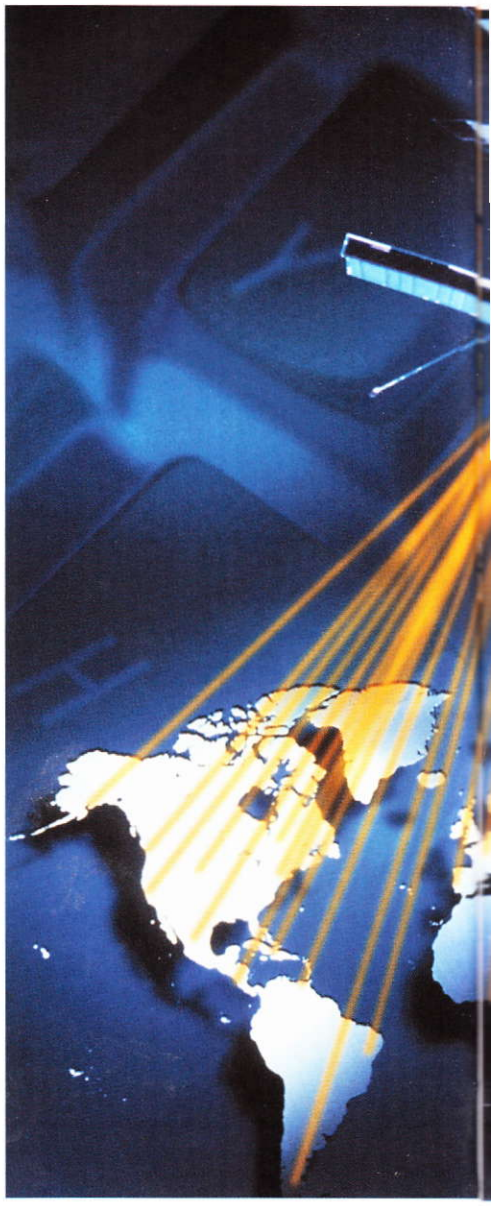
R. Eygendaal CSS CISMP*

De Telecommunicatiewet:

Handig voor opsporing,

Telecom operators (Telcos) en Internet Service Providers (ISP's) zijn conform de Telecommunicatiewet verplicht om bepaalde gegevens van klanten op vordering beschikbaar te maken voor justitiële en opsporingsonderzoeken voor de staatsveiligheid. Het kan daarbij gaan om gegevens over het netwerkverkeer, NAW-gegevens en andere informatie. Deze verplichting kan grote beveiligingsrisico's met zich meenemen, zoals het weglekken van informatie en de kans op inbraak in de beveiliging van geautomatiseerde systemen.



Management-summary

Volgens de Telecommunicatiewet zijn Telecom operators (Telcos) en Internet Service Providers (ISP's) verplicht om gegevens over het netwerkverkeer, NAW-gegevens en andere informatie op vordering beschikbaar te maken voor justitiële en opsporingsonderzoeken voor de staatsveiligheid. Door deze bepaling ontstaan wel beveiligingsrisico's. Een internettap is namelijk eenvoudig te manipuleren en vormt al snel een inbreuk op de privacy. Het is dan ook essentieel dat er geen enkele twijfel bestaat over de juistheid van het toepassen van internettaps.

