

# GEVOLGEN VAN DE WET BEWAARPLICHT TELECOMMUNICATIE- GEGEVENS

## *UITGEBREIDE DATARETENTIEPLICHT VOOR TELECOMAANBIEDERS EN INTERNETPROVIDERS*

Door Frans Plat

ALS ONDERDEEL VAN DE NIEUWE TELECOMMUNICATIEWET IS OOK DE WET BEWAARPLICHT TELECOMMUNICATIEGEGEVENS VAN KRACHT GEWORDEN. DE WET IS EEN UITVLOEISEL VAN DE EUROPESE RICHTLIJN DATARETENTIE. DE WET VERGROOT DE MOGELIJKHEDEN VAN DIGITAAL SPORENONDERZOEK BIJ DE BESTRIJDING VAN TERRORISME EN ANDERE CRIMINALITEIT. VOOR TELECOMAANBIEDERS EN INTERNETPROVIDERS KAN DE UITBREIDING VAN DE WET TOT FORSE INFRASTRUCTURELE AANPASSINGEN LEIDEN.

**P**er 1 september 2009 is in Nederland de *Wet bewaarplicht telecommunicatiegegevens* van kracht geworden. Deze wet is opgenomen in de (nieuwe) Telecommunicatiewet en het Wetboek van strafvordering. Het Agentschap Telecom houdt toezicht op de naleving van de wet. Bij overtreding van de wet kunnen boetes tot maximaal € 450.000 worden opgelegd en kan tot strafvervolgung worden overgegaan.





De wet is een uitvloeisel van de Europese Richtlijn inzake de bewaarplicht ten aanzien van telecomgegevens, ook wel de *Richtlijn Dataretentie* genoemd. Aanleiding voor de Richtlijn waren in 2004 de aanslagen in Madrid. Duidelijk werd dat voor onderzoek en vervolging, bij terrorisme en andere vormen van criminaliteit, snelle toegang tot telecommunicatiegegevens noodzakelijk is.

#### GEGEVENS VAN TELECOM- EN INTERNETPROVIDERS

Onder de vorige Telecommunicatiewet waren telecomaanbieders sinds 2004 al verplicht om naw-gegevens (naam, adres en woonplaats) van gebruikers aan te leveren aan de CIOT, het Centraal Informatiepunt Onderzoek Telecommunicatie. Elke 24 uur worden deze gegevens automatisch centraal opgeslagen. Via het CIOT worden de gegevens aan opsporingsdiensten ter beschikking gesteld. Daarnaast kunnen bij de telecomaanbieders verkeersgegevens opgevraagd worden. Ook kan de overheid gebruik maken van 'taps', het opnemen van telecommunicatie. Wetgeving ten aanzien van de taps wordt echter via andere wetgeving dan de Richtlijn Dataretentie geregeld.

Per 2006 zijn ook de internetproviders verplicht om naw-gegevens van gebruikers aan de CIOT aan te leveren. Voor internetproviders is nu ook, net als voor de telecomproviders, per 1 september 2009 het bewaren en leveren van verkeersgegevens verplicht geworden.

#### GEGEVENS EN BEWAARTERMIJN

Telecomaanbieders en internetproviders dienen gegevens te bewaren over de gebruiker, de bron, de bestemming, de datum, de locatie, het tijdstip, de duur van de communicatie en de (vermoedelijk) gebruikte apparatuur. De gegevens betreffen alle oproepen, de geslaagde en niet-geslaagde oproepen, de afgebroken oproepen, alle e-mails (inclusief spam), sms, mms, de internettoegang (xDSL, kabel en mobiel) en het gebruik van vaste, mobiele en IP-/VoIP-telefonie.

Vooralsnog moeten telecomgegevens en internetgegevens twaalf maanden bewaard worden. Een wetswijziging, waarbij de bewaartermijn van internetgegevens verkort wordt tot zes maanden, is in voorbereiding.

#### KOSTEN VAN SECURITY EN COMPLIANCY

Om de gevraagde gegevens te leveren moeten logfiles uit diverse applicaties, zoals CRM-applicaties, applicaties voor billing, switching, e-mail en VoIP, worden gehaald en vertaald naar een gewenst bruikbaar format. Het zal duidelijk zijn dat het extraheren van de gegevens uit de logfiles van de verschillende systemen in het algemeen een aanzienlijke inspanning zal vragen.

De overheid vergoedt alleen de administratieve kosten en uitvoeringskosten van het op verzoek aanleveren van gegevens. De aanbieders draaien zelf op voor de aanzienlijke infrastructurele kosten. Diverse aanpassingen in techniek, processen en organisatie zijn nodig. Vooral voor kleinere aanbieders kan de impact aanzienlijk zijn. Voor grote aanbieders, die de processen en organisatie al grotendeels naar security- en compliancemaatstaven hebben ingericht, zijn de gevolgen aanzienlijk minder ingrijpend.

