Besluit beveiliging gegevens aftappen

Ronald Eygendaal CSS CISMP

INLEIDING

Telecom operators (Telcos) en Internet Service+ Providers (ISP's) hebben een wettelijk verplichting om het 'netwerkverkeer' van haar klanten en overige informatie over haar klanten zoals NAW gegevens op vordering beschikbaar te maken voor justitiële en staatsveiligheidsopsporingsonderzoeken. Bij staatsveiligheidsopsporingsdiensten moet u denken aan de: Algemene Inlichtingen en Veiligheid Dienst (AIVD) en de Militaire Inlichtingen en Veiligheid Dienst (MIVD)

Globaal zijn de volgende verplichting te onderscheiden.

1. Aftappen van netwerk verkeer; conform Artikel 13.1 en Artikel 13.2 Telecommunicatiewet

2. Verstrekking NAW gegevens klanten; conform Artikel 13.4 Telecommunicatiewet

3. Verstrekking verkeer gegevens van klanten; conform Artikel 13.4 Telecommunicatiewet

Door de hierboven beschreven verplichting voor Telcos en ISP's te introduceren ontstaan grote beveiligingsrisico's zoals het weglekken van informatie en/of gegevens en inbreuk op de beveiliging van geautomatiseerde systemen, bewust al dan niet bewust.

MAATSCHAPPELIJKE BELANGEN VAN BEVEILIGING

In Nederland laten wij er ons op voorstaan, dat de rechtspleging rechtvaardig is. Beide kanten van de zaak krijgen alle aandacht en gelegenheid hun kant van de zaak toe te lichten. En wanneer er twijfel is over de deugdelijkheid van het bewijsmateriaal spreken we liever iemand vrij dan het risico te nemen, iemand onschuldig te veroordelen.

De grote meerwaarde van het Van Tra onderzoek is, dat opnieuw onderstreept is, dat bewijsmateriaal bewijsbaar juridisch deugdelijk moet zijn en volgens de afgesproken regels is verkregen.

Er worden mensen voor lange tijd (soms zelfs levenslang) opgesloten op basis van bewijs, bestaande uit getapte telefoon gesprekken. Ook in die situatie is het essentieel, dat er op dit bewijsmateriaal niets is aan te merken.

Zo dit al geldt voor telefoongesprekken, voor de internet tap is dit van nog veel groter belang. De mogelijkheden van manipulatie op dit punt zijn bijna onbegrensd en het is dan ook een grote zorg, hoe dit opsporingsmiddel ingezet gaat worden. Om slechts 2 eenvoudige voorbeelden te noemen:

1. Iemand breekt in op uw computer en gaat vanaf uw computer allerlei minder frisse websites bekijken en materiaal downloaden.

2. Er worden E-mails verstuurd en ontvangen met uw E-mail adres. Iemand anders gebruikt echter uw E-mail adres, in plaats van uzelf.

Als in situatie 1 een internet tap op uw computer zou staan en in het tweede geval een E-mail tap, zou in beide gevallen een veroordeling volgen, wanneer het tot een rechtszaak zou komen. Een Kafkaachtig scenario.

Het inzetten van bijzondere opsporingsmiddelen, zoals direct afluisteren en het aftappen van telefoongesprekken maakt een ernstige inbreuk op de privacy van de betrokkene. Het is daarom van groot maatschappelijk belang dat er op dit punt geen enkele twijfel bestaat over de juistheid van het toepassen van deze opsporingsmiddelen. Dat geldt voor zowel de wetgeving en afgesproken regels op dit punt als de feitelijke toepassing in een onderzoek.

In een aantal heeft twijfel over de juistheid geleid tot schade claims van 'gedupeerde' klanten.

Naar een discussie van enkele jaren, met de overheid, over de beveiliging van gegevens en aftappen is de overheid met een 'besluit beveiliging gegevens aftappen' gekomen.

In Nederland laten wij er ons op voorstaan, dat de rechtspleging rechtvaardig is.

Het betrouwbaarheids-onderzoek is een pure administratieve aangelegenheid.

