptografische sleutels onder logische en fysieke toegangsbeveiliging van de Belastingdienst te brengen, kan ook buiten de ICT-omgeving van de Belastingdienst de integriteit en de vertrouwelijkheid van gegevens van de Belastingdienst worden gewaarborgd.

Daarnaast biedt encryptie ook mogelijkheden om de beperkingen van toegangsbeveiliging binnen de ICT-omgeving van de Belastingdienst te compenseren. Het toepassen van encryptie op een beperkte hoeveelheid gegevens die extra bescherming vergen, is efficiënter dan de toegangsbeveiliging van de gehele ICT-omgeving op het gewenste hogere niveau te brengen.

Of encryptie toegepast moet worden of dat de toegangsbeveiliging (uit het onderdeel Identity and Access Management) voldoende zijn, is afhankelijk van de mate van integriteit en vertrouwelijkheid van de te beschermen gegevens. Vanuit de wetgeving, met name de Wet Bescherming Persoonsgegevens (WBP), wordt vooral het accent op het niveau van vertrouwelijkheid gelegd. Het VBI sluit hier op aan.

Norm

ENC N-1-1	De communicatie en de opslag van vertrouwelijke gegevens worden buiten de kritische computerruimten van de Belastingdienst in principe door encryptie beschermd.
-----------	--

Toelichting

Vertrouwelijke gegevens zijn in dit kader gegevens van de Belastingdienst die alleen binnen het Ministerie van Financiën (waaronder de Belastingdienst) toegankelijk mogen zijn. Dat zijn alle gegevens behoudens openbare gegevens. Openbare gegevens mogen vrij beschikbaar worden gesteld. Vertrouwelijke gegevens moeten tijdens het transport en de opslag beschermd worden door encryptie. Tijdens de verwerking van deze gegevens mogen de gegevens tijdelijk van hun encryptie worden ontdaan. Kritische computerruimten (denk aan de computerzaal, patchruimten) zijn ruimten waar een strenger regime van fysieke toegangsbeveiliging van toepassing is dan op de niet-openbare ruimten binnen belastingdienst gebouwen (zie HIB-BBN 2005 G&I N-1-1).

In eerder beleid werd aangegeven dat uitsluitend wachtwoorden tussen de server (in een kritische computerruimte) en een werkplek van een belastingdienstmedewerker (in niet-openbare ruimte) encrypt moesten zijn. Deze norm is nu verscherpt. "In principe" betekent dat nog steeds alle vertrouwelijke gegevens binnen openbare ruimten worden encrypt. Daarnaast worden -en dat is nieuw- alle vertrouwelijke gegevens buiten de kritische ruimten encrypt, voorzover dit ten minste binnen redelijke technische mogelijkheden ligt.

Maatregelen

1. Vertrouwelijke gegevens worden zoveel mogelijk binnen kritische ruimtes bewaard, zodat de toepassing van encryptie beperkt kan worden (denk bijvoorbeeld aan het blokkeren van lokale opslag van gegevens op de vaste schijven van desktop PC's en opslag op diskette, DVD en USB-stick zie ook IAM N-3-1-2a).
2. Mediadragers met vertrouwelijke gegevens zijn encrypt indien deze buiten kritische computerruimte worden bewaard (denk bijvoorbeeld aan extern opgeslagen backup tapes, diskettes, DVD's, CD-ROM's en USB-sticks).
3. Het extern geheugen van mobiele apparatuur is encrypt (denk aan de harde schijven van PPC's en geheugenkaarten in PDA's/smartphones).

4. Vertrouwelijke gegevens getransporteerd over een publiek netwerk zijn encrypt tijdens tenminste het transport over het publieke deel van het netwerk (denk aan VPN technologie zoals SSL-VPN en IPsec, zie ENC N-2-2).
5. Bij web gebaseerde applicaties wordt de gegevensuitwisseling tussen de applicatieserver (in een kritische computerruimte) en de werkplek encrypt. Niet web-gebaseerde applicaties kunnen vooralsnog niet encrypt communiceren, tenzij het om bijzonder vertrouwelijke gegevens gaat. Dan moet er wel altijd encrypt worden (zie ENC N-1-2). Ook vertrouwelijke gegevens uitgewisseld tussen servers binnen kritische computerruimtes hoeft niet encrypt te worden. Doordat het servernetwerk gescheiden is van het netwerk met werkstations (zie BP N-2-1), is het servernetwerk feitelijk een netwerk binnen een kritische computerruimte.
6. De datacommunicatie bij mobiele toepassingen (waarbij veelal sprake is van een radiografische verbinding) is encrypt, waarbij het ontwerp van de encryptieoplossing aan een risicoanalyse is onderworpen.
7. Draadloze datacommunicatie gebaseerd op een wireless LAN (gebaseerd op de WIFI standaard IEEE 802.11) wordt bij de Belastingdienst vooralsnog niet toegepast. De sterkte van de encryptiemogelijkheden worden momenteel als onvoldoende beschouwd, ten opzichte van de eenvoud waarmee de radiografische datacommunicatie opgevangen kan worden.

Norm

ENC N-1-2	Bijzonder vertrouwelijke gegevens worden altijd door encryptie beschermd.
-----------	---

Toelichting

Bijzonder vertrouwelijke gegevens zijn gegevens die meer vertrouwelijk zijn dan de doorsnee vertrouwelijke gegevens, omdat bij een inbreuk de gevolgen meer verstrekkend zijn. Voorbeelden van bijzonder vertrouwelijke gegevens zijn wachtwoorden, personeelsvertrouwelijke gegevens, gegevens van vertrouwenspersonen, gegevens van FIOD-ECD. De reden om bijzonder vertrouwelijke gegevens ook binnen kritische ruimte te beschermen is dat de reeds getroffen beveiligingsmaatregelen onvoldoende beschermen tegen onbevoegd raadplegen en muteren, bijvoorbeeld door beheerders. Let op: Encryptie biedt geen extra waarborg voor de beschikbaarheid (denk aan het blokkeren van transport of verwijderen van opgeslagen gegevens).

Maatregelen

1. Het ICT-systeem biedt de mogelijkheid om bijzonder vertrouwelijke gegevens selectief te encrypten. Doordat gegevens niet voorzien zijn van een label volgens een classificatiesysteem, wordt het automatisch selectief toepassen van encryptie behalve voor wachtwoorden, NIET door het systeem ondersteund; het is de verantwoordelijkheid van de eigenaar van de gegevens om te bepalen of encryptie wordt toegepast.
2. Wachtwoorden worden altijd encrypt opgeslagen of verstuurd. Dit geldt nadrukkelijk ook bij het aanmelden op een systeem, het wijzigen van een wachtwoord en het opslaan van een wachtwoord in een wachtwoordbestand. Indien in een berichtenstroom de wachtwoorden niet selectief encrypt kunnen worden, dan wordt de gehele stroom encrypt (bijvoorbeeld bij een Telnet-sessie).
3. Binnen het filesysteem van de PC-omgeving (PC-servers, Desktop PC en Portable PC's) kunnen opgeslagen bestanden of mappen met bestanden (directories) selectief encrypt worden.
4. Binnen de kantooromgeving kunnen uit te wisselen bestanden selectief encrypt worden (momenteel e-mail berichten binnen Lotus Notes en PC-bestanden door Winzip met sterk wachtwoord en AES 256 algoritme, zie ook ENC N-2-2 en ENC N-2-3).
5. Een compartiment (binnen een zone, zie ook BP R-2) met overwegend bijzonder vertrouwelijke gegevens wordt uitsluitend ontsloten via een encrypte netwerkverbinding.

2.3.3 Waaraan moet de encryptie voldoen?

Richtlijn

ENC R-2	De sterkte van de encryptie is in overeenstemming met de waarde en de vertrouwelijkheid van de te beschermen gegevens.
---------	--

Risicoafweging

Indien de encryptie onvoldoende sterk is, kunnen onbevoegden toegang krijgen tot vertrouwelijke en waardevolle gegevens, waardoor inbreuk kan plaats vinden op de vertrouwelijkheid en de integriteit van de gegevens. Alle encryptie is theoretisch te kraken, maar praktisch is dat alleen rendabel indien de encryptie zwak is. Bij sterke encryptie zijn de kosten voor het kraken hoger dan de informatiewaarde van de gegevens die een kraak oplevert. Sterke encryptie wordt bereikt door het gebruik van betrouwbare cryptografische producten (zie ENC N-2-1), robuuste algoritmen (zie ENC N-2-2) en voldoende lange cryptografische sleutels (zie ENC N-2-3).

Norm

ENC N-2-1	Gebruikte cryptografische producten zijn door een onafhankelijke partij volgens algemeen aanvaarde standaards gecertificeerd.
-----------	---

Toelichting

Een door de leverancier overlegd certificaat dat een cryptografisch product aan algemeen aanvaarde standaards voldoet biedt dit een duidelijke meerwaarde. Het incorrect implementeren van standaards en algoritmen in cryptografische producten kan namelijk grote gevolgen voor de sterkte van de encryptie hebben.

Maatregelen

1. Leveranciers eigen oplossingen zijn toegestaan voor zover deze gebruik maken van algemeen aanvaarde algoritmen. De toepassing van proprietary algoritmen is niet toegestaan.
2. Smartcardproducten zijn gecertificeerd volgens FIPS 104-2.
3. Hardware Security Module producten zijn gecertificeerd volgens FIPS 104-3, of Common Criteria EAL 4 of hoger met een HSM protection profile.

Norm

ENC N-2-2	Gebruikte cryptografische algoritmen staan bekend als standaard en robuust.
-----------	---

Toelichting

Er zijn veel algoritmen die veelal onderdeel zijn van een standaard. Een standaard kent een eigen techniek en toepassing. In de maatregelen wordt beschreven wanneer welke techniek en standaard toegepast moet worden en welke algoritmen hier voor gebruikt kunnen worden. In de loop der jaren worden vaak zwaktes in algoritmen bekend. Deze algoritmen mogen dan niet meer gebruikt worden. De maatregelen in dit voorschrift houden hier rekening mee. Zo nodig wordt het voorschrift geactualiseerd.

