Ministerie van Veiligheid en Justitie

Informatiebeveiligingsafspraken IWPI

(gegevensuitwisseling via de spelverdeler t.b.v. implementatie wet en protocol identiteitsvaststelling)

IBA-SRK Versie 1.04

Versie 0.4

Datum 29 augustus 2012
Status

Colofon

Afzendgegevens	**Directoraat-Generaal Rechtspleging en Rechtshandhaving** Directie Veiligheid en bestuur Afdeling Keteninformatisering Schedeldoekshaven 100 2511 EX Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/venj
Contactpersoon	C.H.J. Willemsen *beleidsadviseur* T 070 370 79 11 F 070 370 79 00
Bijlage(n)	Afhankelijkelijksanalyse 0.4 Kwetsbaarheidsanalyse 0.4 Baseline Informatiebeveiliging Rijksdienst
Auteurs	C. Willemsen / K. Terlouw / H. Aghaei

Inhoud

Inhoudsopgave

Inleiding

De Informatiebeveiligingsafspraken strafrechtsketen gegevensuitwisseling via de spelverdeler t.b.v IWPI [1](hierna te noemen de afspraken) bevatten de invulling van bestaande normen en afspraken voor het waarborgen van een adequaat niveau van beveiliging voor het uitwisselen van Departementaal Vertrouwelijk gerubriceerde informatie in de strafrechtsketen tussen Politie, Veiligheid&Justitie en Defensie (KMar) door middel van elektronisch berichtenverkeer. Een groot deel van de organisatorische en procedurele afspraken heeft een meer algemeen karakter. De implementatiehandreiking moet dan ook worden gezien als een “best practice” waaraan de inrichting van (eventuele toekomstige) ketenvoorzieningen in principe dient te voldoen.

Indien binnen de (rijks)overheid de behoefte bestaat om voor overige ketens of andere toepassingen dan berichtenverkeer (zoals e-mail) ook afspraken te maken voor dit beveiligingsniveau, dan zijn de hier beschreven afspraken in te zetten als minimaal vereist beveiligingsniveau.

De afspraken gelden voor alle partijen die betrokken zijn bij de levering, de instandhouding en het gebruik van de Departementaal Vertrouwelijke voorzieningen binnen de strafrechtsketen.

Bij het realiseren van deze afspraken zijn de volgende partijen betrokken geweest: VtsPN, Politie, Ministerie van Justitie (DII, DGRR, BVA, JustID, RvdK, OM, DJI, RvdR) en Ministerie van Defensie (KMar, Ivent)

In dit hoofdstuk komen aan de orde de aanleiding, het doel, de totstandkoming en het resultaat, eigenaarschap en beheer van de afspraken, de leeswijzer en het versiebeheer.

Aanleiding

In de strafrechtsketen is een deugdelijke vaststelling van de identiteit van personen van fundamenteel belang. Persoonsverwisseling en identiteitsfraude hebben ernstige gevolgen voor de integriteit en effectiviteit van de strafrechtspleging en voor de eventuele slachtoffers. Het is daarom van belang dat de werkwijze voor het vaststellen van de identiteit van verdachten en veroordeelden aan hoge eisen voldoet en door heel de keten heen eenduidig wordt gevolgd.
Deze werkwijze is in het Protocol Identiteitsvaststelling [18][2] binnen de strafrechtsketen uitgewerkt. Dit protocol dient door de gehele strafrechtsketen te worden doorgevoerd. Uit dit protocol volgt dat er departementaal vertrouwelijke gegevens uitgewisseld zullen gaan worden. Hierdoor is het noodzakelijk om beveiligingsmaatregelen te treffen waarvoor de bovenliggende afspraken alhier worden beschreven.

Doel

De afspraken hebben tot doel aan te geven welke maatregelen van toepassing zijn om de informatie-uitwisseling door middel van uitwisseling van elektronische berichten in te richten op het niveau Departementaal Vertrouwelijk. De afspraken vormen een

[1] Voorheen benoemd als Beveiligingsstandaard Strafrechtketen waarbij de nadruk vanaf versie 1.1 is verlegd naar het specifiek invullen van bestaande standaarden en normen voor gebruik in de strafrechtsketen.