De artikelen van het besluit houden het volgende in:

Art 2 globale maatregelen

De maatregelen zoals voorgesteld in het 'besluit beveiliging gegevens aftappen' omvat een vijftal hoofdmaatregelen te weten;

1. Personen
2. Gebouwen en ruimten
3. Beveiliging informatiesystemen
4. Voorkomen, vaststellen en onderzoeken van inbreuk
5. Calamiteiten.

Tot deze maatregelen behoren in ieder geval die genoemd in de bijlage van het 'besluit beveiliging gegevens aftappen'. Opgemerkt wordt dat daar waar gesproken wordt over 'alle noodzakelijke beveiligingsmaatregelen', beter gesproken kan worden over 'beveiligingsmaatregelen naar redelijke stand van de techniek'. Op deze manier kan de regeling ook beter met zijn tijd meegaan. Te weinig wordt nu rekening gehouden met toekomstige ontwikkelingen.

Art 3 beveiligingsplan

Artikel 3 regelt dat er een beveiligingsplan moet zijn. De maatregelen en de uitwerking daarvan moeten worden vastgelegd in dit beveiligingsplan. De overheid heeft de bevoegdheid om dit beveiligingsplan te toetsen. Het beveiligingsplan moet tenminste bestaan uit de in de bijlage van het 'besluit beveiliging gegevens aftappen' genoemde maatregelen.

De Code voor informatiebeveiliging geeft een goed kader om de beveiligingsmaatregelen in te richten en uit te werken.

Art 4 uitvoering

Artikel 4 legt aan de Telco's en/of ISP de verplichting op dat de werkzaamheden moeten worden uitgevoerd door betrouwbare personen.

Wat zijn nu Betrouwbaarheidspersonen? Onder betrouwbare personen, zoals omschreven in het eerste lid, wordt verstaan personen welke een vertrouwensfunctie hebben zoals bedoeld in de Wet Veiligheidsonderzoeken. Om werkzaamheden voor de Algemene Inlichtingen en Veiligheid Dienst en/of de Militaire Inlichtingen en Veiligheid Dienst uit te voeren moet men een vertrouwensfunctie bekleden.

Bij de vertrouwensfuncties kunnen drie categorieën worden onderscheiden: A, B en C. Bij een A functie kan men de belangen van de staat meer schade toebrengen dan bij een B of C functie. Voor Telco's en ISP's is een B vertrouwensfunctie voldoende. Bij de grote Telco's is een A vertrouwensfunctie gewenst.

Daarnaast vigeert in Nederland de 'Wet particuliere beveiligingsorganisaties en recherchebureaus'. Deze wet regelt taken en bevoegdheden van de particuliere beveiligingsbranche en stelt de wettelijke eisen ten aanzien van opleiding, betrouwbaarheid personeel (screening), uniformering en legitimering.

Het betrouwbaarheidsonderzoek is een pure administratieve aangelegenheid. Het gaat om de betrouwbaarheid van beveiligingsmedewerkers en het verlenen van toestemming om als zodanig te werken. Of een persoon mag worden belast met beveiligingswerkzaamheden is afhankelijk van een onderzoek naar de betrouwbaarheid (screening) dat door de politie wordt verricht. De verklaring van betrouwbaarheid wordt afgegeven door de korpschef van het politiekorps in de regio waar de desbetreffende persoon woonachtig is.

Dit onderzoek gebeurt bij iedere beveiligingsbeambte, particulier rechercheur en horecaportier voordat deze in het bezit wordt gesteld van een legitimatiebewijs.

Het ziet er naar uit dat 'besluit beveiliging gegevens aftappen' een tweetal extra vormen van betrouwbaarheidsonderzoek toevoegt; de zogenaamde 'vertrouwensfunctie' zoals bedoeld in de Wet veiligheidsonderzoeken (Wvo) en een verklaring zoals bedoeld in de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag.

Met name tussen de verklaringen omtrent het gedrag en het onderzoek naar de betrouwbaarheid zoals dat door de politie wordt verricht zit discrepantie.

Art 5. Melding incidenten

Dit artikel verplicht de Telco en/of ISP tot melden van veiligheidsincidenten in technische apparatuur en/of veiligheidsprocessen, ten behoeve van het nakomen van wettelijk verplichtingen, wanner er sprake is van inbreuk heeft plaats gevonden.

