Checklist inspecties beveiliging gegevens aftappen telecommunicatie

Datum : 24 mei 2005

Inhoudsopgave

1	Inleiding	3
2	Algemene beveiligingseisen	4
3	Beveiligingseisen ten aanzien van personeel	5
4	Outsourcing	7
5	Fysieke beveiliging en beveiliging van de omgeving	8
6	Beheer van communicatie en bedieningsprocessen	10
7	Toegangsbeveiliging van geautomatiseerde informatiesystemen	11
8	Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen	13

1 Inleiding

In hoofdstuk 13 van de Telecommunicatiewet (Tw) staan regels voor het bevoegd aftappen van openbare telecommunicatie netwerk- en dienstenaanbieders. In artikel 13.5 Tw staat voor deze aanbieders de basisverplichting om gegevens die zij krijgen van bijvoorbeeld de opsporings- en inlichtingendiensten goed te beveiligen. De gegevens moeten vooral beveiligd worden omdat het vaak gaat om privacy gevoelige informatie en om informatie die, bij uitlekken, onnodig onderzoekstrajecten kunnen verstoren. De aanbieder heeft deze informatie nodig om te voldoen aan een verzoek om af te tappen, de zogenaamde taplast.

Hoe een aanbieder aan deze beveiligingsverplichting voldoet mag de aanbieder zelf weten. Er moet wel een, op de aard van de gegevens toegesneden, minimum niveau van beveiligingsmaatregelen zijn getroffen. De regels voor dit minimum niveau zijn opgenomen in het Besluit beveiliging gegevens aftappen telecommunicatie. De aanbieder kan aan de hand van een beveiligingsplan dit minimum niveau aantonen. De vorm van het beveiligingsplan staat niet vast. Iedere aanbieder mag zijn eigen vorm kiezen en het op de eigen specifieke situatie toespitsen.

Agentschap Telecom controleert de beveiliging aan de hand van een checklist. Deze checklist is een leidraad en geen invuloefening. Onderdelen van deze checklist zijn onder andere personeel, omgeving, locatie, uitbesteding, beheer en toegangsbeveiliging. In de volgende hoofdstukken staat een korte beschrijving per onderwerp en het deel van de checklist dat op dat onderwerp van toepassing is.

2 Algemeen

Maatregelen die een aanbieder treft om de gegevens te beveiligen moeten worden vastgelegd in een beveiligingsplan. In het beveiligingsplan moet de koppeling zijn gemaakt met het relevante deel van het bedrijfsproces waarvoor de maatregel is getroffen. De beoordeling van de beveiligingmaatregelen kan niet zonder inzicht in het tapproces zoals dat bij de aanbieder verloopt. Daarom moet dit proces ook in het beveiligingsplan zijn beschreven. Aandachtspunten bij de beschrijving zijn:

- bij wie en hoe komen taplasten binnen;
- hoe lopen papierstromen;
- systemen waarop taplasten worden ingevoerd;
- procedure opvragen NAW gegevens en verkeersgegevens;
- procedure ongeoorloofde inbreuk vertrouwelijkheid gegevens.

Bestaat er binnen de organisatie een (zelfstandig) beveiligingsplan m.b.t. bevoegd aftappen?	o ja o nee (niet zelfstandig/aanwezig, onvolledig,)		Kopie verstrekt? o ja o nee
Maakt beveiliging aftappen onderdeel uit van een algeheel beveiligingsplan binnen de organisatie?	o ja o nee		Kopie verstrekt? o ja o nee
Is dit beveiligingsplan geaccordeerd door het management?	o ja o nee		management/directie/.....
Is er een functionaris belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen?	o ja o nee	Indien ja: Naam : Functie:	
Voert deze functionaris regelmatig controles uit?	o Ja o nee		1x per .....
Is deze functionaris tevens eindverantwoordelijke	o ja o nee	Indien nee, wie eind-verantwoordelijk?	
Worden de resultaten van deze controles vastgelegd?	o ja o nee	Waar:	
Waaruit bestaan vervolgacties op resultaten van deze controles?			
Toelichting:			

3 Personeel

Aan medewerkers die rechtstreeks te maken krijgen met tapverzoeken en verstrekking van informatie worden eisen gesteld. Ook als een deel van het tapproces is uitbesteed aan derden, gelden voor de medewerkers van deze partijen de eisen. Eisen zijn onder andere het hebben ondergaan van een veiligheidsonderzoek, in bezit zijn van een verklaring omtrent het gedrag en een getekende geheimhoudingsverklaring.