[2] Referte (zie paragraaf 1.6)

minimumniveau en dienen te worden ingezet bij de uitwisseling over de Haagse Ring van Departementaal Vertrouwelijke informatie tussen Politie, Justitie en Defensie, en in de toekomst aan te sluiten partijen. De informatie-uitwisseling zoals die plaatsvindt in het kader van de identiteitsvaststelling is als uitgangspunt genomen aangezien deze de aanleiding vormde voor de totstandkoming van de afspraken.

De doelgroep van deze afspraken bestaat uit personen die belast zijn met het beschikbaar stellen van Departementaal Vertrouwelijke informatie middels berichtenuitwisseling. De afspraken zijn geschreven met het doel om als handvat te dienen voor specialisten op het betreffende deelterrein (personeel, fysieke beveiliging, beheer, etc.)

Totstandkoming en resultaat

De afspraken zijn tot stand gekomen door een aantal achtereenvolgende stappen door te lopen die hieronder op hoofdlijnen zijn toegelicht. De onderstaande opgeleverde tussenproducten zijn bij het Ministerie van Veiligheid en Justitie opvraagbaar.

Overzicht referentiekader

Hieronder volgt de lijst van wet en regelgeving die van toepassing is op de afspraken:

- Algemene wet- en regelgeving: VIR 2007, VIR-GI, en WBP.
- Specifieke Politie wet- en regelgeving: RIP, BBNP, Podacs, Wet en besluit politiegegevens, Beveiligingsbeleid Politie en Beveiligingsarchitectuur vtsPN.
- Specifieke Justitie wet- en regelgeving: Wet justitiële en strafvorderlijke gegevens, Handboek Beveiliging Ministerie van Justitie Concern (2005), Aansluitbeleid JustitieNet2, Aansluitbeleid externe koppelingen, Wet identiteitsvaststelling verdachten en veroordeelden en getuigen.
- Specifieke Defensie wet- en regelgeving voor de KMar: Defensie Beveiligingsbeleid en Normenkader koppelingen met Defensienetwerken (D401)

Voor een nadere uitwerking van de consequenties van deze documenten voor de afspraken wordt verwezen naar het referentiekader document [19].

Overzicht dreigingen en kwetsbaarheden

In het overzicht dreigingen en kwetsbaarheden zijn de mogelijke scenario's beschreven die van toepassing zijn. Voor deze scenario's is aangegeven welke dreigingen en kwetsbaarheden onderkend moeten worden.

Overzicht kwaliteitscriteria

De kwaliteitscriteria zijn opgesteld om de afspraken vanuit het oogpunt van de betrokken partijen objectief te kunnen beoordelen. De afspraken zijn beoordeeld op technische inpasbaarheid, doorlooptijd van de implementatie, investeringskosten, exploitatiekosten, de noodzaak voor reorganisatie en de effectiviteit van maatregelen.

Het afsprakenkader

In het afsprakenkader zijn de afspraken opgenomen om te komen tot afspraken voor informatie-uitwisseling op het beveiligingsniveau Departementaal Vertrouwelijk. De afspraken zijn geselecteerd naar aanleiding van de opgestelde dreigingen en kwetsbaarheden. Na juiste implementatie van de afspraken wordt de kans dat de dreigingen en kwetsbaarheden manifest worden in voldoende mate beperkt.

De afspraken Strafrechtketen

De hierboven genoemde documenten vormen worden in deze stap samengevoegd tot de afspraken. Deze bestaan uit het afsprakenkader aangevuld met een beschrijving hoe de governance en beheer van de afspraken is ingericht en afgestemd.

Eigenaarschap en beheer van de afspraken

Het eigenaarschap en het beheer van de afspraken is belegd bij de DGRR van het Ministerie van Veiligheid en Justitie in zijn rol als regisseur van de strafrechtsketen.