Verder is de Telco en/of ISP verplicht te vermelden welke maatregelen zijn genomen om verdere ontsluiting van informatie en/of gegeven tegen te gaan.

Overtredingen van de voorschriften wordt gezien als een strafbaar delict.

Art 6. geheimhouding

Artikel 6 regelt alles rond geheimhouding. Alle personeelsleden werkzaam aan of met systemen en of processen benodigd voor het uitvoeren van justitiële en staatsveiligheidsopsporingsonderzoeken dienen een geheimhoudingsverklaring te onderteken.

Als aanvullende maatregel wordt in het 'besluit beveiliging gegevens aftappen' gesproken over een geheimhoudingsverklaring. In de context van het besluit moet dit, mijn inziens, worden gelezen als een verklaring opgesteld tussen werknemer en werkgever.

Uit de toelichting blijkt dat ook nog artikel 272 van het Wetboek van Strafrecht van toepassing is.

Wetboek van Strafrecht.

Artikel 272 GEHEIMHOUDING.

1. Hij, die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep, of wettelijk voorschrift dan wel vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met een gevangenisstraf van ten hoogste één jaar of een geldboete van de vierde categorie.
2. Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

BIJLAGE ALS BEDOELD IN ARTIKELEN 2 EN 3

Beveiligingseisen algemeen

De beveiligingseisen algemeen regelen dat er bij een Telco en/of ISP een functionaris is, die belast is met toezicht op uitvoering en de naleving van beveiligingsmaatregelen. Ook wordt van deze functionaris verwacht dat er regelmatig controles plaats vinden.

Vreemd is dat er in de beveiligingseisen algemeen geen harde eisen ten aanzien van functiescheiding zijn opgenomen

Beveiligingseisen ten aanzien van personeel

In deze eis worden de verplichtingen uit artikel 6 nader uitgewerkt. Het draait om functie beschrijvingen, geheimhoudingsverklaring en toegang tot informatie.

Fysieke beveiliging en beveiliging van de omgeving

In de bijlage van 'besluit beveiliging gegevens aftappen' wil men de informatie en de gegevens zoveel mogelijk concentreren in één ruimte. Als we dit vertalen naar techniek dan zien we een bijna onmogelijk eis, immers het uitkoppelen van netwerkverkeer, ten behoeve van het nakomen van wettelijk verplichtingen, gebeurd op verschillende fysieke locaties. Vanaf deze locaties wordt dit verkeer gerouteerd naar een centraal punt. Vanaf dit centrale punt wordt de informatie verstuurd naar een centraal punt bij de overheid, waar verdere verwerking plaats vindt.

In zowel de Justitiële Tap Standaard (JTS) als in de Transport of Intercepted IP Traffic (TIIT) standaard, is het toegestaan op netwerk elementen op verschillende fysieke locaties geïnstalleerd en in gebruik te hebben (JTS en TIIT standaarden worden gebruikt om bij de Telco en/of ISP afgetapt verkeer te verzenden naar de overheid.)

Verder eist men een 'deugdelijke fysieke beveiliging'. Wat de wetgever verstaat onder deugdelijk is onduidelijk. Echter harde eisen zoals we die bijvoorbeeld zien bij het Politie Keurmerk Veilig Wonen ontbreken waardoor de kans ontstaat dat het uiteindelijk niveau van beveiliging nog minder is dan de beveiliging van een woonhuis.

Praktische gezien gaat het hierom bouwkundige beveiliging. Bouwkundige maatregelen zijn bedoeld om de poging tot indringen van gebouwen, terreinen zo moeilijk en onaantrekkelijk mogelijk te maken.

De belangrijkste onderdelen van de eerste en/of tweede beveiligingsschil zijn de bouwkundige en mechanische beveiliging. Dit zijn zaken zoals gevelelementen, ramen, deuren, kozijnen en uiteraard het hang- en sluitwerk. Verder kan men denken aan het vormen van compartimenten, voor opslag van

Overtredingen van de voorschriften wordt gezien als een strafbaar delict.

speciale of waardevolle goederen, door bepaalde ruimtes bouwkundig zo te versterken dat de inbraak- en brandvertraging maximaal is. Ook kluizen en brandkasten zijn onderdeel van de bouwkundige beveiliging.