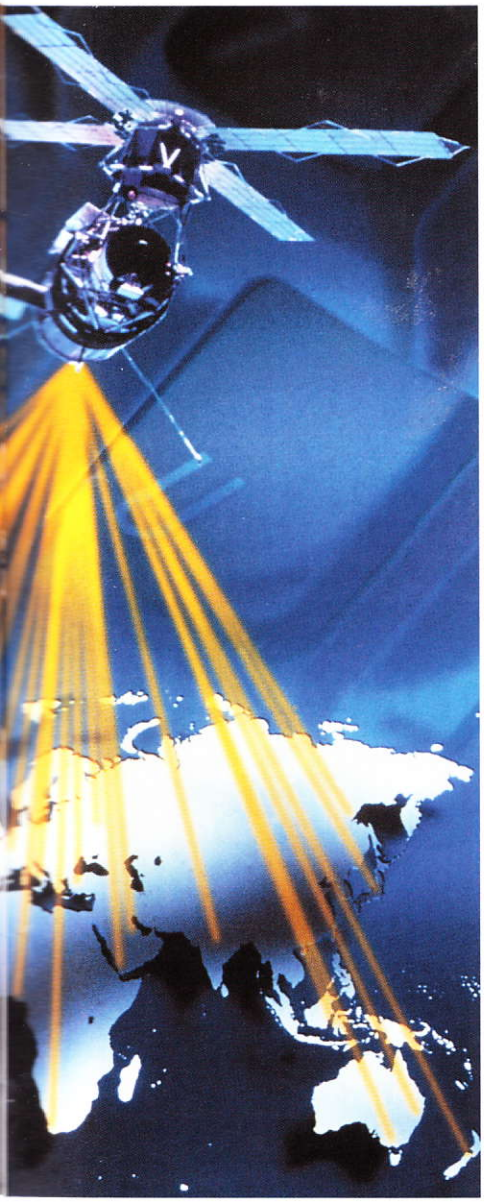
In Nederland laten wij ons er op voorstaan dat de rechtspleging rechtvaardig is. Beide partijen krijgen tijdens een rechtzaak alle aandacht en gelegenheid hun zaak toe te lichten. En wanneer er twijfel is over de deugdelijkheid van het bewijsmateriaal spreken we liever iemand vrij, dan het risico te nemen iemand onschuldig te veroordelen.
De grote meerwaarde van het Van Tra-onderzoek is dat 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 telefoongesprekken. Ook in die situatie is het essentieel dat er op dat bewijsmateriaal niets is aan te merken.
Zo dit al geldt voor telefoongesprekken, voor de internettap is het 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 twee eenvoudige voorbeelden te noemen: Iemand breekt in op uw computer en gaat vanaf die computer allerlei minder frisse websites bekijken en materiaal downloaden. Er worden e-mails verstuurd en ontvangen met uw e-mailadres. Iemand anders gebruikt echter uw e-mailadres, in plaats van uzelf.
Als in de eerste situatie een internettap op uw computer zou staan en in het tweede geval een e-mailtap, zou in beide gevallen een veroordeling volgen wanneer het tot een rechtszaak zou komen. Een Kafka-achtig scenario.

Inbreuk

Het inzetten van bijzondere opspo-

* werkzaam als Security consultant voor Vizzavi

# of juist riskant?



ringsmiddelen, 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 dat 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 rechtszaken heeft de twijfel over de correctheid en juistheid van een tap geleid tot schadeclaims bij Telcos en ISP's. Deze waren ingediend door 'gedupeerde' (afgetapte) klanten.
Na 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.

Hoofdmaatregelen

De maatregelen zoals voorgesteld in het besluit beveiliging gegevens aftappen omvat een vijftal hoofdmaatregelen (Artikel 2 globale maatregelen), te weten: Personen, gebouwen en ruimten, beveiliging van informatiesystemen, voorkomen, vaststellen en onderzoeken van inbreuk en ten slotte calamiteiten.
Tot deze maatregelen behoren in ieder geval die genoemd in de bijlage van het besluit beveiliging gegevens aftappen, die verderop in dit artikel besproken zal worden.
Opgemerkt wordt dat daar waar gesproken wordt over 'alle noodzakelijke beveiligingsmaatregelen' beter gesproken had kunnen worden over 'beveiligingsmaatregelen naar redelijke stand van de techniek'. Op die manier kon de regeling dan ook beter met zijn tijd meegaan. Er wordt nu te weinig rekening gehouden met nieuwe ontwikkelingen.
Artikel 3 regelt dat er een beveiligingsplan moet zijn. De maatregelen en de uitwerking daarvan moeten worden vastgelegd in het beveiligingsplan. De overheid heeft de bevoegdheid om dat plan 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.