Maatregelen

1. Bij de keuze op welk niveau bij datacommunicatie encryptie en decryptie plaatsvindt, gelden de volgende overwegingen:
 - a. Encryptie op applicatieniveau wordt toegepast indien onweerlegbaarheid van de communicatie nodig is;
 - b. Encryptie op transportniveau vindt plaats indien er binnen een sessie verschillend geclassificeerde gegevens worden uitgewisseld. Het deel van de sessie waarbinnen vertrouwelijk geclassificeerde gegevens worden uitgewisseld vindt dan encrypt plaats en het publieke deel van een sessie kan unencrypt plaats vinden;
 - c. encryptie op netwerkniveau vindt plaats indien alle verkeer encrypt plaats moet vinden;
 - d. encryptie op link-niveau (zoals encryptiemodems) worden niet toegepast, vanwege het problematische sleutelbeheer.

2. Encryptie van sessies (delen van sessies) vindt minimaal plaats op basis van SSL v2 en zo mogelijk met SSL v3 of TLS 1.0.
3. Beheersessies over het Belastingdienst netwerk worden encrypt met encryptievoorzieningen binnen Patrol, Kerberos, SSL of SSH.
4. Beheersessies die over een publiek netwerk lopen worden encrypt met een SSL-VPN.
5. Opgeslagen wachtwoorden worden door een one-way hashing algoritme encrypt (zie ENC N-1-2). Daardoor kunnen wachtwoorden in een wachtwoordbestand niet decrypt worden.
6. Persoonlijke mappen binnen de PC-NU omgeving (PC-server en PC-werkplekken) waarin bestanden worden opgeslagen met bijzonder vertrouwelijke gegevens (zie ENC N-1-2) kunnen optioneel (te beoordelen door de gebruiker) gebruik maken van het Encrypted File System van het besturingsstelsel.
7. Intern verzonden e-mail bestanden met bijzonder vertrouwelijke gegevens (zie ENC N-1-2) kunnen optioneel (te beoordelen door de gebruiker) encrypt worden (momenteel door standaard functionaliteit binnen Lotus Notes).
8. Door systeemfouten mag de encryptie niet uitgeschakeld of gecompromitteerd worden (bijvoorbeeld de cryptografische sleutel prijsgeven).
9. Het toepassen van encryptie mag niet leiden tot verstoringen binnen ICT-systemen of het beheer onmogelijk maken. Denk hierbij bijvoorbeeld aan diskfragmentatie, antivirus programmatuur en controle binnen de e-service zone (zie ook BP N-1-2).
10. Er worden alleen algoritmen gebruikt die bekend staan als veilig.
11. Voor nieuwbouw systemen kunnen onder meer de volgende algoritmen gebruikt worden:
 - a. SHA-256;
 - b. RSA;
 - c. AES.
12. In bestaande systemen mogen daarnaast onder meer gebruikt worden:
 - a. SHA-1 of MD5;
 - b. 3DES.
13. Niet gebruikt mogen worden:
 - a. MD4;
 - b. DES;
 - c. PKZIP;
 - d. Wachtwoord beveiliging in MS-Office.

Norm

ENC N-2-3	De sleutellengte is zo gekozen dat het praktisch onmogelijk is een cryptografische sleutel te raden.
-----------	--

Toelichting

De lengte van cryptografische sleutels wordt uitgedrukt in bits. Hoe langer een sleutel, hoe meer mogelijke waarden een cryptografische sleutel kan aannemen. De kans dat een cryptosleutel geraden wordt is dan kleiner. Cryptosleutels kunnen achterhaald worden door alle combinatorische mogelijkheden uit te proberen. Dit vergt echter veel rekenkracht. De lengte van de cryptosleutels kan zo gekozen worden dat het vele jaren rekenwerk op de snelste computer vergt voordat een cryptosleutel achterhaald wordt. De in dit voorschrift gegeven sleutellengtes zullen wanneer nodig geactualiseerd worden, omdat computers sneller en goedkoper worden en daarmee de benodigde rekenkracht meer algemeen beschikbaar komt.

Maatregelen

1. In de ICT-systemen is de gebruikte sleutellengte parametrizeerbaar.
2. De sleutellengte van symmetrische algoritmen is ten minste 256 bits.
3. Bij nieuwbouw is de sleutellengte van asymmetrische algoritmen ten minste 2048 bits.
4. In bestaande systemen is de sleutellengte van asymmetrische algoritmen ten minste 1024 bits.

2.3.4 Hoe moet het sleutelbeheer geregeld worden?

Richtlijn

ENC R-3	De exclusiviteit van cryptografische sleutels is gewaarborgd.
---------	---

Risicoafweging

Encryptie berust op het principe dat uitsluitend met de juiste cryptografische sleutel een bericht decrypt kan worden. Heeft een onbevoegde de beschikking over de cryptografische sleutel dan kan de integriteit en vertrouwelijkheid van een bericht geschaad worden. Daarom moeten cryptografische sleutels beschermd worden tegen onbevoegde kennisname.

Bij asymmetrische encryptie hoeft alleen de private key strikt vertrouwelijk te blijven, terwijl de public key, publiek bekend gemaakt kan worden. Indien de private key bekend wordt, dan kan iemand anders zich uitgeven voor de eigenaar van de private key, berichten elektronisch ondertekenen als de eigenaar van de private key en berichten lezen die exclusief voor de eigenaar van de private key zijn.

Hoewel de vertrouwelijkheid van de publieke sleutel niet gewaarborgd hoeft te worden, is het wel van belang dat de authenticiteit van de eigenaar van de publieke sleutel gewaarborgd wordt. Deze waarborg wordt veelal door een derde onafhankelijke partij verschaft door middel van een elektronisch certificaat. Bij gecorrumpeerde certificaten kan de vertrouwelijkheid en de integriteit van gegevens geschaad worden. De vertrouwelijkheid kan geschaad worden doordat gegevens verstrekt worden aan een onrechtmatige partij. De integriteit kan geschaad worden doordat gegevens geaccepteerd en verwerkt worden als ware de gegevens afkomstig van een rechtmatige partij.

Sleutelbeheer verdient allereerst aandacht tijdens de generatie, transport en opslag van de sleutels. Dit is uit gewerkt in de norm ENC N-3-1. Daarnaast is de kans op corrupte cryptosleutels en certificaten te verkleinen door de geldigheidsduur te beperken en deze geldigheidsduur te controleren. Dit is uitgewerkt in de norm ENC N-3-2.

Norm

ENC N-3-1	De exclusiviteit van cryptografische sleutels is gewaarborgd tijdens de generatie, transport en opslag van de sleutels.
-----------	---

Toelichting

Het ICT-systeem mag cryptografische sleutels niet prijsgeven, anders is de encryptie van gegevens te doorbreken. Daarom moeten er maatregelen genomen worden bij de generatie, transport en opslag van cryptosleutels.

Maatregelen

1. PKI certificaten (onder andere gebruikt bij SSL) zijn gebaseerd op de standaard X.509 v3. Deze worden uitgegeven via het SSL-loket (onderdeel van Serviceteam Beveiliging binnen de sector Continuïteit).
2. Voor testdoeleinden gebruikte cryptografische sleutels en certificaten blijven beperkt tot het gebruikt binnen de testomgeving.
 - a. Cryptografische sleutels en certificaten worden bij in productie name opnieuw gegenereerd.
 - b. Voor testdoeleinden genereert het SSL-loket zelf certificaten (self-signed certificaten).
 - c. Certificaten voor productiedoeleinden worden door het SSL-loket afgenomen bij een vertrouwde derde partij.
3. Cryptografische sleutels en certificaten worden uitgegeven en beheerd conform de standaard PKCS#11
4. Er wordt zo mogelijk gebruik gemaakt van een sessiesleutel. Een sessiesleutel is uniek voor een sessie. Deze sleutel wordt random gegenereerd, is bij voorkeur symmetrisch en wordt bij voorkeur uitgewisseld met een asymmetrisch algoritme.

5. Generatie en installatie van een private keys, master keys en root certificates vinden plaats binnen een beschermende omgeving van cryptohardware.
6. Deze cryptohardware is tamper-resistant. Dit betekent dat er bijzondere voorzieningen zijn getroffen tegen onbevoegde kennisname van de opgeslagen cryptosleutels bij een fysieke inbreuk op de hardware.
7. Interactieve bediening van cryptohardware vindt plaats onder een vier ogen principe. Denk hierbij aan installatie, wijzigingen in configuratie en generatie van master keys.
8. Generatie van PKI-client sleutelparen vindt plaats op de client (veelal de PC van de gebruiker). Door client-side generatie hoeft de private key niet van een server overgebracht te worden naar de client.
9. Bij het ondertekenen (het waarborgen van integriteit en onweerlegbaarheid) en het encrypten (het waarborgen van de vertrouwelijkheid) van berichten worden verschillende sleutelparen gebruikt. Voor authenticatiedoeleinden hoeft geen separaat sleutelpaar te worden gegenereerd. Hiervoor mag het sleutelpaar voor ondertekening gebruikt worden.

Norm

ENC N-3-2	De geldigheid van certificaten en cryptografische sleutels wordt gewaarborgd.
-----------	---

Toelichting

Certificaten worden gebruikt bij cryptografische toepassingen gebaseerd op een PKI om de publieke sleutel te distribueren. Deze certificaten worden uitgegeven door een Certificate Service Provider (CSP). De entiteit binnen de CSP die verklaart dat een publieke sleutel in het certificaat tot de houder van het certificaat behoort heet Certification Authority.

