OPERATORS MOETEN NAW-GEGEVENS OVERTREDERS VRIJGEVEN

Bestrijding cyberstalking gereguleerd in Telecomwet

Telefoonterreur is dichterbij dan veel mensen vermoeden. Wie denkt dat stalkers alleen bellen, heeft het mis. Veel overtreders maken gebruik van berichtendiensten zoals SMS, MMS en e-mail om mensen lastig te vallen. Aanpassingen in de Telecomwet maken de vervolging van telefoonterroristen eenvoudiger.

Door Ronald Eygendaal

Van de vrouwen ouder dan 15 jaar heeft één op de twaalf regelmatig last van hijgers, dreigers en zwijgers, zo blijkt uit onderzoek van het CBS. Eén op de achttien mannen krijgt te maken met vervelende telefoontjes terwijl in 1999 slechts één op de twintig ouderen een ongewenste beller aan de lijn had.

Bij de berichtendiensten zoals SMS en e-mail bestaat telefoonterreur vaak uit discriminerende, angstaanjagende of soms hatelijke berichtjes. MMS-terreur breidt dat scala uit met confronterende plaatjes. Cyberstalking is een verzamelnaam voor aanhoudende stromen van ongewenste telefoontjes of berichtjes waarvan de ontvanger niet weet van wie deze afkomstig zijn. De telefoontjes en berichtjes worden vaak op de meest onmenselijke tijden verstuurd en geven de ontvangers het gevoel dat ze in de gaten worden gehouden. Het grote aantal rechtbankzaken omtrent ongewenste SMS-jes illustreert de overlast van cyberterrorisme. Voor gedupeerden is het een uiterst bedreigende ervaring.

Ronald Eygendaal *is werkzaam als security consultant voor Protection Company, is voorzitter van de vakgroep ICT beveiliging van de Vereniging Beveiligingsmanagers Nederland en lid van het International Advisory Board van de International Foundation for Protection Officers. (ronaldeygendaal@protectioncompany.com)*

De daders worden vaak in de relationele sfeer gezocht. Ook per ongeluk tot stand gekomen telefoonverbindingen veroorzaken overlast. Denk maar aan verkeerd geprogrammeerde apparatuur of broekzakbellers.

Nieuw telefoonnummer

Veel oplossingen tegen cyberstalking worden met de huidige techniek en wetgeving nog niet geboden. Gedupeerden kunnen hooguit een nieuw telefoonnummer aanvragen. Dit kan enige tijd soelaas bieden, vooral wanneer slachtoffers een geheim nummer aanvragen. Wie zo'n nummer aanvraagt, kan kiezen voor het niet-vermelden van NAW-gegevens in de telefoongidsen en eventueel voor het niet-vermelden in het inlichtingenbestand. Omdat de dader echter vaak in de relationele sfeer moet worden gezocht zal een nieuw telefoonnummer het stalken vaak slechts tijdelijk onderbreken.

Het internet biedt de mogelijkheid om SMS-, MMS- en e-mailberichten volledig anoniem, van waar ook ter wereld te versturen. Vaak is hier niets tegen te doen. Soms helpt het om bij de netwerkaanbieder te klagen over de ongewenste berichtjes. Operators hebben vaak in hun algemene voorwaarden regels opgenomen over het misbruik van de diensten en kunnen bij overtreding hiervan nummers blokkeren. Ook dit zal leiden tot een slechts tijdelijke, soms zeer korte onderbreking van het stalken. Het enige wat de dader hoeft te doen is zijn activiteiten naar een andere netwerkaanbieder te verschuiven.