Betrouwbaar

Artikel 4 legt aan de Telco's of ISP's de verplichting op dat de werkzaamheden uitgevoerd moeten worden door betrouwbare personen.
Maar wat zijn nu betrouwbare personen? Hieronder, 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 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.

Administratief

Het betrouwbaarheidsonderzoek is een puur 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. Dat onderzoek gebeurt bij iedere beveiligingsbeambte, particulier rechercheur, bodyguard en horecaportier voordat deze in het bezit wordt gesteld van een legitimatiebewijs.
Het ziet er naar uit dat het 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. Tussen de verklaringen betreffende het gedrag en het onderzoek naar de betrouwbaarheid zoals dat door de politie wordt verricht zit discrepantie.

Melding

Artikel 5 verplicht de Telco en ISP tot melden van veiligheidsincidenten in technische apparatuur of veiligheidsprocessen ten behoeve van het nakomen van wettelijke verplichtingen. Er moet gemeld worden wanneer er sprake is van inbreuk en wanneer die inbreuk heeft plaatsgevonden. Verder is de Telco en ISP verplicht te vermelden welke maatregelen zijn genomen om verdere ontsluiting van informatie of gegevens tegen te gaan. Overtredingen van deze voorschiften wordt gezien als een strafbaar (economisch) delict.

Wetboek van Strafrecht.

Artikel 272 GEHEIMHOUDING.

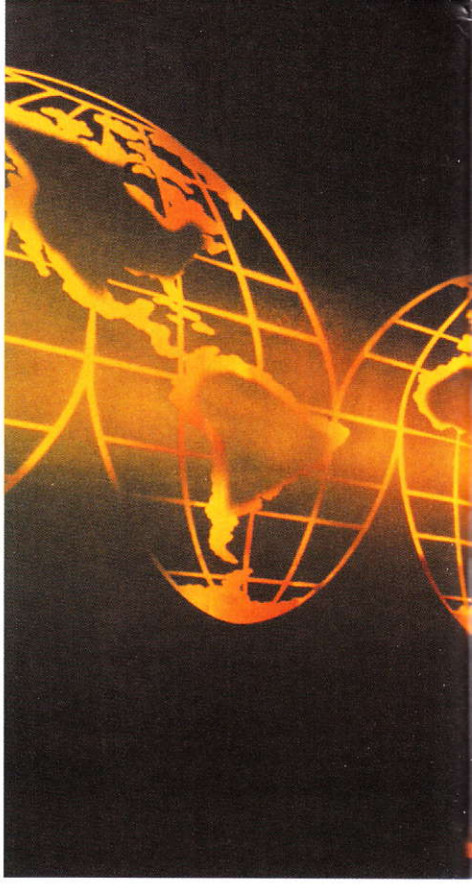
1. Hij, die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep, of wettelijk voorschrift dan wel vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met een gevangenisstraf van ten hoogste één jaar of een geld boete van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