Maatregelen

1. Cryptografische sleutels en certificaten die de Belastingdienst gebruikt en accepteert kennen een geldigheidstermijn van 1 jaar.
2. De Belastingdienst controleert van ontvangen certificaten de geldigheidsdatum en of de certificaten voorkomen op een Certification Revocation List.
3. In het ontwerp wordt de noodzaak om cryptografische sleutels en certificaten tijdig te vernieuwen onder de aandacht gebracht (Dit verlengen gebeurt door het Serviceteams Beveiliging).
4. Certificaten zijn ondertekend door een geaccrediteerde Certification Authority conform de voorwaarden in de wet elektronische handtekening (zie de internetsite van de OPTA voor een actuele lijst van geaccrediteerde Certificate Service Providers).
5. Bij het verwijderen van een machine uit de productie omgeving dienen alle cryptosleutels gewist te worden. Ook dient het certificaat te worden ingetrokken.

2.4 Boundary Protection**2.4.1 Wat is boundary protection?**

Boundary protection is het containerbegrip voor beveiligingsmaatregelen die op een grensvlak worden genomen om die grens te handhaven. Meestal gaat het bij boundary protection om het scheiden van netwerken die een verschillende eigenaar of beveiligingsniveau hebben. Boundary protection is van belang op die plaatsen waar (netwerk)koppelingen bestaan tussen de verschillende netwerken.

Boundary protection beschermt tegen bedreigingen zoals:

- denial of service attacks;
- indringers;
- ongewenste "content";
- heimelijke programmatuur, zoals virussen.

Voor het realiseren van boundary protection kan gebruik gemaakt worden van een variëteit aan technieken, bijvoorbeeld firewalling, intrusion detection en content scanning. Binnen de Belastingdienst komt boundary protection voor op het koppelvlak tussen de Belastingdienst en haar omgeving (zie BP R-1) en ten behoeve van het realiseren van zones en compartimenten binnen de Belastingdienst (zie BP R-2).

2.4.2 Hoe moeten externe verbindingen worden beveiligd?

Richtlijn

BP R-1	<i>Externe verbindingen worden gelegd via een centraal en gecontroleerd koppelvlak.</i>
--------	---

Risicoafweging

Controle op externe verbindingen is essentieel om te voorkomen dat gegevens van de Belastingdienst naar buiten lekken, waardoor de vertrouwelijkheid geschaad kan worden. Daarnaast moet voorkomen worden dat onbevoegden gegevens op ICT-systemen van de Belastingdienst kunnen plaatsen of de werking van deze systemen kunnen beïnvloeden, waardoor de integriteit en beschikbaarheid geschaad kan worden. Door de koppeling en de controle centraal in te richten is de beveiliging beter te waarborgen.

De controle op het koppelvlak bestaat uit:

- het controleren welke verbindingen er worden gelegd (ongewenste verbindingen worden geblokkeerd, zie BP N-1-1);
- het inhoudelijk controleren van de gegevens die worden uitgewisseld (ongewenste inhoud wordt geblokkeerd, zie BP N-1-2).

Norm

BP N-1-1	Een koppeling met een extern netwerk is in een ontwerp gespecificeerd en wordt uitsluitend gelegd via de e-service zone.
----------	--

Toelichting

Binnen de e-service zone is een centraal koppelvlak ingericht om veilig te kunnen koppelen met externe netwerken. Dit koppelvlak wordt het e-fundament genoemd. Het voorziet in business areas om toepassingen te hosten die gebruikt worden door belastingplichtigen, andere relaties van de Belastingdienst en belastingdienstmedewerkers die via een extern netwerk contact leggen met het interne belastingdienstnetwerk. Binnen het e-fundament is er een filter geïmplementeerd waarmee ongewenste verbindingen geblokkeerd kunnen worden. Van een connectie moet exact gespecificeerd worden via welke componenten, welke poorten en welke adressen een connectie gelegd wordt. Alleen op basis van deze gegevens wordt een filter opgezet.

Maatregelen

1. Het interne belastingdienstnetwerk of ICT-systeem aangesloten op dit interne netwerk worden nooit rechtstreeks gekoppeld met externe systemen of netwerken. Een koppeling verloopt altijd via een sessieonderbreker die gepositioneerd is binnen de e-service zone.
2. Encrypte gegevensstromen worden decrypt binnen de e-service zone zodat gegevenstromen inhoudelijk gecontroleerd kunnen worden (zie BP N-1-2).
3. In principe mogen er binnen de e-service zone uitsluitend openbare gegevens opgeslagen worden en nooit vertrouwelijke gegevens. Indien er toch vertrouwelijke gegevens worden opgeslagen dienen er aanvullende maatregelen getroffen te worden (zoals host intrusion detectie).
4. In het ontwerp wordt gespecificeerd hoe de connectie via het e-fundament wordt gelegd. Specificatie vindt plaats conform de "Ontwikkelrichtlijnen en aansluitvoorwaarden GI Poort" die te verkrijgen zijn via de ICT-Servicebeheerder NTGS. Onder meer wordt aangegeven via welke componenten binnen het e-fundament, via welke poorten en van/naar welke ip-adressen de connectie wordt gelegd.

Norm

BP N-1-2	Gegevensuitwisseling wordt geautomatiseerd inhoudelijk gecontroleerd, waarbij ongewenste gegevens worden geblokkeerd.
----------	---

Toelichting

Naast filtering op het tot stand brengen van verkeersstromen (zie BP N-1-1) en autorisatie voor het mogen uitwisselen van gegevens via randapparatuur (zie IAM N-3-1) wordt binnen een tot stand gebrachte connectie de ongewenste gegevens geblokkeerd. Dit is een inhoudelijk filter. Geblokkeerd wil hierbij zeggen dat ongewenste gegevens (zoals virussen, spam en niet ondersteunde berichtformaten) in ieder geval niet worden doorgelaten. Voor incidentrespons en diagnosedoeleinden kunnen gegevens wel in quarantaine geplaatst worden.

Een algemeen beveiligingsprincipe is dat er een meerlaagse verdedigingslinie wordt ingevuld (defence in dept). Het doorbreken van een verdedigingslinie kan dan verderop in de keten van systemen en op een ander tijdstip opgevangen worden. Indien bijvoorbeeld de virusscanner binnen de e-service Zone een nieuw virus doorlaat (omdat er nog geen patroon voor het virus beschikbaar is), dan kan een aanvullende virusscanner binnen de datacenter zone op een later tijdstip (wanneer het patroon intussen bekend is), een virus alsnog herkennen en onschadelijk maken. Ook kunnen gelijksoortige beveiligingsproducten aanvullend op elkaar werken door verschillende leveranciers te kiezen. Een tweede product controleert daarbij het eerste product op de goede werking.

Maatregelen

1. Ongewenste gegevensuitwisseling via externe e-mail (via de e-service zone) wordt voorkomen. Hierbij geldt het volgende:
 - a. e-mail berichten met bijlagen worden uitsluitend doorgelaten indien het formaat van de bijlage voorkomt op een lijst met toegestane bijlagen (whitelist). Het formaat van een bijlage wordt door een inhoudelijke inspectie van de bijlage vastgesteld en dus niet afgeleid van de bestandsextensie;
 - b. er is antivirusprogrammatuur actief die e-mail berichten blokkeert met kwaadaardige code (virussen, wormen, trojans, spyware, etc) in zowel ontvangen als verzonden e-mails. Gecomprimeerde bestanden en macro's in documenten worden daarbij ook geïnspecteerd. De gebruikte antivirusprogrammatuur werkt op basis van zowel bekende viruspatronen als op basis van heuristische zoekalgoritme. Een update van antivirusdefinities vindt tenminste ieder uur geautomatiseerd plaats;
 - c. aan een verzonden e-mail bericht wordt een standaard disclaimer toegevoegd. Hierin is opgenomen dat de Belastingdienst e-mail NIET voor officiële mededelingen gebruikt.
 - d. e-mail berichten met een buitensporige grote omvang worden geweerd (momenteel berichten groter dan 2MB);
 - e. er is een (spam) filter geactiveerd voor zowel ontvangen als verzonden berichten. Het filter kan berichten weren op basis van herkomst, berichtonderwerp en het voorkomen van bepaalde woorden in het bericht. Filtering vindt plaats op basis van zowel een door de Belastingdienst onderhouden blacklist als van een blacklist van een leverancier. Een update van het spam filter vindt ten minste ieder uur geautomatiseerd plaats.
2. Op de interne mailservers (momenteel Lotus Domino-servers) is antivirusprogrammatuur resident actief. Deze virusscanner is orthogonaal aan de antivirusprogrammatuur gebruikt binnen de e-service zone. Een update van antivirusdefinities vindt dagelijks geautomatiseerd plaats.
3. Op alle PC-werkplekken is antivirusprogrammatuur resident actief is. Een update van virusdefinities en/of antivirusprogrammatuur kan op ieder moment (handmatig) uitgevoerd worden en vindt ten minste wekelijks geautomatiseerd plaats.
4. Alle PC-servers worden ten minste één keer per week geautomatiseerd gecontroleerd op virussen, nadat een update van de virusdefinities en/of antivirusprogrammatuur geautomatiseerd plaats heeft gevonden. De controle moet op ieder gewenst tijdstip ook handmatig gestart kunnen worden.

5. Al het gegevensverkeer door de e-service zone wordt inhoudelijk geïnspecteerd op inbraakpogingen door een standaard hulpmiddel voor Intrusion Detection and Prevention (momenteel van de leverancier Juniper). Hierbij geldt het volgende:
 - a. het IDP hulpmiddel is in-line geplaatst, dat wil zeggen dat alle verkeerstromen real-time geanalyseerd kunnen worden en dat real-time actie ondernomen kan worden op mogelijke aanvallen;
 - b. in het ontwerp wordt gespecificeerd welk IDP hulpmiddel (in welke grensbescherming) waarop (richting verkeer, ip-adressen, protocol, applicatieversie, etc) moet filteren conform de "Ontwikkelrichtlijnen en aansluitvoorwaarden GI Poort" die te verkrijgen zijn via de ICT-Servicebeheerder NTGS. De IDP-regels worden getuned door de daarvoor verantwoordelijk beheerders (van de sector exploitatie);
 - c. een update van de repository met aanvalspatronen vindt geautomatiseerd minimaal dagelijks plaats.