## RICHTLIJNEN VOOR BEHEER

Als gevolg van de Wet bewaarplicht telecommunicatiegegevens dienen telecomaandieners en internetproviders dagelijks enkele gigabytes aan gegevens te verwerken en op te slaan. De bewaarde gegevens dienen van dezelfde kwaliteit te zijn als de gegevens in het netwerk. De aanbieders zijn zelf verantwoordelijk voor de opslag en de volledigheid van de gegevens. De gegevens zijn strikt vertrouwelijk. Er gelden dan ook strenge regels voor de beveiliging van de gegevens, voor de screening van het personeel dat toegang heeft tot de gegevens, voor het opstellen en uitvoeren van een beveiligingsplan en voor de vernietiging van de bewaarde gegevens.

## DE PRAKTIJK

Gebruikmaken van dataretentie is een belangrijke opsporingsmethode voor politie en justitie. Ingewikkelde datamining- of profilingtechnieken worden bij het gebruik van de gegevens niet toegepast. Het gebruik is eenvoudig en direct. Indien uit onderzoek naar voren komt dat een bepaald telefoonnummer, IP-nummer of bijvoorbeeld een e-mailadres als verdacht moet worden beschouwd, wordt in het bestand vervolgens gezocht naar bijvoorbeeld de corresponderende naw-gegevens en naar nummers waarmee het verdachte nummer contact heeft gehad op bepaalde dagen, tijdstippen etc.

## ELEKTRONISCHE MAZEN

In forensisch onderzoek worden digitale sporen in toenemende mate gebruikt, naast het traditionele sporenonderzoek. Digitaal onderzoek heeft bijvoorbeeld geleid tot de identificatie en arrestatie van de moordenaar van de Nijmeegse activist Louis Sévèke. De richtlijn kan echter op allerlei manieren nog worden ontweken. Zo bestaat er in niet-EU-landen veelal geen dataretentierichtlijn. Over het bellen via Skype kunnen slechts in beperkte mate relevante gegevens worden opgeslagen. Ook gaat de richtlijn niet in op nieuwe contactkanalen, zoals chat en sociale media. Deze elektronische 'mazen' hebben de aandacht van de EU en de diverse nationale overheden. Aanpassingen en verdere uitbreidingen van de richtlijn zijn dan ook te verwachten. **CCM**

De inhoud van dit artikel is onder andere gebaseerd op de whitepaper *Dataretentie: waarom, wie, wat en hoe?, Een Nederlandse situatieschets*, Novion Group, onderdeel van de Lawrence Wellingham Group, november 2009.

Dr. Frans Plat is oprichter van de kennisportal op het terrein van customer management vraagstukken, [www.klantinteractiekenniscentrum.nl](http://www.klantinteractiekenniscentrum.nl), en van de Customer Management Professionals Group op LinkedIn.com

## WAT TE DOEN TEGEN ONLINE FRAUDE?

Oplichters zijn voorafgaand aan de feestdagen massaal aanwezig op het web. Maar volgens de security experts van Unisys Corporation kunnen consumenten veel doen om zichzelf te beschermen tegen financiële fraude of identiteitsdiefstal. Hier volgen acht tips:

- 1. Online winkelen.** Winkel altijd op een website met een SSL-certificaat voor een veilige verbinding. Controleer het 'browser-slotje' en check regelmatig je rekeninggegevens op betalingen waar je niks van af weet.
- 2. Spyware.** Open nooit een e-mail van een onbekende verzender; het aantal 'kwaadaardige' digitale kerstkaarten neemt toe. Download geen .exe-bestanden, die bevatten vaak adware of spyware.
- 3. Social networking.** Kijk uit met het overbrengen van gelukswensen. Sociale netwerken als Facebook en Twitter zijn een goudmijn voor identiteitsdieven. Geef nooit persoonlijke informatie via het internet en zeg nooit wanneer je op vakantie bent.
- 4. Online betaalsites.** Fraudeurs zetten steeds vaker valse betaalwebsites op om geld af te troggelen. Controleer het 'slotje' (SSL-certificatie). Kijk of het adres begint met https://, waarbij de extra 's' staat voor secure. Een echte betaalservice vraagt geld over te maken via de bank, dus via een traceerbare overdracht. Weiger een andere methode.

## IDENTITY THEFT



**5. Goede doelen.** Wees voorzichtig met e-mails en tweets van goede doelen die vragen om donaties.

**6. Bescherm je nieuwe laptop.** Installeer direct antivirus software op je nieuwe pc of laptop en stel de firewall in voor je verbinding maakt met internet. De eerste 'ping'-aanval is binnen 9 seconden, een virus heeft minder dan één minuut nodig.

**7. Gratis WiFi en draadloze netwerken.**

Maak gebruik van een veilig draadloos netwerk. Het bereik van een WiFi-netwerk reikt verder, maar is zeer kwetsbaar. Wardrivers – mensen die voorbij rijden met een laptop op zoek naar een draadloos netwerk – hacken computers om zo persoonlijke informatie te stelen.

**8. Accountgegevens en phishing.** Wantrouw telefoontjes van zogenaamde vertegenwoordigers die accountgegevens willen controleren. Fraudeurs vergaren zo waardevolle informatie. Hetzelfde geldt voor een e-mail die mensen naar een valse website lokt om zogenaamd de inloggegevens te controleren (phishing).