Geheimhouding

Artikel 6 regelt alles rond geheimhouding. Alle personeelsleden werkzaam aan of met systemen of processen die nodig zijn voor het uitvoeren van justitiële- en opsporingsonderzoeken voor de staatsveiligheid 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 dat worden gelezen als een verklaring opgesteld tussen werknemer en werkgever. Uit de toelichting blijkt dat artikel 272 van het Wetboek van Strafrecht ook nog van toepassing is (zie kader).
Artikel 7 geeft de grenzen van uitbesteding aan. Het verplicht de partijen om een contractuele overeenkomst te hebben. Het artikel regelt de medewerking aan toezicht op de geheimhouding en de naleving van beveiligingsmaatregelen. Ook wijst het artikel de Telco of ISP als eindverantwoordelijke aan.
In de bijlage als bedoeld in de artikelen 2 en 3 zijn de volgende dingen opgenomen: De beveiligingseisen algemeen regelen dat er bij een Telco en ISP een functionaris is die belast is met toezicht op de uitvoering en naleving van beveiligingsmaatregelen. Ook wordt van deze functionaris verwacht dat er regelmatig controles plaatsvinden.
Vreemd is dat er in de beveiligingseisen algemeen geen harde eisen ten aanzien van functiescheiding zijn opgenomen.
In de beveiligingseisen ten aanzien van personeel worden de verplichtingen uit artikel 6 nader uitgewerkt. Het draait om functiebeschrijvingen, geheimhoudingsverklaring en toegang tot informatie.
In de bijlage van het besluit beveiliging gegevens aftappen over fysieke beveiliging en de beveiliging van de omgeving wil men de informatie en de gegevens zoveel mogelijk concentreren in één ruimte. Als we dit vertalen naar techniek dan zien we een bijna onmogelijke eis, immers het uitkoppelen van netwerkverkeer ten behoeve van het nakomen van wettelijke verplichtingen gebeurt op verschillende fysieke locaties. Vanaf deze locaties wordt dat verkeer gerouteerd naar een centraal punt. Vanaf daar wordt de informatie verstuurd naar een centraal punt bij de overheid, waar verdere verwerking en analyse plaatsvindt.

Fysieke locaties

In zowel de Justitiële Tap Standaard (JTS) als in de Transport of Intercepted IP Traffic (TIIT) standaard is het toegestaan netwerkelementen op verschillende fysieke locaties geïnstalleerd en in gebruik te hebben.
Verder eist men een 'deugdelijke



fysiek beveiliging'. Wat de wetgever verstaat onder deugdelijk is onduidelijk. Harde eisen zoals we die bijvoorbeeld zien bij het Politie Keurmerk Veilig Wonen ontbreken echter, waardoor de kans ontstaat dat het uiteindelijke niveau van beveiliging nog lager is dan de beveiliging van een woonhuis. Praktisch gezien gaat het hier om bouwkundige beveiliging. Bouwkundige maatregelen zijn bedoeld om het indringen van gebouwen en terreinen zo moeilijk en onaantrekkelijk mogelijk te maken.
De belangrijkste onderdelen van de eerste en tweede beveiligingsschil zijn bouwkundige en mechanische beveiliging. Dat zijn zaken zoals gevelelementen, ramen, deuren, kozijnen en uiteraard het hang- en sluitwerk. Verder kan men denken aan het vormen van compartimenten voor de opslag van speciale of waardevolle goederen door bepaalde ruimtes bouwkundig zo te versterken dat de inbraak- en brandvertraging maximaal zijn. Ook kluizen en brandkasten zijn onderdeel van bouwkundige beveiliging.