2.4.3 Welke zonering en compartimentering moet worden toegepast?

Richtlijn

BP R-2	<i>Compartimentering van ICT-systemen voorkomt dat beveiligingsincidenten uitbreiden naar de gehele infrastructuur van de Belastingdienst.</i>
--------	--

Risicoafweging

De normen en maatregelen onder deze richtlijn zijn schadebeperkend. De impact van een inbreuk op de beveiliging van een ICT-systeem wordt beperkt tot het compartiment waarbinnen het ICT-systeem is opgenomen. Zonder compartimentering kan een inbreuk op de beschikbaarheid, de integriteit en de vertrouwelijkheid zich uitstrekken tot alle verbonden ICT-systemen.

De noodzaak tot compartimentering van ICT-systemen komt mede voort uit verschillen in beveiligingseisen die gesteld zijn aan systemen in verschillende fasen van systeemontwikkeling. In het HIB CICT wordt onderscheid gemaakt in systemen in ontwikkeling, acceptatie en productie. Hierin worden eisen gesteld aan de wijze waarop werkzaamheden verricht dienen te worden.

Te noemen proceseisen zijn:

- Werkzaamheden tijdens ontwikkeling, acceptatie en operatie van ICT-systemen zijn gescheiden en de overdracht van gegevens en programmatuur tussen deze werkzaamheden vindt gecontroleerd plaats. Daarnaast wordt het operationeel beheer verricht vanuit een separate omgeving (HIB CICT Alg N-1-1);
- programmatuur in de acceptatietest- en productieomgeving mag niet gewijzigd worden (zie HIB CICT O&B N-1-2);
- er mogen geen persoonsgebonden productiegegevens gebruikt worden binnen de ontwikkelomgeving (zie HIB CICT O&B N-2-1 en HIB CICT Ex N-3-4);
- er wordt onderscheid gemaakt tussen programmatuur binnen de ontwikkel-, acceptatietest- en productieomgeving (zie HIB CICT O&B N-2-2);
- overdracht van programmatuur tussen deze omgevingen vindt gecontroleerd plaats (zie HIB CICT O&B N-1-3, HIB CICT O&B N-2-2 en HIB CICT Ex N-1-1).

In het VBI worden geen proceseisen maar wel producteisen uitgewerkt. Hier wordt ingegaan op:

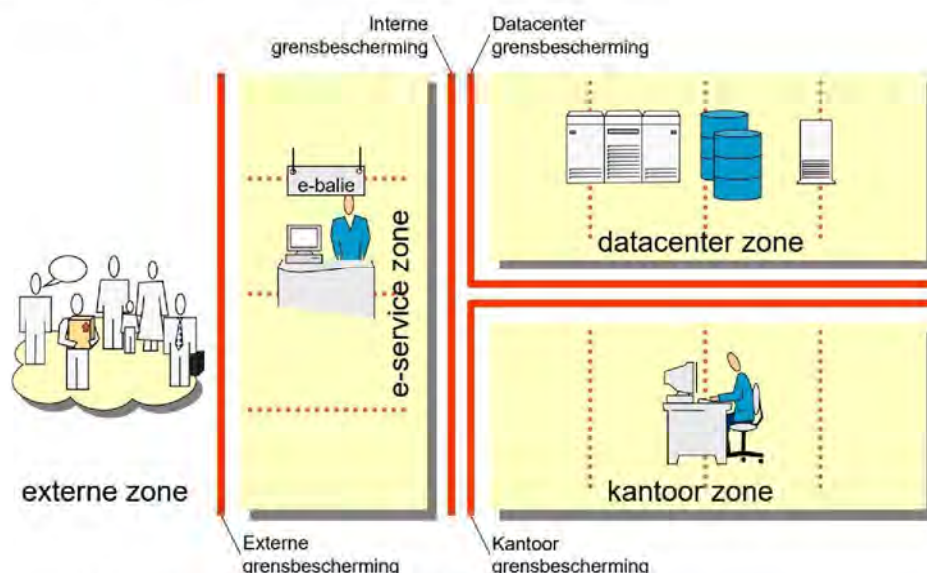
- welke zones en compartimenten gescheiden moeten worden (BP N-2-1);
- de wijze waarop de scheiding in de techniek wordt afgedwongen (BP N-2-2).

Norm

BP N-2-1	Een ICT-systeem wordt op grond van het beveiligingsniveau gepositioneerd bij systemen in een zone en een compartiment met een vergelijkbaar beveiligingsniveau.
----------	---

Toelichting

Het verschil in beveiligingsniveau van de diverse zones heeft vooral te maken met kwetsbaarheid van systemen. Systemen die in contact staan met onvertrouwde systemen zijn meer kwetsbaar dan systemen die uitsluitend een connectie hebben met een vertrouwde systemen. Het verschil in beveiligingsniveau van compartimenten heeft onder meer betrekking op de zekerheid dat een ICT-systeem naar behoren werkt. In de productieomgeving bevinden zich alleen ICT-systemen waarvan de goede werking door acceptatietesten zijn bewezen. In de acceptatietestomgeving wordt getest of het systeem naar behoren werkt. Er bestaat dus nog geen zekerheid over de juiste werking, wel ligt de functionaliteit vast. In een ontwikkelomgeving wordt de functionaliteit van systemen gewijzigd en worden fouten hersteld.



Figuur 6: Zonering en compartimentering

Figuur 6 geeft globaal gehanteerde zonering en compartimentering van de infrastructuur van de Belastingdienst weer. Zones worden gerealiseerd door grensbescherming, aangeduid met een doorgetrokken rode streep. Binnen een zone bestaan compartimenten. Een compartimentgrens is aangeduid met een rode onderbroken streep.

Maatregelen

1. In de exploitatietopologie van een ontwerp worden de (deel)systemen gepositioneerd in de bestaande zonering en compartimentering.
2. De volgende zonering geldt:
 - a. In de externe zone worden systemen gepositioneerd die buiten de gebouwen van de Belastingdienst staan;
 - b. het ontwikkelen en afstellen van technische systemen vindt plaats in een fysiek gescheiden (lab) omgeving en dat binnen de externe zone wordt gepositioneerd;
 - c. in de e-service zone worden servers gepositioneerd die binnen de Belastingdienst staan en een connectie met de externe zone hebben;
 - d. werkstations aangesloten op een Local Area Network (LAN) binnen een gebouw van de Belastingdienst worden gepositioneerd binnen de kantoorzone;
 - e. mobiele clients en werkstations die zich bevinden buiten een kantoor van de Belastingdienst worden gepositioneerd in de externe zone;
 - f. in de datacenter zone worden de servers gepositioneerd die uitsluitend benaderbaar zijn vanuit kantoorzone of de e-service zone.

3. Bij compartimentering binnen een zone wordt het volgende in acht genomen:
 - a. Compartimenten binnen een zone worden gescheiden op basis van V-LAN technologie;
 - b. gemeenschappelijke systemen worden in een compartiment voor gemeenschappelijke systemen gepositioneerd (denk bijvoorbeeld aan mail-servers);
 - c. systemen kunnen in een separaat compartiment (een eigen business area) worden opgenomen indien zij niet communiceren met andere compartimenten binnen dezelfde zone of alleen met systemen in het gemeenschappelijke compartiment van de zone;
 - d. systemen in de fase systeemontwikkeling, acceptatietest en productie worden door in specifiek daarvoor (reeds) ingerichte gescheiden compartimenten opgenomen.
 - e. Systemen met overwegend bijzonder vertrouwelijke gegevens (denk aan systemen van FIOD-ECD, zie ook ENC N-1-2), worden in een eigen compartiment binnen de datacenter zone gepositioneerd. Dit compartiment, ook wel aangeduid als restricted business area, wordt in een fysiek gescheiden LAN aangesloten op de grensbescherming van de datacenter zone. Dit compartiment wordt dus in tegenstelling tot andere compartimenten niet gescheiden op basis van V-LAN technologie.

Norm

BP N-2-2	De communicatie tussen zones en compartimenten is tot het minimaal noodzakelijke beperkt.
----------	---

Toelichting

De communicatie tussen zones en compartimenten is risicovol omdat het gaat om systemen met een verschillend beveiligingsniveau. De systemen met een verschillend beveiligingsniveau zijn immers in verschillende zones en compartimenten geplaatst (Zie BP N-2-1). Het risico bestaat dat de zone en compartiment met een hoger beveiligingsniveau degradeert tot het beveiligingsniveau van de zone of compartiment met het lagere beveiligingsniveau.

Maatregelen

1. Koppelingen tussen zones en compartimenten zijn in het ontwerp uitgewerkt, waarbij de richting en de poorten (systeemservices) waarover gecommuniceerd worden, exact worden benoemd.
2. In de Access Control Lists van Routers zijn werkstations (in een compartiment van de kantoorzone) gekoppeld aan een servers (in een compartiment van de datacenter zone) op basis van IP-nummers. Hierbij geldt het volgende:
 - a. Werkstations kunnen onderling nooit rechtstreeks met elkaar communiceren;
 - b. servers binnen eenzelfde compartiment kunnen wel rechtstreeks met elkaar communiceren;
 - c. server-naar-server communicatie over compartimentgrenzen heen verloopt via de grensbescherming van de zone;
 - d. werkstations kunnen aan gemeenschappelijke servercompartimenten gekoppeld worden (voor gemeenschappelijke services zoals SAP, Lotus Notes, e.d.) en verder uitsluitend aan één specifiek compartiment (een koppeling met gelijktijdig systemen in compartimenten voor ontwikkeling, acceptatietest en productie is dus uitgesloten).
3. Zonering en compartimentering wordt ingericht met uitsluitend hardend componenten (de functionaliteit van de componenten is beperkt tot uitsluitend die functionaliteit die absoluut nodig is).