Een ander eist dat 'ongeautoriseerde toegang en poging daartoe worden gedetecteerd en dat tijdige interventie plaats vindt'. Dit komt neer op een elektronisch inbraakdetectiesysteem (ook wel alarminstallatie genoemd) en alarmopvolging.

Elektronische inbraakdetectiesystemen waarbij alarmopvolging, door een particuliere beveiligingsdienst en/of de politie gewenst is, moeten, zoals omschreven in de 'Wet particuliere beveiligingsorganisaties en recherchebureaus', voorzien zijn van een BORG certificaat.

BORG is een kwaliteitssysteem zodat beveiligingsbedrijven garant kunnen staan voor het leveren van kwalitatief goede beveiligingsdiensten en/of producten. Als een product of dienst geleverd is kan een klant hiervoor een schriftelijke bewijs ontvangen; het zogenaamde BORG certificaat. BORG kent een 4-tal risicoklassen waarvan 1 het laagste risico is en 4 de hoogste.

Uiteraard zullen we de fysieke toegang tot de ruimten en/of compartimenten waar de technische apparatuur staat opgesteld, moeten beheren, ten behoeve van het nakomen van wettelijke verplichtingen. Gedacht kan worden aan het gebruik van een toegangsverleningssysteem welke is aangesloten op de deur van de ruimten en/of het compartimenten. Door middel van het aanbieden van pasjes, ook wel badges genoemd, aan een naast de deur hangende lezer, kan toegang worden verkregen.

Hierdoor ontstaat gecontroleerde en herleidbare toegang en als men er voor zorgt dat pasje persoonsgebonden zijn dan kan men de toegang op individueel niveau beheren.

Hiermee voldoen we aan een deel van de eisen welke geformuleerd staan in 'besluit beveiliging gegevens aftappen'. Het gaat dan om de eisen 'daartoe geautoriseerde personen' en 'gecontroleerde en achteraf herleidbare toegang op individueel niveau'.

Iets verder in de bijlage van de regeling wordt het volgende gesteld: 'Documenten waarin, dan wel verwisselbare gegevensdragers waarop, de informatie en de gegevens zijn vastgelegd worden in deugdelijk beveiligende opbergmiddelen bewaard'.

Hiervoor zou een inbraakwerende kluis en/of brandkast kunnen worden gebruikt. Uiteraard verdient een brand- en inbraakwerende kast de voorkeur. Deze zal conform BORG regelgeving geïnstalleerd meten worden.

De laatste eis in dit hoofdstuk gaat over begeleiding van onderhouds- en reparatiewerkzaamheden. De volgens 'Wet particuliere beveiligingsorganisaties en recherchebureaus' gescreende beveiligingsmedewerkers kunnen dit uitvoeren. Praktisch gezien zou een contact met een beveiligingsbedrijf welke mobiele surveillanten hebben uitkomst kunnen bieden. In geval van onderhoud en/of reparatie zou de mobiele surveillanten de begeleiding op zich kunnen nemen.

Beheer van communicatie en bedieningsprocessen

Het tonen van de status/rubricering van staatsgeheim of vertrouwelijk op een fysieke zaken zoals documenten en gegevensdragers vergt weinig inspanning en kan zonder problemen worden geïmplementeerd. De eis om de status/rubricering zichtbaar te maken op een beeldscherm betekent dat de geautomatiseerde systemen, ten behoeve van het nakomen van wettelijke verplichtingen, ingrijpend gewijzigd moeten worden.

De eis om de status/rubricering zichtbaar te maken op een beeldscherm voegt, gezien vanuit een beveiligingsoptiek, niets toe aan de beveiliging. Een gelaagde manier van toegangsverlening zou een oplossing kunnen zijn. Personen met een vertrouwensfunctie A krijgen dan toegang tot staatsgeheim en vertrouwelijk en personen met een vertrouwensfunctie B uitsluitend tot vertrouwelijk.

De eisen over reproductie, vervoer en opslag buiten de beveiligde ruimte en de eisen over verwijdering en vernietiging zijn normale goed toepasbare beveiligingseisen. In de dagelijkse beveiligingspraktijk doen we dit ook al met onze bedrijfsinformatie.