Versiebeheer

Versie	Datum	Status	Opmerkingen
0.1	04-12-2008	Concept	Eerste opzet
0.99	20-02-2009	Eindconcept	Opmerkingen uit 2de Decision Board overleg verwerkt
1.0	18-02-2009	Definitief	Na vaststelling in de Coördinatiegroep Informatievoorziening strafrechtsketen (CIS) d.d.
1.1	6-10-2011	Concept	

Referenties

[1] Aansluitbeleid JustitieNet2
[2] Aansluitvoorwaarden Haagse Ring
[3] Basisbeveiligingsniveau Nederlandse Politie (BBNP)
[4] Baseline Informatiebeveiliging Rijksoverheid (BIR)
[5] Beveiligingsarchitectuur vtsPN v1.0
[6] Beveiligingsbeleid Politie
[7] Code voor Informatiebeveiliging (ISO/IEC 17799:2002 nl)
[8] Defensie Beveiligingsbeleid
[9] Defensie Normenkader koppelingen met Defensienetwerken (D401)
[10] Dreigingen en kwetsbaarheidsanalyse Beveiligingsstandaard Progis
[11] Handboek Beveiliging Ministerie van Justitie Concern (2005)
[12] Justitie Aansluitbeleid externe koppelingen
[13] Kwaliteitscriteria Beveiligingsstandaard Progis
[14] Lessons learned rapport - Realisatie IBOS via de Haagse Ring, versie 0.4, 14 september 2007
[15] Normenkader Informatiebeveiliging Rijksweb (NIR)
[16] Plan van Aanpak Beveiligingsstandaard Progis
[17] Podacs
[18] Protocol Identiteitsvaststelling
[19] Referentiekader Beveiligingsstandaard Progis
[20] Regeling Informatiebeveiliging Politie (RIP)
[21] Standaard Beveiligingsniveau Departementaal Vertrouwelijk, Ministerie van Defensie (SBN LLL)
[22] Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere informatie, 2004 (VIR-BI)
[23] Voorschrift Informatiebeveiliging Rijksdienst, 2007 (VIR 2007)
[24] Wet bescherming persoonsgegevens (WBP)
[25] Wet en besluit politiegegevens
[26] Wet identiteitsvaststelling verdachten, veroordeelden en getuigen
[27] Wet justitiële en strafvorderlijke gegevens

Toepassing van de afspraken

Dit hoofdstuk beschrijft op welke wijze de afspraken moeten worden toegepast. De onderwerpen die aan de orde komen zijn algemene uitgangspunten, verantwoordelijkheden, governance en referenties.

Algemene uitgangspunten

Voor de afspraken dient het VIR BI als basis. Hierin wordt aangegeven hoe tot het beveiligingsniveau Departementaal Vertrouwelijk te komen. Voor de politie staat dit gelijk aan de rubricering Politie Intern (oftewel groen). Naast de vertrouwelijkheid betreffen de afspraken ook de exclusiviteit en de integriteit van de gegevens.

De aangesloten organisaties dienen te voldoen aan de aansluitvoorwaarden voor de Haagse Ring. De maatregelen die al van toepassing zijn op de aangesloten organisaties uit hoofde van de aansluitvoorwaarden voor de Haagse Ring zijn dan ook niet meer afzonderlijk opgenomen in dit maatregelenkader, behalve indien dit noodzakelijk wordt geacht voor de context.

Aangezien de afspraken zich richten op de informatie-uitwisseling tussen partijen is deze geen vervanging voor informatiebeveiligingsnormen en maatregelen ten aanzien van de interne informatievoorziening van partijen. Hiervoor blijven de bestaande normen gelden. De in de afspraken gestelde normen en maatregelen vormen hierop een aanvulling die een veilige uitwisseling van informatie waarborgt.

Verantwoordelijkheden

Deze afspraken onderscheiden verschillende verantwoordelijkheden (rollen). Afhankelijk van haar rol(len) is een partij verantwoordelijk voor de naleving van bepaalde maatregelen. Concreet betekent dit dat de hoeveelheid maatregelen per partij kan variëren afhankelijk van de rol(len) die de partij vervult. In de praktijk zal het treffen van maatregelen vaak een samenwerking vereisen van de verschillende partijen. Denk bijvoorbeeld aan het beheer van autorisaties en uitwisselen van certificaten.

<u>De aanbieder</u>
De aanbieder is de partij welke verantwoordelijk is voor het aanbieden van een bepaalde dienst waarmee departementaal vertrouwelijke informatie uitgewisseld kan worden met afnemers. De aanbieder de aanbieder controleert of de vragende partij voldoende is geautoriseerd om de dienst te kunnen gebruiken.