Bewijsmateriaal

Tegen iemand die anderen digitaal lastigvalt, is moeilijk op te treden. De politie grijpt niet in zolang er niets is gebeurd en er geen aangifte is gedaan. Het bewijzen van stalking is een lastige zaak. In het geval van telefoonterreur zal het slachtoffer zelf een lijst moeten bijhouden met tijden dat deze telefoontjes binnenkomen. De gedupeerde kan de telefoongesprekken opnemen en achtergelaten berichten bewaren op het antwoordapparaat. Maar zelfs al is cyberterreur bewezen, dan nog blijft het erg moeilijk om te bewijzen dat de persoon op wiens naam het telefoonnummer staat ook diegene is die heeft gebeld. Om een vervolging voor belaging volgens artikel 285B van het Wetboek van Strafrecht in te stellen moet de politie voldoende bewijzen hebben. Bij berichtendiensten zoals SMS, MMS is het bewijs gemakkelijker te verzamelen omdat de berichten in het geheugen van het toestel kunnen worden opgeslagen. Toch hoeft de abonnee of gebruiker van dit nummer nog niet per se de afzender van het bericht te zijn. Het toestel kan immers in een onbewaakt moment door een ander zijn gebruikt. Nu SMS- en MMS-berichten ook via het internet kunnen worden verstuurd kunnen cyberstalkers dit soort berichten volledig anoniem versturen. Wanneer er sprake is van strafbare feiten kan politie en justitie technieken gebruiken om de verzender achterhalen, dit is voor particulieren en bedrijven echter onmogelijk.

Bij telefoonterreur binnen bedrijven maken daders vaak gebruik van telefoontoestellen in algemene ruimtes zoals vergaderzalen, liften en kantines. De meeste PABX'en hebben een *malicious call trace*-functie waarmee gesprekken kunnen worden opgenomen en geregistreerd. Om dit te doen moet er tijdens een gesprek een code worden ingetoetst. Allereerst moet worden vastgesteld vanaf welk telefoontoestel de telefoonterreur plaatsvindt. De gedupeerde zal lijsten met data en tijden moeten bij-

houden met daarbij eventueel de resultaten van de malicious call trace. Zodra bekend is vanaf welke telefoontoestellen de dader opereert, zal hij via observatie moeten worden geïdentificeerd. Dit is dus werk voor een, door het ministerie van Justitie toegelaten, particulier recherchebureau.

Telecomwet

Door aanpassingen in de Telecomwet kan justitie optreden tegen telefoonterreur in openbare netwerken. Hierdoor voldoet de wet alsnog aan de Europese richtlijn nr. 97/66/EG (tweede kamer stuk 28962). In artikel 11.11 worden de procedures rond hinderlijke of kwaadwillige oproepen en de afhandeling daarvan geregeld. Artikel 11.11 behelst tevens de implementatie in de Telecomwet van artikel 10 van de Europese richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende privacy en elektronische communicatie. Met deze wijzigingen in de Telecomwet worden de mogelijkheden tegen telefoonterreur groter.

Bij de daadwerkelijke uitvoering en de effectiviteit van dit nieuwe artikel kunnen vraagtekens worden gezet omdat er niet wordt gesproken over berichtendiensten zoals e-mail. Het ziet ernaar uit dat er een verschuiving in de wijze van stalking zal plaatsvinden. Daarnaast zal de uitvoering van het artikel nog de nodige problemen geven. Vooral het eerste, tweede en vierde lid laten nog ruimte open voor misbruik.

Artikel 11.11

1. Een abonnee die last heeft van hinderlijke of kwaadwillige oproepen, waarbij de verstrekking van het nummer van het oproepende netwerkaansluitpunt is geblokkeerd, kan aan de aanbieder van een openbaar telecommunicatienetwerk of van een openbare telecommunicatiedienst verzoeken om het nummer van de oproepende abonnee en de daarop betrekking hebbende naam-, adres, postcode- en woonplaatsgegevens, te verstrekken.
2. Een verzoek als bedoeld in het eerste lid voldoet aan de volgende vereisten:
a. het verzoek is schriftelijk en bevat de naam-, adres-, postcode- en woonplaatsgegevens van de verzoeker alsmede het nummer waarop de oproepen betrekking hebben;
b. het verzoek behelst een omschrijving van de aard en ernst van de ondervonden last als gevolg van de oproepen waarop het verzoek betrekking heeft;
c. het verzoek bevat een indicatie van de data en tijdstippen waarop de desbetreffende oproepen hebben plaatsgevonden.
3. De verzoeker informeert de aanbieder onverwijld omtrent hinderlijke of kwaadwillige oproepen, die plaats hebben gevonden na indiening van het verzoek, bedoeld in het eerste lid.
4. De aanbieder stelt naar aanleiding van het verzoek een onderzoek in, teneinde vast te stellen of tot verstrekking van de gegevens, bedoeld in het eerste lid, dient te worden overgegaan.
5. Indien bij het onderzoek blijkt dat het oproepende nummer toebehoort aan een abonnee van een andere aanbieder, verleent de desbetreffende aanbieder op een daartoe strekkend verzoek van de met het onderzoek belaste aanbieder medewerking aan het onderzoek en verstrekt de op het oproepende nummer betrekking hebbende naam-, adres-, postcode- en woonplaatsgegevens aan de aanbieder die met het onderzoek is belast.
6. Van het feit van de gegevensverstrekking aan een verzoeker wordt door de aanbieder mededeling gedaan aan de abonnee, wiens gegevens het betreft.
7. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot:
a. het onderzoek, bedoeld in het vierde lid;
b. de gegevensverstrekking, bedoeld in het vierde lid;
c. de medewerkingsverplichting, bedoeld in het vijfde lid;
d. de kennisgeving van de verstrekking van de gegevens, bedoeld in het zesde lid.