Toegangsbeveiliging van geautomatiseerde informatiesystemen

De eisen met betrekking tot de logische toegangsbeveiliging van de informatiesystemen zoals beperking van het aantal inlog-pogingen en persoonsgebonden wachtwoorden die eenmaal per

BORG is een kwaliteitssysteem zodat beveiligingsbedrijven garant kunnen staan voor het leveren van kwalitatief goede beveiligingsdiensten en/of producten.

maand wijzigen zijn zo basaal dat implementatie op vrijwel elk systeem mogelijk is.

Anders zit het met detectie en de interventie op het aantal inlog-pogingen. Het is niet altijd mogelijk om deze pogingen te detecteren en vervolgens daarop acties uit te zetten

Als we dit goed willen doen, dan zouden we de toegang tot de geautomatiseerde informatiesystemen bijvoorbeeld via een biometrisch device kunnen regelen, want alleen dan kan er persoonsgebonden toegang worden geforceerd.

Uiteraard zullen zaken zoals beeldschermbeveiliging automatisch moeten inschakelen na ongeveer 5 minuten inactiviteit op het informatiesysteem. Door middel van het ingeven van wachtwoord kunnen de activiteiten op het systeem weer worden hervat.

Audit trail functies zullen moeten worden geïmplementeerd zodat aan de eis van 'alle handelingen met betrekking tot de verwerking van de informatie en de gegevens in het geautomatiseerde informatiesysteem worden persoonsgebonden vastgelegd ten einde onderzoek mogelijk te maken' kan worden voldaan.

Ook zal de administratieve organisatie zoals processen voor beheerder, aanvragen toegangsrechten en de autorisatie matrix ingericht moeten zijn. Ook deze eisen zijn verwoord in dit hoofdstuk.

Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen

De eisen welke in dit hoofdstuk van de bijlage geformuleerd zijn, hebben betrekking op alle technische ontwikkel- en beheeractiviteiten van geautomatiseerde informatiesystemen. Er zitten niet veel echte beveiligingseisen in dit hoofdstuk; toch is er iets wat we er willen uitlichten.

De eisen met betrekking tot betrouwbare personen, zoals omschreven in de Wet veiligheidsonderzoeken (Wvo) kan in de praktijk de nodige problemen geven. De gebruikte technische systemen worden vaak in het buitenland ontwikkeld en vaak ook het buitenland beheerd. Het komt er dus op neer dat de leverancier betrouwbare personen in dienst zal moeten hebben. Of dit gezien de vrijmarktwerking juist is, moet worden bezien.

Conclusies

Als we de hele keten van gegevens bekijken, dus van Telco en/of ISP via publieke netwerken naar uiteindelijk een tapkamer bij de overheid, dan zou ketenbeveiliging het uitgangspunt moeten zijn. Er hoort een spiegelbepaling te zijn met beveiligingsvoorschriften voor de beveiliging van afgetapte gegevens bij de overheid.

Overigens zal het 'besluit beveiliging gegevens aftappen' niet leiden tot structurele verbeteringen op het gebied van de (informatie)beveiliging. Dit komt omdat de maatregelen onvoldoende en zelfs incompleet zijn. Daarnaast zijn er geen industrienormen en/of kwaliteitssystemen zoals BORG en de Code voor informatiebeveiliging voorgeschreven.

Men ontneemt de burger niet het 'big brother is watching you' gevoel. De Kafka-achtige scenario's blijven dus mogelijk.

Het heeft er alle schijn van dat men de kosten die gemaakt moeten worden voor goede beveiligingen niet wil maken, waardoor het risico van inbreuk op privacy aanzienlijk wordt vergroot.

Over de auteur: Ronald Eygendaal is werkzaam als Security consultant voor Vizzavi, heeft meer dan 10 jaar ervaring in beveiliging en informatiebeveiliging in het bijzonder; is voorzitter van de vakgroep ICT beveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN); lid van het International Advisory Board van de International Foundation for Protection Officers (IFPO), is Certified Security Supervisor (CSS) en Certificate in Information Security Management Principles (CISMP).

Men ontneemt de burger niet het 'big brother is watching you' gevoel.