2.5 Business Continuity

2.5.1 Wat is business continuity?

De Belastingdienst is dermate afhankelijk geworden van ICT, dat wanneer ICT-systemen uit de lucht zijn de bedrijfsvoering praktisch stil ligt. Om de continuïteit van de bedrijfsprocessen veilig te stellen is het daarom noodzakelijk dat ICT-systemen robuust zijn. Incidenten kunnen dan opgevangen worden (denk bijvoorbeeld aan noodstroomvoorziening). Bij grote incidenten zoals overstromingen, uitslaande brand, aardbeving spreken wordt de term calamiteit gebruikt. Om adequaat te reageren op calamiteiten worden draaiboeken ontwikkeld en periodiek getest. Het VBI gaat daar verder niet op in. Wel gaat het VBI in op de technische infrastructuur die vooraf ingericht moet zijn (denk bijvoorbeeld aan uitwijksystemen en datacommunicatie), om conform de calamiteitendraaiboek de systemen waarvoor dat noodzakelijk wordt geacht weer snel beschikbaar te maken.

2.5.2 Hoe moet de continuïteit van ICT-systemen worden gewaarborgd?

Richtlijn

BC R-1	<i>Er zijn technische voorzieningen getroffen om de beschikbaarheid van ICT-systemen te waarborgen conform het niveau dat vastgelegd is het programma van eisen.</i>
--------	--

Risicoafweging

Het risico bestaat dat als gevolg van incidenten of calamiteiten er verstoringen optreden in de beschikbaarheid van ICT-systemen. Indien een ICT-systeem niet beschikbaar is kan de continuïteit van het bedrijfsproces dat door het ICT-systeem wordt ondersteund in gevaar komen. Om dit risico op te vangen kan de gebruikersorganisatie maatregelen treffen om discontinuïteit van ICT-systemen op te vangen. Vaak is dit echter niet mogelijk, vanwege de grote afhankelijkheid van ICT-systemen. Anders gezegd, de Belastingdienst zal in dat geval zonder ICT-systemen niet kunnen functioneren. De eisen die de klant-opdrachtgever stelt aan de beschikbaarheid van ICT-systemen zijn vastgelegd in een programma van eisen (zie HIB AM N-1-1 en later wordt dit ook vastgelegd in de service niveau overeenkomst zie HIB AM N-1-3).

Om de continuïteit van ICT-systemen te garanderen dient er afhankelijk van de klanteisen infrastructuur ingericht te worden:

- om te voorkomen dat systemen onbeschikbaar worden (zie BC N-1-1);
- om adequaat te reageren indien zich toch een verstoring voordoet (zie BC N-1-2);
- en om ICT-systemen weer snel operationeel te maken (BC N-1-3).

Norm

BC N-1-1	ICT-systemen worden aangesloten op voorzieningen gericht op het voorkomen van discontinuïteit.
----------	--

Toelichting

Computers hebben stroom nodig, mogen niet te heet worden, kunnen slecht tegen water, kunnen stuk gaan, er kunnen fouten optreden en hebben een gelimiteerde verwerkingscapaciteit. Door voorzorgsmaatregelen te treffen kunnen ICT-systemen minder kwetsbaar voor uitval worden, waardoor voorkomen wordt dat ICT-systemen ongewenst onbeschikbaar worden.

Maatregelen

1. In de exploitatietopologie van het ontwerp wordt apparatuur zoveel mogelijk fysiek geplaatst en aangesloten op voorzieningen binnen kritische ruimten voor het conditioneren van de omgeving (denk aan: noodstroomvoorziening, UPS en spanningstabilisator, klimaatbeheersing, brandblusinstallatie, branddetectiesensoren, waterdetectie).
2. In het ontwerp wordt een afweging gemaakt of de voorzieningen voor het conditioneren van de omgeving voldoende capaciteit hebben om ook het voorliggende systeem te ondersteunen, of dat er wellicht uitbreiding plaats moet vinden. Uitbreidingen worden tijdig aangevraagd.

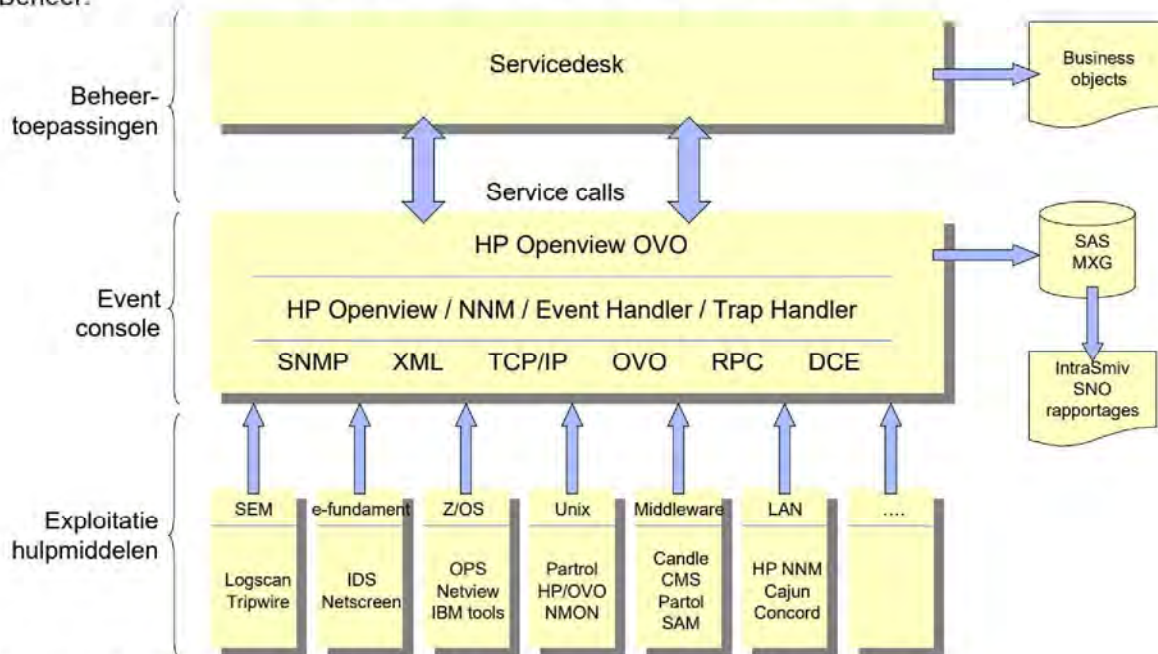
3. Bij de dimensionering van de benodigde capaciteit is rekening gehouden met piekverwerkingen en is een overcapaciteit begroot (denk aan benodigde capaciteit voor schijfruimte, netwerkbelasting, CPU belasting).
4. In het ontwerp worden componenten dubbel uitgevoerd, indien het gewenste beschikbaarheidsniveau hoog of gemiddeld is (denk aan redundante gegevensopslag zoals RAID5 op fileservers en databaseservers, redundante bekabeling tussen rekencentra en regio's).
5. In het ontwerp worden beperkingen opgelegd aan gebruikers en systemen ten aanzien van het gebruik van gemeenschappelijke resources (denk aan CPU-load, netwerkbandbreedte), zodat enkele gebruikers of een systeem niet een overmatig deel van resources kunnen opeisen en daarmee de beschikbaarheid van systemen in gevaar brengen (denk ook aan (D)DOS-aanvallen).

Norm

BC N-1-2	ICT-systemen maken gebruik van voorzieningen die het mogelijk maken om alert en adequaat te anticiperen bij discontinuïteit van ICT-systemen.
----------	---

Toelichting

Helaas zijn storingen nooit helemaal te voorkomen. Daarom worden er exploitatiehulpmiddelen geïmplementeerd om een storing tijdig te signaleren. Al deze signalen worden gerapporteerd aan een centraal punt (het Event Console) van waaruit verdere passende maatregelen genomen worden om de impact van storingen te beperken. Figuur 7 geeft de huidige implementatie van producten en protocollen op dit gebied. Deze figuur is gebaseerd op de Domeinarchitectuur Beheer.



Figuur 7: Exploitatiehulpmiddelen integreren met het Event Console

Maatregelen

1. Er worden standaard voorzieningen geïmplementeerd om de beschikbaarheid van TIS componenten te bewaken. Signalen worden gerapporteerd aan het Event Console (momenteel geïmplementeerd door het product HP Openview). Ook de Security Event Manager (zie ook SM N-2-1) is aangesloten op het Event Console.
2. De drempelwaarde van de capaciteit worden gespecificeerd in het ontwerp. (denk aan: maximale opslagruimte, CPU-load, netwerkbelasting).
3. Het Event Console alarmeert de beheerorganisatie op basis van drempelwaarden en rapporteert periodiek het behaalde service niveau.

Norm

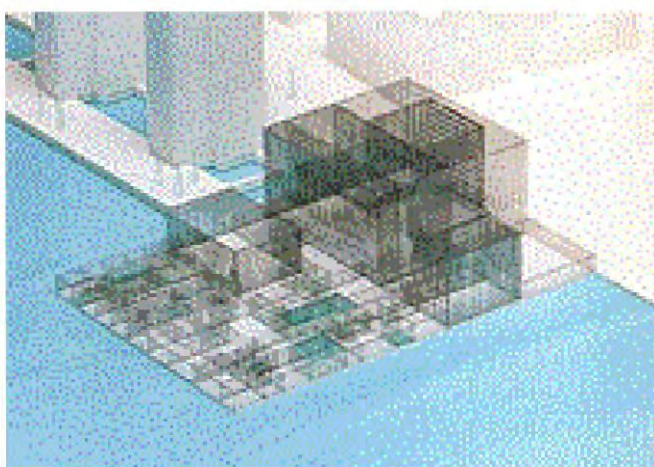
BC N-1-3	Er zijn voorzieningen getroffen om ICT-systemen weer operationeel te maken bij discontinuïteit van ICT-systemen.
----------	--

Toelichting

Allereerst moet voorkomen worden dat gegevens blijvend verloren gaan. Daarnaast moet de tijd dat een storing voort duurt zo kort mogelijk gehouden worden. Maar alles heeft zijn prijs. Ook hier zijn de eisen van de klant-opdrachtgever daarom leidend, mits deze passen in het product- en dienstenaanbod van B/CICT

Maatregelen

1. Er worden routines voor herstart en foutherstel ontworpen en voorzien van een duidelijke handleiding. Het starten van de routine en de acties of correcties die door de routine worden gedaan, worden gelogd (zie ook IAM N-1-1).
2. In het ontwerp wordt aangegeven of het calamiteitenplan van B/CICT (thans belegd bij de serviceteams B/CICT-CO) aangepast moet worden, naar aanleiding van de nieuwbouw of het wijzigen van ICT-services.
3. Voor systemen met hoge beschikbaarheidseisen wordt automatic failover en load balancing ontworpen, waarbij de verwerking gespreid is over twee locaties (momenteel gebouw P en Q, beide in Apeldoorn).
4. Voor systemen met gemiddelde beschikbaarheidseisen zijn in het ontwerp alternatieve (logische) verbindingen ontworpen (denk aan alternatieve routing, back-up inbelverbinding, clusteringtechnologie van servers).
5. De broncode van een standaardpakket komt beschikbaar voor de Belastingdienst indien de leverancier in faillissement verkeert (een escrow regeling maakt deel uit van het eisenpakket bij de selectie van een standaardpakket).
6. Voor alle systemen (met zowel hoog, gemiddelde als lage beschikbaarheidseisen) zijn voorzieningen getroffen voor Backup & Restore van gegevens met een mogelijkheid van Off-site storage. (De voorziening moet dus altijd geregeld worden; alleen de backupfrequentie is afhankelijk van de beschikbaarheidseisen).