Detectiesystemen

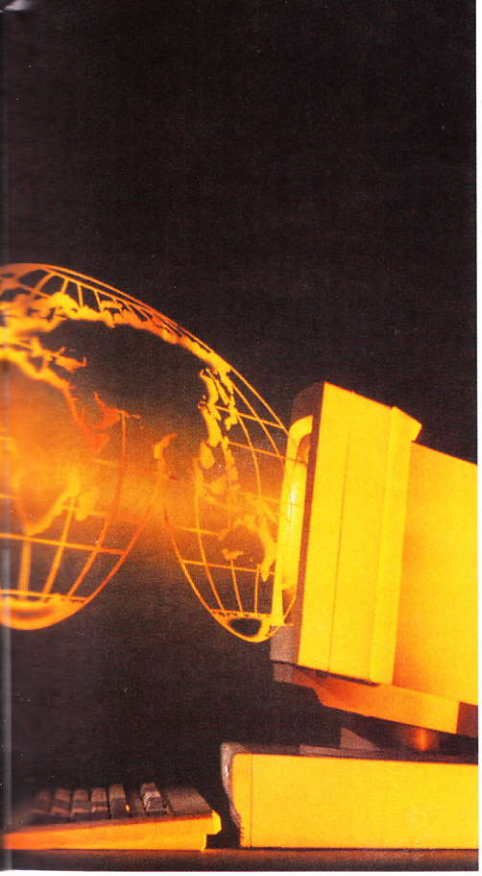
Een andere beveiligingseis ten aanzien van personeel is dat 'ongeautoriseerde toegang en poging daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt'. Dit komt neer op een elektronisch inbraakdetectiesysteem (ook wel alarminstallatie genoemd) en alarmopvolging. Elektronische inbraakdetectiesystemen waarbij alarmopvolging door een particuliere beveiligingsdienst of de politie gewenst is moeten voorzien zijn van een BORG-certificaat. Dat staat in de Wet particuliere beveiligingsorganisaties en recherchebureaus. BORG is een kwaliteitssysteem dat er voor zorgt dat beveiligingsbedrijven garant kunnen staan voor het leveren van kwalitatief goede beveiligingsdiensten en producten. Als een product of dienst geleverd is kan een klant hiervoor een schriftelijk bewijs ontvangen; het zogenaamde BORG-certificaat. BORG kent een viertal risicoklassen, waarvan één het laagste risico is en vier het hoogste.
Uiteraard zullen we de fysieke toegang tot de ruimten en de compartimenten waar de technische apparatuur staat opgesteld moeten beheren. Gedacht kan worden aan het gebruik van een toegangsverleningssysteem dat is aangesloten op de deur van de ruimte of het compartiment. Door middel van het aanbieden van enkele pasjes aan een lezer kan toegang worden verkregen.
Hierdoor ontstaat een gecontroleerde en herleidbare toegang. Als er bovendien voor gezorgd wordt dat pasjes persoonsgebonden zijn kan de toegang op individueel niveau beheerd worden.
Hiermee voldoen we aan een deel van de eisen die geformuleerd staan in het besluit beveiliging gegevens aftappen. Het gaat dan om de eisen 'daartoe geautoriseerde personen' en 'gecontroleerde en achteraf herleidbare toegang op individueel niveau'.

Reparatie

Iets verder in de bijlage van de regeling wordt het volgende gesteld: 'Documenten of verwisselbare gegevensdragers waar de informatie en de gegevens in zijn vastgelegd worden in deugdelijk beveiligende opbergmiddelen bewaard'.
Hiervoor zou een inbraakwerende kluis of brandkast kunnen worden gebruikt. Uiteraard verdient een brand- en inbraakwerende kast de voorkeur. Deze zal conform BORG-regelgeving geïnstalleerd moeten worden.
De laatste eis in dit hoofdstuk gaat over de begeleiding van onderhouds- en reparatiewerkzaamheden. Volgens de Wet particuliere beveiligingsorganisaties en recherchebureaus moeten gescreende beveiligingsmedewerker die werkzaamheden uitvoeren. Praktisch gezien zou een contract met een beveiligingsbedrijf met mobiele surveillanten uitkomst kunnen bieden, want deze surveillanten kunnen dan de begeleiding op zich nemen.

Rubricering

Het tonen van de status of rubricering (staatsgeheim of vertrouwelijk) op documenten en gegevensdragers vergt weinig inspanning en kan zonder problemen worden geïmplementeerd. De eis om de status of rubricering zichtbaar te maken op een beeldscherm betekent dat de geautomatiseerde systemen ingrijpend gewijzigd moeten worden ten behoeve van het nakomen van wettelijke verplichtingen.
Deze eis voegt niets toe aan de beveiliging. Een gelaagde manier van toegangsverlening zou een oplossing kunnen zijn. Personen met een vertrouwensfunctie A krijgen dan toegang tot documenten met het etiket '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.