1.	Naam : Tel : Mob : E-mail :	Geboortedatum:			
		Functie :			
		Rol in tapproces	o juridisch o technisch o		
		Verantwoordelijkheid voor beveiliging in functieomschrijving opgenomen	o ja o nee o		
		Vertrouwensfunctie	o ja o nee	VO[1]	o ja o nee
		Geheimhoudingsverklaring (t.a.v. aftapproces)	o ja o nee o	Bijlage	o ja o nee
		Verklaring omtrent gedrag[2]	o ja o nee	Bijlage	o ja o nee
	Toelichting:				

2.	Naam : Tel : Mob : E-mail :	Geboortedatum:			
		Functie :			
		Rol in tapproces	o juridisch o technisch o		
		Verantwoordelijkheid voor beveiliging in functieomschrijving opgenomen	o ja o nee o		
		Vertrouwensfunctie	o ja o nee	VO	o ja o nee
		Geheimhoudingsverklaring (t.a.v. aftapproces)	o ja o nee o	Bijlage	o ja o nee
		Verklaring omtrent gedrag	o ja o nee	Bijlage	o ja o nee
	Toelichting:				

[1] VO = veiligheidsonderzoek.
[2] Verklaring omtrent het gedrag als bedoeld in de Wet op de justitiële gegevens. Deze verklaring wordt in de volksmond "Bewijs van goed gedrag genoemd. Aanvraaginformatie www.justitie.nl/themas/vog

3.	Naam : Tel : Mob : E-mail :	Geboortedatum:			
		Functie :			
		Rol in tapproces	o juridisch o technisch o		
		Verantwoordelijkheid voor beveiliging in functieomschrijving opgenomen	o ja o nee o		
		Vertrouwensfunctie	o ja o nee	VO	o ja o nee
		Geheimhoudingsverklaring (t.a.v. aftapproces)	o ja o nee o	Bijlage	o ja o nee
		Verklaring omtrent gedrag	o ja o nee	Bijlage	o ja o nee
	Toelichting:				

4.	Naam : Tel : Mob : E-mail :	Geboortedatum:			
		Functie :			
		Rol in tapproces	o juridisch o technisch o		
		Verantwoordelijkheid voor beveiliging in functieomschrijving opgenomen	o ja o nee o		
		Vertrouwensfunctie	o ja o nee	VO	o ja o nee
		Geheimhoudingsverklaring (t.a.v. aftapproces)	o ja o nee o	Bijlage	o ja o nee
		Verklaring omtrent gedrag	o ja o nee	Bijlage	o ja o nee
	Toelichting:				

Welke procedure wordt gevolgd indien kennisnemers in dienst treden, intern een andere functie krijgen of het dienstverband beëindigen?	o geen procedure o procedure als volgt: (zie toelichting)
Toelichting:	

4 Uitbesteden

Als een aanbieder (een deel van) zijn werkzaamheden uitbesteedt aan een derde partij, waardoor deze derde partij over gegevens en informatie uit het tapproces kan beschikken, moet de aanbieder erop toezien dat de informatie voldoende wordt beveiligd. De aanbieder is verplicht om de beveiliging in een schriftelijke overeenkomst met de derde partij vast te leggen. Bovendien moet in deze overeenkomst worden vastgelegd dat de derde partij alle informatie moet verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.

Zijn er werkzaamheden uitbesteed aan derde partij(en)?	o ja o nee
Zijn de verplichtingen voortvloeiende uit het besluit in een schriftelijke overeenkomst met deze derde partij(en) vastgelegd?	o ja o nee
Is een afschrift van deze overeenkomst als bijlage aan het beveiligingsplan toegevoegd?	o ja o nee

Wie is/zijn deze derde partij(en)?
1.
2.
3.

Wie zijn de aanspreekpunten bij deze derde partij(en)?

Partij:	Naam:	Functie:
Partij:	Naam:	Functie:
Partij:	Naam:	Functie:
Partij:	Naam:	Functie:
Partij:	Naam:	Functie:
Partij:	Naam:	Functie:

Toelichting:

5 Locatie en omgeving

Ook voor de fysieke toegang tot gebouwen en ruimten waarin de aftapgegevens en informatie aanwezig zijn moeten beveiligingsmaatregelen zijn getroffen.