VBA: Voorschriften Beveiliging Applicaties

Versie: 1.0

03 mei 2002

Inhoud

0	Documentgegevens	1
0.1	Documenteigenschappen	1
1	Inleiding	2
1.1	Afbakening en relaties	2
1.2	Achtergrond	2
1.3	Minimale beveiligingsmaatregelen	2
2	VBA: Maatregelen in de applicaties	4
2.1	Identificatie & Authenticatie	4
2.2	Autorisatie	5
2.3	Vertrouwelijkheid	6
2.4	Integriteit	7
2.5	Controleerbaarheid	8

0 Documentgegevens**0.1 Documenteigenschappen**

Filenaam	vbia_1.0.doc
Laatste wijziging	3 mei 2002
Aantal pagina's	9
Huidlge status	Final
Versienummer	1.0

1 Inleiding

1.1 Afbakening en relaties

In dit document wordt aangegeven welke maatregelen moeten worden getroffen teneinde aan de eisen ten aanzien van beveiliging te voldoen. Er wordt aangegeven wat op *dit* moment de te treffen maatregelen zijn.

De *eisen* zijn gesteld op 'strategisch' niveau en worden belegd bij B/CPP. De verwachting is dat de eisen niet of nauwelijks aan verandering onderhevig zullen zijn.

De *maatregelen* zijn gesteld op 'tactisch' niveau en zijn vooralsnog bij het B/AC (B/CICT) belegd. Ze zijn dus niet 'operationeel', in die zin dat ze exact voorschrijven welke acties op een bepaald platform of database uitgevoerd moeten worden. De maatregelen zelf zullen ook weinig veranderen in de loop van de tijd.

Infrastructurele maatregelen worden behandeld in Voorschrift beveiliging Infrastructuur (VBI). Applicatieve maatregelen worden behandeld in het Voorschrift beveiliging Applicaties (VBA). Procesmatige maatregelen komen in het Handboek Risicomanagement en het Handboek Informatiebeveiliging Belastingdienst (HIB) aan bod.

Strategisch	Normenkader IB	Eisen
	HIB	eisen, maatregelen (suggesties)
Tactisch	Handboek Risicomanagement	maatregelen (voorschriften) voor processen
	VBA	maatregelen (voorschriften) voor producten
	VBI	
Operationeel	Standaarden zoals Platform Informatiebeveiliging	maatregelen (technisch)
	Configuratiehandboek	

Wanneer in de toekomst de eisen worden uitgebreid of scherper worden gesteld (d.i. hogere beveiligingsniveaus worden geeist) of wanneer nieuwe technologieën beschikbaar komen om andere maatregelen te treffen, dan zal er een nieuwe versie van dit document worden uitgebracht.

1.2 Achtergrond

Vanuit beveiligingsoptiek gelden een aantal uitgangspunten met betrekking tot beveiligingsfunctionaliteit:

- Gebruikers hebben geen last van beveiliging. Dit wil overigens niet zeggen dat beveiliging voor gebruikers onzichtbaar is.
- Applicaties zijn zoveel mogelijk 'security-unaware'. Dit betekent dat de meeste beveiligingsfuncties binnen generieke componenten zullen worden opgenomen.
- Er worden twee beveiligings'domeinen' onderkend: intern, d.w.z. binnen en tussen belastingdienstgebouwen via eigen netwerken, en extern, d.w.z. buiten de muren van de belastingdienst via publieke netwerken. De reden voor dit onderscheid is het ontbreken van fysieke controle mogelijkheden buiten de belastingdienstgebouwen en het lagere beveiligingsniveau van publieke netwerken t.o.v. eigen netwerken.

Concreet betekent dit dat in de komende jaren beveiligingsfuncties beschikbaar gesteld zullen worden vanuit de TIS en/of in de vorm van generieke componenten. De applicatie-ontwikkelaar moet gebruik maken van deze componenten zodra deze beschikbaar zijn. In afwachting van deze componenten moeten applicatieve oplossingen zoveel mogelijk voldoen aan de eisen zoals die aan de te realiseren componenten worden gesteld en zo veel mogelijk losgekoppeld zijn van applicaties om latere migraties te vergemakkelijken.

1.3 Minimale beveiligingsmaatregelen

De in dit hoofdstuk weergegeven maatregelen beschrijven de beveiliging die op dit moment **minimaal** geïmplementeerd moet worden in de TIS-componenten en de applicaties.

De maatregelen voor de TIS zijn uitgewerkt in het VBI 2006. De maatregelen voor de applicaties zijn uitgewerkt in § 2 VBA: Maatregelen in de applicaties. De maatregelen gaan niet in op de wijze waarop de

TIS en applicaties gerealiseerd worden. Dit is uitgewerkt in het Handboek Risicobeheersing. De maatregelen worden geconcretiseerd tijdens het realisatieproces.

Binnen de belastingdienst wordt de indeling in beveiligingsklassen volgens het handboek Informatiebeveiliging Belastingdienst gebruikt.

De onderstaande tabel wordt als referentiekader gezien voor het opstellen van een A&K analyse. Op grond van de gegevensclassificatie is deze tabel geschikt als algemene handreiking. Voor de specifieke toepassing moet uiteraard een zorgvuldige analyse worden gemaakt van de te gebruiken gegevens en processen.

Bev. klasse		Vertrouwelijkheid	Integriteit	Beschikbaarheid
1a	Cryptosleutels	Zeer hoog (essentieel)	zeer hoog (essentieel)	hoog (belangrijk)
1	Beveiligings- en systeemgegevens	Hoog (belangrijk)	zeer hoog (essentieel)	zeer hoog (essentieel)
2a	Gevoelige persoonsgegevens (bijvoorbeeld VIP's)	Hoog	hoog (belangrijk)	Standaard
2	Persoonsgegevens	Standaard (enigszins belangrijk)	standaard (enigszins belangrijk)	Hoog (belangrijk)
3	Vertrouwelijke bedrijfsgegevens	Hoog	standaard	Standaard
4	Interne gegevens	Standaard	standaard	Standaard
5	Openbare gegevens	Geen (ongeclassificeerd)	hoog	Geen (ongeclassificeerd)

Wanneer maatregelen spreken over externe communicatie, wordt bedoeld communicatie met relaties van de Belastingdienst. Onder interne communicatie wordt verstaan de communicatie tussen belastingdienstmedewerkers en/of –systemen.

Deze set van eisen zoals uitgewerkt in het VBI en VBA wordt als basisniveau beschouwd. Ten aanzien van hoog-kritische gegevens of risicovolle omgevingen kunnen extra beveiligingseisen worden gesteld. Dit zal echter (volgens de huidige inzichten) op basis van een afhankelijkheids- en kwetsbaarheidsanalyse (A&K analyse) moeten worden aangegeven. Voor het stellen van extra eisen aan de beveiliging van gegevens is een classificatie van gegevens, informatiesystemen en processen nodig. Binnen de belastingdienst wordt de indeling in beveiligingsklassen volgens het handboek Informatiebeveiliging Belastingdienst [HIB] gebruikt.

De soorten classificaties (voor processen, informatiesystemen en betrouwbaarheidscriteria vertrouwelijkheid, integriteit en beschikbaarheid) staan beschreven in het HIB. De classificatie van *processen en informatiesystemen* moet, net als bovenstaande gegevensclassificaties, als basis worden ingezet in een Afhankelijkheids- en Kwetsbaarheidsanalyse. De A&K analyse wordt op dit moment in het ontwerp van informatiesystemen gehanteerd en moet antwoord geven op de vraag 'moet ik bovenop de basisset van beveiligingseisen en –maatregelen, op grond van de classificaties, extra maatregelen treffen om de vertrouwelijkheid, integriteit en beschikbaarheid te kunnen garanderen'.

2 VBA: Maatregelen in de applicaties

Werkwijze

1. Selecteer, o.b.v. van het te realiseren applicatietype, de te ondernemen maatregelen uit de VBA en VBI.
2. Stel de beveiligingsbehoefte vast met de klant en onderzoek of met het resultaat van stap 1 de beveiligingsbehoefte wordt afgedekt.
3. Indien dit niet het geval is: Voer een beperkte A&K-analyse uit om aanvullende eisen en maatregelen vast te stellen.
4. Implementeer. Selecteer hiertoe bestaande (TIS)-componenten en realiseer bij gebrek aan standaard componenten 'eigen' oplossingen zoveel mogelijk buiten de applicatie.