<u>De afnemer</u>
Een afnemer is de partij die gebruik maakt van diensten die door een aanbieder worden aangeboden. Door gebruik te maken van de aangeboden dienst krijgt de afnemer de beschikking over de gewenste departementaal vertrouwelijk informatie. De afnemer kan op basis van functierollen specifieke informatie beschikbar stellen aan personen die voor of bij hem werken.

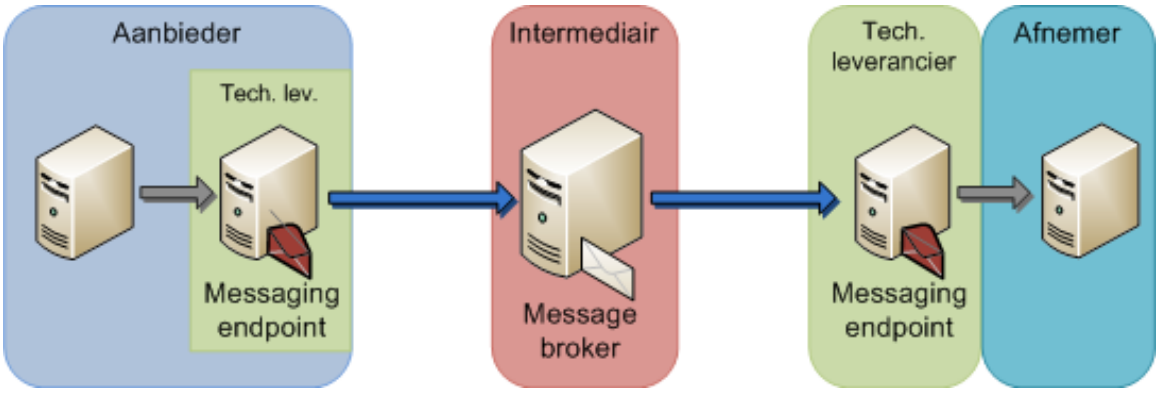
<u>Technisch leverancier</u>
De technische leverancier is de partij welke de benodigde technische infrastructuur, inclusief de messagingservers levert. De technisch leverancier schept de technische

voorwaarden voor een aanbieder dan wel afnemer van een dienst om deze te kunnen aanbieden respectievelijk afnemen.
Een technisch leverancier kan een onderdeel (afdeling) zijn van een aanbiedende of afnemende partij, maar kan ook een externe leverancier zijn die in opdracht van een partij handelt.

Een verbijzondering van de technisch leverancier is de intermediar. Een intermediair is een partij of service die een messagebroker levert die het berichtenverkeer tussen de technische leverancier van de aanbieder en afnemer verzorgt door het routeren van berichten tussen de verschillende partijen.
In het kader van het Spelverdeler project is Jubes (c.q. de tegenhanger, de Externe Politie Broker) de intermediair die het berichtenverkeer verzorgt tussen de ketenpartners, registers en de Spelverdeler.

Volgens VIR (art 4) bestaat er een eigenaarschap van een informatiesysteem. Dit eigenaarschap moet in de lijn belegd zijn. Het woord 'systeem" wordt in VIR ruim opgevat (techniek, applicatie, bijbehorende processen). De hiervoor beschreven aanbieder en/of de technisch leverancier is (doorgaans) de eigenaar van de aangeboden dienst maar het eigenaarschap van de dienst kan ook elders belegd zijn.
De eigenaar van de informatie is een aparte rol en beschrijven we de geest van VI-BI (art 8 dat gaat over het rubriceren en herrubriceren van informatie) als volgt:
- degene die de inhoud van de informatie heeft vastgesteld,
- of diens ambtsopvolger
- of een door of namens de SG daartoe aangewezen ambtenaar.
Bij archivering van stukken en de daarmee gepaard gaande herrubricering, spreekt VIR-BI over een verantwoordelijkheid van "het overbrengende ministerie".

In de onderstaande figuur zijn de hierboven gedefinieerde rollen schematisch weergegeven. Opgemerkt dient te worden dat het niet noodzakelijk is dat een intermediair in het berichtenverkeer tussen aanbieder en afnemer is opgenomen.