Inlog-pogingen

De eisen met betrekking tot de logische toegangsbeveiliging van informatiesystemen, zoals beperking van het aantal inlog-pogingen en persoonsgebonden wachtwoorden die eenmaal per maand wijzingen, zijn zo basaal dat implementatie op vrijwel elk systeem mogelijk is. Anders zit het met detectie en de interventie op het aantal inlogpogingen. Het is niet altijd mogelijk om deze pogingen te detecteren en vervolgens acties uit te zetten. Als we dit goed willen doen zouden we de toegang tot de geautomatiseerde informatiesystemen bijvoorbeeld via een biometrisch device kunnen regelen, want alleen dan kan er persoonsgebonden toegang worden geforceerd of afgedwongen.
Uiteraard zullen zaken zoals beeldschermbeveiliging automatisch moeten inschakelen na ongeveer vijf minuten inactiviteit op het informatiesysteem. Door middel van het ingeven van een wachtwoord kunnen de activiteiten op het systeem weer worden hervat. Audit-trail-functies zullen moeten worden geïmplementeerd, zodat aan de eis kan worden voldaan 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'.
Ook zal de administratieve organisatie en de autorisatiematrix ingericht moeten zijn. Deze eisen zijn ook verwoord in dit hoofdstuk.

Onderhoud

De eisen die in het hoofdstuk 'Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen' van de bijlage geformuleerd zijn, hebben betrekking op alle technische ontwikkel- en beheeractiviteiten van geautomatiseerde informatiesystemen. Er staan niet veel echte beveiligingeisen in dat hoofdstuk, maar toch is er iets wat we er uit willen lichten. De eisen met betrekking tot betrouwbare personen, zoals aan omschreven in de Wet veiligheidsonderzoeken (Wvo), kunnen in de praktijk de nodige problemen geven. De gebruikte technische systemen worden vaak in het buitenland ontwikkeld en technisch beheerd. Het komt er dus op neer dat de leverancier betrouwbare personen in dienst zal moeten hebben. Of dit gezien de vrije markt werking juist is moet worden bezien.

Spiegelbepaling

Als we alle gegevens bekijken, dus van Telco en ISP via publieke netwerken uiteindelijk naar 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. Deze is nog niet aanwezig.
Overigens zal het besluit beveiliging gegevens aftappen niet leiden tot structurele verbeteringen op het gebied van de (informatie)beveiliging. Dat komt doordat de maatregelen onvoldoende en zelfs incompleet zijn. Daarnaast zijn er geen industrienormen 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 voor een goede beveiliging niet wil maken, waardoor het risico van inbreuk van privacy aanzienlijk wordt vergroot.

Oplossingsrichting

Het is een zware belasting voor een Telco en ISP om een proces 24 uur, zeven dagen per week beschikbaar te hebben voor de overheid. De wet verplicht immers een Telco en ISP om terstond een taplast uit te kunnen voeren. Of dat nu op onmenselijke tijden is of niet wordt niet als relevant beschouwd.
Praktisch gezien liggen hier commerciële kansen voor particuliere beveiligingsorganisaties om dit soort werkzaamheden uit te voeren. Een Particuliere AlarmCentrale (PAC) moet voldoen aan een heel stelsel van fysieke en organisatorische beveiligingsmaatregelen. Door de Wet particuliere beveiligingsorganisaties en recherchebureausgescreende beveiligingsmedewerker kunnen deze relatief eenvoudige werkzaamheden uitvoeren. Al sinds 1998 is één van de grote particuliere beveiligingsorganisaties actief met dit soort werkzaamheden. Echter dit gebeurt vanuit de bedrijfsalarmcentrale van de Telco. Het is dan ook een gemiste kans voor zowel de overheid en de Telco's en ISP's als de particuliere beveiligingsbranche dat een discussie over uitbesteding van deze werkzaamheden nooit heeft plaatsgevonden.