Toelichting bij tabellen

De eisen en maatregelen die worden gesteld aan applicaties worden geclusterd naar beveiligingsaspecten volgens de Domein Architectuur Beveiliging (DAB). De daar genoemde definities zijn ook op dit document van toepassing, met uitzondering van die van integriteit. De DAB, als architectuur voor *infrastructuur*, richt zich alleen op het integer *blijven* van gegevens tijdens transport en opslag: raken ze niet op een of andere wijze 'verminkt'. In VBA richten we ons ook op het integer *zijn* van gegevens: zijn ze conform de werkelijkheid die ze trachten weer te geven.

Per maatregel is aangegeven voor welke typen applicaties ze gelden. We onderkennen vijf typen applicaties. Deze typering is aangegeven middels de volgende codering:

Code	Kenmerken
1	massaal, hoge beschikbaarheid, belastingdienstmedewerkers
2	online, zaaksgewijs, interactief, belastingdienstmedewerkers
3	online, persoonsgebonden, belastingplichtigen, hoge openstelling en beschikbaarheid
4	online, geen mutaties, aggregatie van informatie, belastingdienstmedewerkers
5	online, geen mutaties, 'algemene' informatie, belastingplichtigen, hoge openstelling en beschikbaarheid

2.1 Identificatie & Authenticatie

I&A.1: Elke gebruiker van de Belastingdienst systemen (TIS en applicaties) moet, binnen deze systemen, uniek identificeerbaar én herleidbaar zijn tot één persoon of proces.

Nr	Maatregel	1	2	3	4	5
1	Applicaties hebben hun eigen, <i>unieke</i> identificatie. Ook elk voorkomen (instance) van een applicatie heeft een uniek id.	√	√	√	√	√
2	Applicatietaken dienen zich altijd te identificeren en authenticeren als ze applicatietaken van andere applicaties aanroepen of als ze over systeemgrenzen heen gaan. De aangeroepen applicatie(taak) is verantwoordelijk voor het valideren hiervan.	√	√	√	√	√

I&A.2: Gebruikers dienen hun identiteit te bewijzen (authenticatie) op basis van kennis (wachtwoord).
Maatregelen worden in 'Voorschrift beveiliging infrastructuur' beschreven.

I&A.3: De authenticatie voor gebruikers met vergaande bevoegdheden moet aan zwaardere eisen voldoen.

Maatregelen worden in 'Voorschrift beveiliging infrastructuur' beschreven.

I&A.4: De exclusiviteit van het identificatie en authenticatiemiddel moet gewaarborgd zijn.

Nr	Maatregel	1	2	3	4	5
1	Authenticatiegegevens worden altijd versleuteld opgeslagen en verzonden. (Authenticatie van gebruikers wordt nooit aan de applicatie beschikbaar gesteld.)	√	√	√	√	
2	Zet geen gevoelige informatie zoals passwords als parameter bij het starten van een programma (m.n. in scripts).	√	√	√	√	

I&A.5: Voordat een geslaagde identificatie & authenticatie heeft plaatsgevonden mag er uitsluitend informatie verstrekt welke noodzakelijk is voor de aanlog procedure.

Maatregelen worden in 'Voorschrift beveiliging infrastructuur' beschreven.

2.2 Autorisatie

Aut.1: Op alle objecten moet toegangsbeveiliging van toepassing zijn op basis van: "Niets mag, tenzij ..."

Opmerking: Deze eis geldt voor applicaties voor de volgende objecten: de applicatie zelf, (groepen) applicatietaken en DBMS.

Nr	Maatregel	1	2	3	4	5
1	Gebruikers en processen hebben geen toegang tot procestaken en gegevens, tenzij dit expliciet is toegestaan.	√	√	√	√	
2	Alle applicatietaken zijn default disabled.	√	√	√	√	
3	De applicatie is zelf verantwoordelijk voor het (laten) uitvoeren van autorisatiecontroles. ¹	√	√	√	√	

Aanvullende maatregelen worden in 'Voorschrift beveiliging infrastructuur' beschreven.

Aut.2: Alleen eigenaars van objecten mogen gebruikersrechten delegeren.

Maatregelen worden in 'Voorschrift beveiliging infrastructuur' beschreven.

Aut.3: Maak gebruik van autorisatie conform de functiescheiding uit de organisatie.

Nr	Maatregel	1	2	3	4	5
1	Richt applicaties (taken) in volgens rollen. Een rol is een zodanige groep van functioneel bij elkaar behorende rechten, taken, transacties of commando's dat er binnen deze rol (en ten opzichte van andere rollen) uit eisen van functiescheiding geen onverenigbare autorisaties kunnen ontstaan. Dit wordt door de gebruikersorganisatie vastgesteld.	√	√	√	√	
2	Gebruikers(groepen) en processen dienen hun autorisaties via rollen te verkrijgen.	√	√	√	√	
3	Invoer of mutatie van gegevens dient strikt gescheiden te worden van de controle daarop. Dit geldt voor zowel gebruikers als processen. [Leg daarom vast welke gebruiker/proces de invoer of mutatie van een 'gegeven' heeft uitgevoerd, zodat gesignaleerd kan worden dat deze (niet) gerechtigd is de controle daarop uit te voeren.]	√	√	√		
4	Systeem- en applicatiebeheertaken moeten gescheiden zijn van de overige gebruikerstaken.	√	√	√	√	√
5	Transacties met een aanzienlijk financieel belang moeten van overige transacties gescheiden worden.	√	√	√		
6	Bij massale data-invoerprocessen moeten eerste invoer, eventuele controle-invoer en het aanbrengen van correcties naar aanleiding van uitgevoerde applicatie-controles of -signaleringen als afzonderlijke taken worden onderkend.	√				

AUT.4: Breng onderscheid aan tussen functionele autorisatie en competentie.

¹ Gebruik bijvoorbeeld een standaard autorisatievoorziening.

Nr	Maatregel	1	2	3	4	5
1	Verschil in autorisatie leidt tot afzonderlijke gebruikerstaken. Verschil in competentie wordt binnen de gebruikerstaak geregeld. Competentie bepaalt welke subset van gegevens mag worden bewerkt of benaderd.	√	√	√	√	
2	Maak voor functionele autorisaties gebruik van een standaard autorisatievoorziening of –module.	√	√	√	√	
3	Beleg het beheer van functionele autorisaties buiten de applicatie.	√	√	√	√	

AUT.5: Het moet altijd inzichtelijk zijn tot welke objecten een gebruiker rechten heeft.

Nr	Maatregel	1	2	3	4	5
1	Maak voor dat deel van de autorisaties die <i>in</i> de applicatie zijn vastgelegd een functie die de daarin toegekende rechten inzichtelijk maakt.	√	√	√	√	

AUT.6: Objecten moeten alleen via een vooraf gedefinieerd logisch toegangspad benaderbaar zijn.

Nr	Maatregel	1	2	3	4	5
1	Voorkom de mogelijkheden om programmaonderdelen rechtstreeks – bijv. vanuit een OS-commandline-omgeving - aan te roepen, indien dit niet expliciet de bedoeling is.	√	√	√	√	√

2.3 Vertrouwelijkheid

VER.1: Vertrouwelijke/gevoelige gegevens mogen niet leesbaar over het netwerk gaan. Maatregelen worden in 'Voorschrift beveiliging infrastructuur' beschreven.²

VER.2: Alleen de te verzenden gegevens -en niet meer- mogen over het netwerk gaan.

Nr	Maatregel	1	2	3	4	5
1	Verstuur alleen die gegevens die nodig zijn naar de ontvanger (ook: client), filter niet pas op de bestemming	√	√	√	√	√

VER.3: Alleen vertrouwelijke gegevens die strikt noodzakelijk zijn voor het uitvoeren van een taak mogen worden weergegeven aan de uitvoerende.

Nr	Maatregel	1	2	3	4	5
1	Output, gegenereerd door een applicatie mag alleen voor de ontvanger noodzakelijke informatie bevatten.	√	√	√	√	√
2	Het maken van kopieën moet voorzien zijn in een gebruikers- of applicatietaak, de hardcopy functie van de werkstations mag daarvoor niet worden gebruikt.	√	√			
3	Tijdelijke informatie blijkt vaak langer beschikbaar te zijn dan verwacht (bijv. printerspoolbestanden). Zorg dat ook tijdelijke informatie niet door onbevoegden kan worden ingezien.	√	√			
4	Vertrouwelijkheid van gegevens moet voldoen aan de Wet bescherming persoonsgegevens en de wetgeving met betrekking tot bewaartermijnen (archivering) van gegevens. <i>(Deze maatregel zal in release 2.0 van VBA verder worden uitgewerkt.)</i>	√	√	√	√	

² Er wordt uitgegaan van een constructie waarin de keuze of een bericht verwerkt mag worden buiten de applicatie is belegd. Ook acties naar aanleiding van onjuiste omgang met vertrouwelijkheid (bijv. melding naar verzender) liggen buiten de applicatie.

2.4 Integriteit

INT.1: Het mag niet mogelijk zijn ongemerkt ongeautoriseerde wijzigingen op infrastructuur, programmatuur, en opgeslagen en verstuurde data aan brengen.

Nr	Maatregel	1	2	3	4	5
1	Wanneer gegevens van klasse 2a, 2, 3 en 4 over een publiek netwerk worden verzonden, moet over alle gegevens een integriteitskenmerk worden aangebracht. Gebruik hiervoor bij voorkeur een elektronische handtekening. Andere maatregelen zijn: Hash, controlegetallen.	√	√	√	√	
2	Bij externe en interne verzending dient het eventuele aanbrengen en controleren van integriteit zo mogelijk buiten de applicatie geregeld te worden. Zie ook VBI.	√	√	√	√	
3	Wanneer de integriteit van gegevens gecompromitteerd is, mag de verwerking van die gegevens niet plaatsvinden. Er wordt een log aangemaakt. Verder moet dit leiden tot onmiddellijke alarmering van de eigenaar van de gegevens. Indien mogelijk moet dit worden gemeld bij de leverancier van gegevens.	√	√	√	√	
4	Alle fourtherstelacties moeten in "was-wordt" verslagen worden vastgelegd (nadat de fourtherstelactie vooraf door de gegevens- of proceseigenaar is gefiatteerd).	√	√			

INT.2: De integriteit van in te voeren gegevens moet zoveel mogelijk gewaarborgd worden door automatische (geautomatiseerde) controles.