Figuur 1 - Overzicht van de rollen betrokken bij informatie-uitwisseling

De aanbiedende of afnemende partij is in beginsel verantwoordelijk voor de juiste toepassing van de afspraken bij zijn technische leverancier. Indien een partij gebruik maakt van een externe technische leverancier zoals bijvoorbeeld de afnemer uit bovenstaande figuur, dan is deze dus ook verantwoordelijk voor de handhaving en toepassing van de normen en maatregelen van de afspraken bij deze externe leverancier.

Zoals in de voorgaande paragraaf reeds beschreven richten de afspraken zich op het beveiligen van de informatie-uitwisseling tussen partijen, aangeduid door de blauwe

pijlen in bovenstaande figuur. De normen en maatregelen in de afspraken hebben dan ook met name betrekking op deze communicatie.
De aanbieder en afnemer zijn in beginsel verantwoordelijk voor het waarborgen van de vertrouwelijkheid van informatie tot het moment dat deze verstuurd wordt. Enkel de implementatie van deze afspraken kan deze vertrouwelijkheid niet garanderen. Hiervoor zijn aanvullende maatregelen of procedures noodzakelijk in de organisaties van de aanbieder en afnemer.

De afspraken

Het voorstel is BIR TNK (Basis Informatiebeveiliging Rijksdienst Tactisch Normenkader) als het informatiebeveiliging kader voor IWPI te hanteren (gebaseerd op de kwetsbaarheidsanalyse versie 0.4).
Aangezien betrouwbaarheidsniveau van IWPI op Beschikbaarheid=M, Exclusiviteit=M integriteit=H vastgelegd is dienen de volgende concrete en aanvullende IB-normen toegepast te worden[3]. Deze afspraken hebben veelal betrekking op de IT-architectuur doch kunnen ook consequenties hebben voor de organisatie, de procedures en de mensen die de voorzieningen beheren en gebruiken.

Nr.	*IWPI Integrale Beveiligingsnormen*	*organisatorisch*	*technisch*
1.	Toegang tot gegevens moet overeenkomen met het need-to-know en need-to-have-principes en de rechten van de gebruiker.	policy	
2.	De eigenaar van gegevens is verantwoordelijk voor het toekennen van toegang tot deze gegevens. De systeemeigenaar is namens de gegevenseigenaar verantwoordelijk voor de uitvoering van deze norm.	Policy	
3.	Toegangsrechten tot een systeem en toegangsmogelijkheden (bijv. lezen, schrijven etc.) tot de informatie in het systeem door middel van een autorisatiebeheerproces worden bepaald.	Policy	IAAM
4.	Het autorisatiemechanisme moet zoveel mogelijk afgedwongen worden door de onderliggende ICT-infrastructuur.	Policy	IAAM
5.	De toegangsrechten van gebruikers moeten minimaal om de 90 dagen worden geëvalueerd.	Policy	IAAM
6.	Bij het toekennen van toegangsrechten aan rollen moet de organisatie (gegevens- en systeemeigenaar) rekening houden met eventueel van toepassing zijnde functiescheiding.	Policy	
7.	Tref maatregelen om kwaadaardige programmatuur op het ICT-systeem te detecteren en de schade te minimaliseren.		antivirus IDS/IPS
8.	Leg vooraf vast op welke patronen en gebeurtenissen gescand moet worden.	Policy	antivirus IDS/IPS
9.	Scan de ICT-infrastructuur op mogelijke activiteit van kwaadaardige programmatuur of ander ongeautoriseerd gebruik.	Policy	antivirus IDS/IPS
10.	De detectieprogrammatuur moet actueel zijn en actueel blijven.		antivirus IDS/IPS

[3] Bronnen: Defensie beveiligingsmaatregelen (conform VIR)/ BIR TNK versie 0.99f.