Worden informatie en gegevens zoveel mogelijk binnen één ruimte geconcentreerd?	o Ja o Nee		
Wat staat/ligt waar? (systemen/documenten)	1.		
	2		
	3.		
Locatiegegevens (NAW)	1.		
	2.		
	3.		
Wordt er bij de fysieke beveiliging gebruik gemaakt van zonering?	o ja o nee	Welke?	
Toelichting:			
Zijn tapproces specifieke zones aangewezen?	o ja o nee	Welke?	
Toelichting:			
Waaruit bestaat de fysieke beveiliging van de ruimte(n) waarbinnen de informatie en gegevens aanwezig zijn?			
1. Constructie: wanden van beton/steen/gips/systeemwanden/.....			
2. Binnenbeglazing: venster-/draad-/dubbel-/braakwerend-/doorgooibeperkend glas/geen/.....			
3. Buitenbeglazing: venster-/draad-/dubbel-/braakwerend-/doorgooibeperkend glas/geen/.....			
4. Electronische detectie: ruimtelijke detectie/camera/glasbreukdetectie/.....			
5. Toegangsverlening: sleutel/pasje/codeslot/.....			
Toelichting:			
Wordt toegangsverlening geregistreerd?	o ja o nee		
Is het binnentreden en verlaten van de ruimte achteraf herleidbaar op individueel niveau?	o ja o nee		
Wie is verantwoordelijk voor beheer toegangsverlen-de middelen?			
Hebben uitsluitend geautoriseerde personen (kennisnemers) toegang?	o ja o nee		
Hoe wordt ongeautoriseerde toegang en poging daartoe gedetecteerd?			
Toelichting:			
Hoe en door wie is tijdige interventie in dit geval geborgd?			
Toelichting:			

Beschrijf hoe opvolging alarmering is geregeld. Indien opvolging door beveiligingsbedrijf vermeldt naam en NAW-gegevens.	
Is geborgd dat medewerkers van dit beveiligings-bedrijf geen toegang kunnen krijgen tot informatie en/of gegevens?	o ja o nee
Toelichting:	
Hoe worden documenten (bijv. taplasten) en verwisselbare gegevensdragers waarop informatie en gegevens zijn vastgelegd bewaard?	
Zijn deze opbergmiddelen deugdelijk beveiligd?	o ja o nee
Waaruit bestaat deze beveiliging?	brandwerende-/braakwerende asten/beide/kluis/.....
Toelichting:	
Worden personen belast met onderhouds- en reparatiewerkzaamheden in de ruimte waarin de informatie en gegevens zich bevinden door eigen geautoriseerd personeel begeleid?	o ja o nee
Waaruit bestaat de fysieke beveiliging van de ruimte(n) waarbinnen hardware staat opgesteld?	
Toelichting:	

6 Beheer van communicatie- en bedieningsprocessen

Er wordt onderscheid gemaakt tussen bevoegd gegeven taplasten afkomstig van justitie en die van de Algemene Inlichtingen en Veiligheidsdienst (AIVD) en Militaire Inlichtingen en Veiligheidsdienst (MIVD). De laatst genoemde diensten beschouwen het afgeven van taplasten aan aanbieders als het buiten de dienst brengen van staatsgeheimen. Deze informatie moet dan ook aangegeven en vastgesteld worden als staatsgeheim (rubriceren). Het volgende deel van de checklist gaat over de rubricering.

Hoe is de status/rubricering van de informatie en gegevens (vertrouwelijk/staatsgeheim) te allen tijde kenbaar gemaakt?	
Toelichting:	
Worden informatie en gegevens op enig moment gereproduceerd en zo ja door wie?	o ja, door: o nee
Indien informatie of gegevens buiten de normale werkruimte worden gebracht, noodzakelijk voor de goede voortgang van de werkzaamheden, wordt de verblijfplaats hiervan dan geregistreerd	o ja o nee
Toelichting:	
Hoe lang blijven taplasten in elektronische of papieren vorm na sluiting van de tap bewaard?	
Toelichting:	
Is er sprake van een boekhouding in elektronische of papieren vorm in verband met het in rekening brengen van administratieve- en personele kosten bij de behoeftestellers (register)	o ja o nee
In geval van verwijdering of vernietiging van informatie en gegevens, hoe vindt dit dan plaats	
Toelichting:	
Geschiedt dit op onomkeerbare wijze?	o ja o nee
Toelichting:	
Wordt van verwijdering of vernietiging rapport opgemaakt?	o ja o nee
Zo ja, krijgt de betrokken bevoegde autoriteit hiervan een afschrift	o ja o nee
Toelichting:	

7 Toegangsbeveiliging van geautomatiseerde informatiesystemen

Ook de informatiesystemen zelf moeten worden beveiligd, zodat alleen gerechtigde personen toegang kunnen krijgen. Beveiliging van geautomatiseerde informatiesystemen kan door middel van persoonsgebonden authenticatie of bijvoorbeeld door gebruik te maken van biometrie. De aanbieder moet alle handelingen met betrekking tot de verwerking van de informatie en gegevens in het geautomatiseerde informatiesysteem vastleggen. Ook de persoonsgebonden gegevens moeten hierbij zijn geregistreerd.