Nr	Maatregel	1	2	3	4	5
1	De ingevoerde gegevens moeten een complete en consistente gegevensset in de context van de applicatie vormen. Controleer daarvoor de toegestane waarden van de ingevoerde gegevens, door middel van validatie-, bestaanbaarheid-, relatie- en redelijkheidscontroles. Bij voorkeur worden deze opgenomen in de regels van het operationele gegevensmodel.	√	√	√		
2	Voorzie relevante code-aanduidingen (fiscaalnummer, etcetera) van 4 of meer posities van een check-digit aan de hand waarvan de bestaanbaarheid van de code-aanduiding door het informatiesysteem kan worden vastgesteld.	√	√	√	√	
3	Druk foutieve invoer op grond van validatie- en bestaanbaarheidscontroles af op een foutenlijst. De invoer mag niet in het informatiesysteem worden verwerkt.	√	√	√		
4	Druk afwijkende invoer op grond van de redelijkheidscontrole af op een signaleringslijst. De invoer mag wel in het informatiesysteem worden verwerkt.	√	√	√		
5	Controleer de volledigheid van de invoer door controletoeetsen (dubbele invoer) en/of volgnummercontroles. Door middel van voortellingen (hash-totalen over kritische gegevens en som van bedragen) wordt de volledigheid van de invoer en de juistheid van enkele rubrieken uit de invoer gewaarborgd.	√	√	√		
6	Sta geen default waarden toe bij kritische gegevenselementen, koppel hier een verplichte veldinvulling aan vast.	√	√	√		
7	Leg logische regels (b.v. fiscale regels) zoveel mogelijk vast in door toepassingsbeheerders te beheren tabellen. Deze regels, samen met integriteitsregels, moeten bij voorkeur via het DBMS bewaakt kunnen worden in een aparte gebruikerstaak.	√	√	√	√	√

INT.3: De integriteit van binnen de belastingdienst te verspreiden gegevens moet zoveel mogelijk gewaarborgd worden door automatische (geautomatiseerde) controles.

Nr	Maatregel	1	2	3	4	5
1	Als kritische uitvoerlijsten niet met een vaste periodiciteit worden	√	√	√		

Nr	Maatregel	1	2	3	4	5
	geproduceerd, moeten zij volgnummers bevatten.					
2	Voorzie de uitvoerbestanden van geleidelijsten met (hash) totalen van kritische gegevens en bedragen. Deze (hash) totalen moeten ook op het bestand voorkomen (voorloop- of sluitrecord).	√	√			

INT.4: Door de Belastingdienst gegenereerde documenten / formulieren moeten eenduidig zijn opgesteld en de uniciteit en volledigheid moet worden gewaarborgd.

Nr	Maatregel	1	2	3	4	5
1	Maak gebruik van huisstijl van de belastingdienst en standaardformulieren.	√	√	√	√	√
2	Bewaar een kopie van de uitvoer van uitwisselingsbestanden totdat de ontvangst daarvan bevestigd is.	√	√			

2.5 Controleerbaarheid

CON.1: De gewenste gebeurtenissen in het systeem welke gelogd moeten worden moeten door de opdrachtgever worden aangegeven.

Zie VBI.

CON.2: De logging/audittrail moet voldoende informatie bevatten om te kunnen herleiden welke handelingen zijn verricht, wie/wat deze handelingen initieel heeft gestart en wanneer deze zijn uitgevoerd.

Nr	Maatregel	1	2	3	4	5
1	Minimaal vast te leggen in de logging/audittrail: datum/tijd (t/m seconde), gebruiker-id (of applicatie/proces-id), uitgevoerde actie.	√	√	√		
2	De applicatie moet inzicht kunnen geven in de verwerking van de invoerstroom tot uitvoer. Daarbij moet de volledigheid en juistheid van invoer, verwerking en uitvoer worden gegarandeerd en aantoonbaar worden gemaakt.	√	√	√		
3	Invoer-, verwerkings- en uitvoerverslagen moeten altijd worden aangemaakt nadat verwerkingen zijn geactiveerd.	√	√	√		
4	De controletotalen op genoemde verslagen worden gesplitst naar soort invoer, uitvoer of verwerking en worden gepresenteerd in de vorm van een doorrekening in aantallen en bedragen: Beginstand + nieuw +/- wijzigen – vervallen = eindstand. Ingevoerde mutaties = verwerkt (verder uitsplitsen) + niet verwerkt.	√	√	√		
5	De eindtotalen van mutatielijsten, signaallijsten en foutverslagen moeten kunnen worden aangesloten op de totalen van het verwerkingsverslag.	√	√	√		
6	Alle ingevoerde, gemuteerde of vervallen posten moeten op doelmatige wijze raadpleegbaar zijn (database, papier, microfiche).	√	√	√		
7	Laat bij variabele instelmogelijkheden de selectiecriteria (waaronder ook begindatum en einddatum), die gebruikt zijn om de uitvoer te bepalen, op de betreffende uitvoerlijsten afdrukken.	√	√			
8	Als een proces geen uitvoer produceert, moet een nihilverslag of nihilbestand aangemaakt worden. Hierdoor is het voor de volgende processen duidelijk dat er terecht geen uitvoer is.	√	√	√		
9	Om onvolledige uitvoer te voorkomen, dient elk verslag afgesloten te worden met een "einde-verslag" regel.	√	√	√	√	
10	In doorrekeningen kunnen "sprongen" voorkomen in het element van doorrekening, doordat de posten financieel worden gewaardeerd of naar andere waarden worden omgerekend (bijv. van inkomensgrondslag naar aanslag). De aansluiting moet dan te constateren zijn via de aantallen posten.	√	√			
11	De controletellingen moeten zoveel mogelijk gebaseerd zijn op tijdens de computerverwerking opgebouwde tellingen. Indien tellingen worden overgenomen uit bestanden, moet dat kenbaar gemaakt worden.	√	√			

Nr	Maatregel	1	2	3	4	5
12	Bij het on-line verwerken van mutaties in een database kunnen controletellingen apart worden bijgehouden en gemuteerd. Frequent moet dan worden gecontroleerd of deze controletellingen in overeenstemming zijn met de daadwerkelijke telling van de database. Voor deze controle moet een aparte gebruikerstaak worden gedefinieerd.	√	√	√		

CON.3: De volledigheid van de logging/audit-trail moeten worden gewaarborgd en kunnen worden vastgesteld. (Integriteit van het log).

Maatregelen worden in 'Voorschrift beveiliging infrastructuur' beschreven.

Hostname	Klantgroep	te Last LogUsername	Naam
apandu06	EH (prod)	25/18 9:10	Persoonsgegevens
apandu07	EH (ontw)	3/18 10:20	
apandu06	EH (prod)	7/18 14:58	
apandu07	EH (ontw)	3/18 12:47	
apandu06	EH (prod)	3/18 15:28	
apandu07	EH (ontw)	1/18 14:37	
apandu06	EH (prod)	0/18 13:37	
apandu06	EH (prod)	1/18 13:25	
apandu07	EH (ontw)	0/18 11:56	
apandu06	EH (prod)	0/18 14:27	
apandu06	EH (prod)	3/18 13:47	
apandu06	EH (prod)	1/18 11:58	
apandu07	EH (ontw)	1/18 14:17	
apandu06	EH (prod)	3/18 11:17	
apandu06	EH (prod)	3/18 15:22	
apandu07	EH (ontw)	3/18 10:44	
apandu06	EH (prod)	0/18 15:05	
apandu07	EH (ontw)	2/18 10:19	
apandu06	EH (prod)	7/18 10:13	
apandu07	EH (ontw)	19/18 9:22	
apandu06	EH (prod)	1/18 10:50	
apandu06	EH (prod)	3/18 11:40	
apandu06	EH (prod)	3/18 14:47	
apandu06	EH (prod)	31/18 8:55	
apandu07	EH (ontw)	3/18 11:28	
apandu06	EH (prod)	2/18 11:46	
apandu07	EH (ontw)	2/18 11:42	
apandu06	EH (prod)	7/18 13:10	
apandu07	EH (ontw)	3/18 14:44	
apandu06	EH (prod)	/7/18 8:26	
apandu07	EH (ontw)	1/18 11:24	
apandu06	EH (prod)	0/18 13:46	
apandu07	EH (ontw)	14/18 7:27	
apandu06	EH (prod)	3/18 11:06	
apandu07	EH (ontw)	3/18 11:27	
apandu06	EH (prod)	5/18 15:45	
apandu06	EH (prod)	0/18 13:54	
apandu06	EH (prod)	31/18 8:32	
apandu07	EH (ontw)	/1/18 8:46	
apandu06	EH (prod)	0/18 13:10	
apandu06	EH (prod)	NULL	
apandu06	EH (prod)	30/18 8:40	
apandu06	EH (prod)	/1/18 9:00	
apandu07	EH (ontw)	19/18 8:44	
apandu06	EH (prod)	/3/18 9:38	
apandu07	EH (ontw)	30/18 8:40	
apandu06	EH (prod)	2/18 23:04	

Persoonsgegevens

Persoonsgegevens

apandu07	EH (ontw)	2/18 23:04	Persoonsgegevens	Persoonsgegevens
apandu06	EH (prod)	1/18 10:06		
apandu06	EH (prod)	3/18 15:54		
apandu07	EH (ontw)	30/18 6:21		
apandu06	EH (prod)	7/18 14:10		
apandu06	EH (prod)	3/18 16:27		
apandu06	EH (prod)	31/18 8:34		
apandu07	EH (ontw)	1/18 13:39		
apandu06	EH (prod)	17/18 6:43		

userid

naam gebruiker

Persoonsgegevens

Persoonsgegevens

Persoonsgegevens

Persoonsgegevens

Persoonsgegevens

Persoonsgegevens