Eerste lid

Het eerste lid van artikel 11.11 gaat over situaties waarbij hinderlijke of kwaadwillige oproepen plaatsvinden vanaf een telefoonaansluiting waarvan de nummerweergave is geblokkeerd. Door alsnog de gegevens van de oproepende abonnee te achterhalen via de telecomoperator kan de ontvanger van de gesprekken vervolgens civiel- of strafrechtelijke stappen ondernemen. Opvallend in dit artikel is dat de ontvanger geen NAW-gegevens kan achterhalen van een oproeper die zijn nummerweergave aan heeft staan en anoniem prepaid belt of gegevens niet heeft laten vermelden in een abonneelijst of nummerinformatiedienst. Dit geldt eveneens voor oproepen vanuit telefooncellen, openbare gelegenheden en bedrijven.

Tweede lid

Het tweede lid beschrijft de bewijsvoering. De gedupeerde zal een schriftelijke omschrijving moeten geven van de aard en ernst van de ondervonden last. In de memorie van toelichting staat dat er sprake moet zijn van een bepaald belpatroon dat in het maatschappelijk verkeer als hinderlijk wordt gekarakteriseerd. Hiermee is automatische een drempel vastgesteld. Daarnaast zal iemand die last heeft van stalking zelf moeten noteren op welke tijden de telefoontjes binnenkomen. Wanneer de stalker een boodschap op een antwoordapparaat heeft ingesproken, kan eventueel een stemvergelijking worden gemaakt. Zonder deze vormen van bewijs is het erg moeilijk om aan te tonen dat de persoon op wiens naam het telefoonnummer staat ook degene is die heeft gebeld.

Vierde lid

Om vast te stellen of er sprake is van hinderlijke of kwaadwillige oproepen zullen operators de verkeersgegevens moeten onderzoeken en analyseren. Operators kunnen echter slechts beoordelen of er sprake is van hinderlijke of kwaadwillige oproepen op basis van subjectieve informatie van de klager. Objectief kan er slechts worden vastgesteld dat en op welke momenten er communicatie tussen stalker en gedupeerde heeft plaatsgevonden. Het onderzoek kan niet bewijzen dat er sprake is van hinderlijke of kwaadwillige oproepen.

In Nederland vigeert 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, uniformering en legitimering. Tijdens het onderzoek zal er grove inbreuk worden gemaakt op de privacy van zowel de gedupeerde als van de dader. Het is wel vreemd dat wanneer het gaat om onderzoeken in het kader van Telecomwet artikel 11.11 de Wet particuliere beveiligingsorganisaties en recherchebureaus niet van toepassing is. Zeker in het contrast van inbreuk op privacy versus vergunninggebonden particulier recherchewerk. ■

Conclusies

De recente wijziging in de Telecomwet kan worden gezien als een verdere invulling van de wetgeving rond stalking. Als stalking bewezen is, kan de belaagde een klacht indienen zoals gesteld in artikel 285b van het Wetboek van Strafrecht. Het is jammer dat in de Europese richtlijn 2002/58/EG betreffende privacy en elektronische communicatie niet wordt gesproken over de berichtendiensten. Het verder reguleren van onderzoeken in het kader van artikel 11.11 van de Telecomwet is in een democratische samenleving noodzakelijk. Er moet echter wel worden voorkomen dat onderzoeken onevenredig en ongeoorloofd tegen mogelijke stalkers worden uitgevoerd. Een controlemechanisme zoals in de Wet particuliere beveiligingsorganisaties en recherchebureaus is daarom noodzakelijk.