Geef aan de hand van een schema uitleg van de taparchitectuur.	Schema als bijlage	o ja o nee
Wie is de leverancier van de tapapparatuur?	Hardware: Software:	
Wordt er bij het zetten van de tap onderscheid gemaakt tussen gerubriceerde/ongerubriceerde taps?	o ja o nee	
Toelichting:		
Wordt tapapparatuur geprogrammeerd via een stand alone pc of via een (bedrijfs)netwerk?		
Toelichting:		
Indien sprake is van een stand alone pc kan men dan door vervanging van deze pc door een andere ongeautoriseerd toegang verkrijgen?	o ja o nee	
Toelichting:		
Wordt deze communicatie versleuteld?	o ja o nee	
Toelichting:		
Is het verkrijgen van toegang tot geautomatiseerde informatiesystemen, waarin de informatie en de gegevens worden verwerkt, beveiligd door middel van persoonsgebonden authenticatie?	o ja o nee	
Toelichting:		
Wie (bijv. kennisnemers) bezitten deze authenticatie?	Naam: Naam: Naam: Naam:	Functie: Functie: Functie: Functie:
Toelichting:		
Wordt in de authenticatie nog onderscheid gemaakt in rechten (gelaagde autorisatie)?	o ja o nee	
Toelichting:		
Waar zijn deze rechten vastgelegd?		
Toelichting:		
Is het aantal foutieve inlogpogingen is beperkt tot 3?	o ja o nee	

Leidt overschrijding van dit aantal tot definitieve blokkering?	o ja o nee	
Toelichting:		
Wie is geautoriseerd deze blokkering op te heffen?	Naam: Naam: Naam:	Functie: Functie: Functie:
Toelichting:		
Is logische beveiliging zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd?	o ja o nee	
Toelichting:		
Hoe is zeker gesteld dat in dat geval tijdige interventie plaatsvindt?		
Toelichting:		
Door wie wordt geïntervenieerd?	Naam: Naam: Naam:	Functie: Functie: Functie:
Worden alle handelingen met betrekking tot de verwerking van informatie en gegevens in het geautomatiseerde systeem persoonsgebonden gelogd?	o ja o nee	
Toelichting:		
Welke gegevens worden precies gelogd?		
Toelichting:		
Wie is verantwoordelijk voor de bewaking van dit logfile?	Naam: Naam:	Functie: Functie:
Worden de toegangsrechten periodiek geëvalueerd?	o ja o nee	Periodiciteit:

8 Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen

Ook aan de technische ontwikkel- en beheersactiviteiten van geautomatiseerde informatiesystemen zijn eisen gesteld. Voorbeeld: als bij onderhoud op afstand niet in het vereiste beveiligingsniveau kan worden voorzien, zal dit onderhoud op locatie plaats moeten vinden. Onderhoud is in dit geval onder andere bestandsreparatie en (regulier) systeemonderhoud. Reparatie is de meer fysieke reparatie aan de hardware.

Wie is binnen de organisatie verantwoordelijk voor het onderhoud en beheer van de apparatuur alsmede voor het aanbrengen van wijzigingen in hard- of software?	Naam: Naam: Naam:	Functie: Functie: Functie:	
Toelichting:			
Vindt onderhoud aan geautomatiseerde informatie-systemen voor zover deze toegang verschaffen tot informatie en gegevens op locatie plaats?	o ja o nee		
Indien dit onderhoud op afstand plaats vindt, door wie wordt dit dan uitgevoerd?	Naam: Naam: Naam:	Functie: Functie: Functie:	
Hoe is het beveiligingsniveau van de informatie en gegevens in dit geval geborgd? (procedure, registratie wie wanneer onderhoud uitvoert)			
Toelichting:			
Indien reparatie aan het geautomatiseerde infor-matiesysteem waarin de informatie en gegevens worden verwerkt extern plaats vindt, worden deze informatie en gegevens dan onomkeerbaar verwijderd?	o ja o nee		
Toelichting:			
Indien de aanbieder de uitvoering van werkzaamheden uitbesteedt aan een derde en in dat kader de derde kennis neemt of kan nemen van informatie en gegevens, draagt de aanbieder zorg voor een schriftelijke overeenkomst tussen hem en de derde partij. De derde verplicht zich daarin: - geheimhouding te betrachten; - gestelde in BBGAT na te leven; - informatie en gegevens te beveiligen tegen kennisneming door onbevoegden; - medewerking te verlenen aan toezicht.			
Bestaat een dergelijke overeenkomst?	o ja o nee	Kopie als bijlage?	o ja o nee
Toelichting:			