Nr.	*IWPI Integrale Beveiligingsnormen*	*organisatorisch*	*technisch*
11.	Zorg dat het netwerk zo is ingericht dat het, indien noodzakelijk, mogelijk is om externe koppelingen te identificeren en te controleren of deze externe koppelingen zijn geautoriseerd.		Netwerk-portaal
12.	In verschillende schakels van een keten binnen de infrastructuur van een organisatie wordt bij voorkeur antivirusprogrammatuur van verschillende leveranciers toegepast.	Policy	antivirus IDS/IPS
13.	Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.	BCP	Backup BCP
14.	Een gebruiker moet geen extra rechten kunnen toekennen aan programma's die mobiele code uitvoeren.	Policy	Browser netwerk portaal
15.	Gegevensuitwisseling tussen vertrouwde en onvertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware. Deze controle wordt door minimaal twee verschillende beveiligingssystemen uitgevoerd. Constatering leidt tot signalering. De update voor de detectiedefinities vindt minimaal dagelijks (geautomatiseerd) plaats. Hogere frequentie indien daar aanleiding toe is (bijv. uitbraak van nieuw virus of malware).	Policy	IDS/IPS
16.	De koppeling dient te zijn voorzien van een Intrusion Detection System (IDS) of een Intrusion Prevention System (IPS).		IDS/IPS
17.	Het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten ontdekt en hersteld kunnen worden en de betrouwbaarheid van het netwerk niet onder het afgesproken minimumniveau komt.		SIEM en SOC
18.	Er is een overeenkomst tussen de eigenaren van informatiedomeinen in het IWPI keten waarin de wederzijdse beveiligingsmaatregelen zijn beschreven en de partijen verklaren dat de maatregelen daadwerkelijk zijn geïmplementeerd.	overeenkomst	
19.	De data-uitwisseling tussen de ketenpartners moet met een door de gegevenseigenaren van beide ketenpartners goedgekeurd product of door middel van PKI voor de overheid sleutels/ certificaten versleuteld worden.	Policy	PKI infra
20.	De exclusiviteit van informatie moet worden beschermd gedurende de gehele transmissieketen.		Encryptie vlgs NBV norm
21.	Data-uitwisseling moet voor zover mogelijk elektronisch plaatsvinden (dus geen fax-	Policy	Message broker

Nr.	*IWPI Integrale Beveiligingsnormen*	*organisatorisch*	*technisch*
	verkeer).		
22.	Digitale handtekening, PKI voor de overheidscertificaten en de ontvangstbevestiging van de berichten dienen toegepast te worden.	Policy	PKI en messaging
23.	De eigenaren van de gegevens stemmen in met de invoer of uitvoer van data vanuit of naar het informatiedomein van de wederpartij, als sprake is van een verschillend rubriceringsdomein of rubriceringsniveau.	policy en derubricering	
24.	De koppelingen moeten conform de SLA's tussen de partijen altijd beschikbaar zijn.	Policy	BCP
25.	Van de koppelingen zijn beheerdossiers aanwezig, waarin het functioneel en technisch beheer is beschreven, inclusief de hieraan gerelateerde beheerprocessen (zoals het configuratie-, incidenten- en wijzigingsbeheer).		logging
26.	De koppeling dient te zijn voorzien van actuele malwarescan software.		Virus scanning
27.	De koppelvlakken dienen onder gegarandeerde controle van de eigenaren en voor wat betreft de spelverdeler onder controle van Min V&J te staan en te blijven.	Policy	
28.	Alleen geautoriseerde functionarissen mogen met de netwerkinfrastructuur en de koppelvlakken van IWPI werken. De werkzaamheden moeten traceerbaar zijn.	Policy	Beheersreg eis netwerk en rekencentra
29.	De datacommunicatielijnen dienen voldoende capaciteiten te hebben. Performance van de datacommunicatie lijnen moeten continue in de gaten gehouden worden.		Capacity management
30.	De boven genoemde normen zijn concrete/aanvullende normen die naar aanleiding van de kwetsbaarheid analyse vastgelegd zijn. Daarnaast zijn de fysieke, organisatorische (o.a. regulier audit en controle) en personele beveiligingsmaatregelen (o.a. screening) van BIR TNK voor betrouwbaarheidsniveau van IPWI (Betrouwbaarheid=H, Exclusiviteit=M en Integriteit=H) van toepassing. Zie voor detail BIR TNK 0.99.	Policy	beheerders

De normen kunnen ok op een andere manier worden ingedeeld ter verduidelijking: