Cyberstalking en bestrijding

Ronald Eygendaal CISMP CSS

Cyberstalking, ook wel telefoonterreur genoemd, komt veel voor. Wie denkt dat het uitsluitend om telefoontjes gaat heeft het mis, ook via berichtendiensten zoals SMS, MMS en e-mail worden mensen ongewenst lastiggevallen. Voornamelijk vrouwen zijn slachtoffer. Van de vrouwen ouder dan 15 jaar heeft één op de twaalf regelmatig te maken met 'hijgers, dreigers en zwijgers', zo blijkt uit onderzoek van het Centraal Bureau voor de Statistiek (CBS). Eén op de achttien mannen heeft last van vervelende telefoontjes. Oudere mensen worden het minst telefonisch lastiggevallen; slechts één op de twintig ouderen had in 1999 een ongewenste beller aan de lijn.

Zodra bekend is vanaf welke telefoontoestellen de dader opereert, zal met behulp van een statische observatie de dader moeten worden geïdentificeerd.

De stalking bestaat meestal uit het uiten van bedreigingen, het niets zeggen, vloeken, schelden, hijgen of ander ongewenste uitingen. Bij de berichten diensten zoals SMS en e-mail zijn het vaak discriminerende en angstaanjagende of soms hatelijke berichtjes.

Het zijn vaak aanhoudende stromen van ongewenste telefoontjes of berichtjes en veelal weet de ontvanger niet van wie deze afkomstig zijn. Het ontvangen van telefoontjes en berichtjes vindt vaak plaats op de meest onmenselijke tijden (niet iedereen kan of wil de telefoon gedurende de nacht uitzetten) en geeft het gevoel dat men 'in de gaten wordt gehouden'. Voor de gedupeerden is het een uiterst vervelende en bedreigende ervaring, vooral wanneer het 's avonds of 's nachts gebeurt.

De daders moeten vaak in de relationele sfeer, bijvoorbeeld een afgewezen ex-partner, worden gezocht. En vooral: ex-en die hun vroegere partners 'stalken' met hatelijke berichtjes. Wie rechtbankzaken bijhoudt, staat er van te kijken in hoeveel gevallen ongewenste sms-jes een rol spelen. Maar ook jongeren die hun pesterijen van het schoolplein verleggen naar het mobieltje. Soms moeten de daders worden gezocht in bepaalde groepen of organisaties.

Ook kan het gaan om telefoonverbindingen die per ongeluk tot stand komen, bijvoorbeeld door verkeerd geprogrammeerde apparatuur bij de beller. Mensen die een mobieltje in hun (broek)zak hebben, activeren soms per ongeluk het toestel. Dit zijn de zogenaamde broekzakbellers.

NIEUW TELEFOONNUMMER OF AFSLUITEN?

De gedupeerde kan hooguit een nieuw telefoonnummer aanvragen. Dit kan enige tijd soelaas bieden, vooral als men een geheim nummer aanvraagt. Bij het aanvragen van een geheim nummer kan men kiezen voor het niet-vermelden van naam, adres en nummer in de telefoongidsen, eventueel ook voor het niet-vermelden in het bestand Inlichtingen.

De gedupeerde zal zijn nieuwe telefoonnummer uitsluitend in een zeer kleine kring bekend kunnen maken. Omdat de dader vaak in de relationele sfeer moeten worden gezocht, zal een nieuw telefoonnummer vaak leiden tot een tijdelijke onderbreking van het stalken.

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 te klagen over de ongewenste berichtjes, bij de netwerkaanbieder. Vaak heeft deze in zijn algemene voorwaarden regels over het misbruik van de diensten opgenomen en zal afsluiting volgen. Ook dit zal leiden tot een tijdelijke, soms zeer korte, onderbreking van het stalken. De dader verschuift zijn activiteiten naar een andere netwerkaanbieder. En het verhaal begint weer van voren af aan.

BEWIJSMATERIAAL

Tegen iemand die anderen 'digitaal' lastigvalt is moeilijk op te treden. De politie grijpt niet in zolang er niets gebeurd is en er geen aangifte is gedaan. Als de mogelijkheid tot identificatie van de beller bestaat, is het belangrijk om aangifte bij de politie te doen. Van elk strafbaar feit (hoe gering ook) moet aangifte bij de politie worden gedaan!

Het bewijzen van stalking is een lastige zaak, bij telefonie zal het slachtoffer zelf een lijst moeten bijhouden op welke tijden deze telefoontjes binnenkomen. De gedupeerde kan bijvoorbeeld alle telefoongesprekken opnemen en de berichten bewaren op het antwoordapparaat. Ondanks dat blijft het erg moeilijk om te bewijzen dat de persoon op wiens naam het telefoonnummer staat, ook daadwerkelijk diegene is die heeft gebeld. De politie moet voldoende bewijzen hebben om een vervolging voor belaging (artikel 285B Wetboek van Strafrecht) in te stellen.

Bij berichtendiensten zoals SMS en MMS is het bewijs makkelijker te verzamelen. De berichten kunnen vaak in het geheugen van het toestel worden opgeslagen. De gedupeerde kan zelf, wanneer het berichtje via een mobieltje is verstuurd, het verzendende nummer zien. De abonnee of gebruiker van dit nummer hoeft nog niet per se de afzender van het bericht te zijn; het toestel kan in een onbewaakt moment door een ander zijn gebruikt.

Internet biedt de mogelijkheid om dit soort berichten volledig anoniem, van waar ook ter wereld, te versturen. Het is dan ook zo goed als onmogelijk om van SMS-berichtjes, verstuurd via internet, de verzender te achterhalen.

BEDRIJFSTELEFONIE

Bij telefoonterreur in bedrijven zien we vaak dat de daders gebruikmaken van telefoontoestellen in algemene ruimtes zoals vergaderzalen, liften en kantines. De meeste bedrijfstelefoniesystemen hebben een functie 'Malicious Call Trace'. Hiermee is het mogelijk om gesprekken op te nemen en te registreren. Om dit te doen moet er tijdens een gesprek een code worden ingetoetst. Zoals vermeld, maken de daders over het algemeen gebruik van telefoontoestellen in algemene ruimtes waardoor een onderzoek naar de eventuele daders op andere wijze uitgevoerd dient te worden. In dit kader moet allereerst worden vastgesteld vanaf welk telefoontoestel de telefoonterreur plaatsvindt. De gedupeerde zal lijsten met data en tijden moeten bijhouden, eventueel aangevuld met de resultaten van de 'Malicious Call Trace'. Zodra bekend is vanaf welke telefoontoestellen de dader opereert, zal met behulp van een statische observatie de dader moeten worden geïdentificeerd.

TELECOMMUNICATIEWET

Recentelijk is de Telecommunicatiewet aangepast en bestaat de mogelijkheid op te treden tegen telefoonterreur in openbare netwerken. In een nieuw artikel, 11.11, worden de procedures rond hinderlijke of kwaadwillige oproepen en de afhandeling daarvan geregeld. Artikel 11.11 TW behelst de implementatie in de Telecommunicatiewet van artikel 10 van richtlijn 2002/58/EG (betreffende privacy en elektronische communicatie) van het Europees Parlement en de Raad van 12 juli 2002. Met deze wijziging in de Telecommunicatiewet worden de mogelijkheden om tegen deze vorm van telefoonterreur op te treden, groter.

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, indien het onderzoek daartoe aanleiding geeft, de op het oproepende nummer betrekking hebbende naam-, adres-, postcode- en woonplaatsgegevens aan de aanbieder die met het onderzoek belast is.
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.

UITVOERING EN EFFECTIVITEIT

Bij de daadwerkelijke uitvoering en de effectiviteit van dit nieuwe artikel kunnen vraagtekens worden gezet. Immers, doordat dit artikel geheel in lijn is met de Europese richtlijn 2002/58/EG (betreffende privacy en elektronische communicatie) wordt niet gesproken over de berichtendiensten zoals e-mail.

Het bewijzen van stalking is een lastige zaak, bij telefonie zal het slachtoffer zelf een lijst moeten bijhouden op welke tijden deze telefoontjes binnenkomen.

In Nederland vigeert de 'Wet particuliere beveiligings-organisaties en recherchebureaus'.

Het ziet er naar uit dat er een verschuiving in de wijze van stalking zal gaan plaatsvinden. Daarnaast zal de uitvoering van het artikel nog de nodige problemen geven. Lidsgewijs zijn er de volgende punten van aandacht:

EERSTE LID; NUMMERWEERGAVE GEBLOKKEERD

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

TWEEDE LID; BEWIJS

De gedupeerde zal een schriftelijke omschrijving moeten geven van de aard en ernst van de ondervonden last. In de memorie van toelichting wordt gesproken van: "Er moet sprake zijn van een bepaald belpatroon dat in het maatschappelijk verkeer als hinderlijk moet worden gekarakteriseerd." Hiermee is automatisch een drempel vastgesteld. Daarnaast zal iemand die last heeft van stalking, zelf moeten noteren op welke tijden de telefoontjes binnenkomen. Ook wanneer de stalker bijvoorbeeld een boodschap op een antwoordapparaat heeft ingesproken, kan eventueel een stemvergelijking worden gemaakt. Zonder deze vormen van 'bewijs' is het erg moeilijk om te bewijzen dat de persoon op wiens naam het telefoonnummer staat, ook daadwerkelijk degene is die gebeld heeft.

VIERDE LID; ONDERZOEK

De telecomoperator zal voor het vaststellen of er sprake is van hinderlijke of kwaadwillige oproepen, een onderzoek en analyse van de verkeersgegevens moeten uitvoeren. Opgemerkt moet worden dat een operator slechts kan 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 en/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 (screening), uniformering en legitimering.

Tijdens het onderzoek, wat een telecomoperator moet doen, zal er grove inbreuk worden gemaakt op de privacy van zowel de gedupeerde als van de dader. Vreemd is dat, wanneer het gaat om onderzoeken in het kader van Telecommunicatiewet artikel 11.11, de 'Wet particuliere beveiligingsorganisaties en recherchebureaus' niet van toepassing is. En zeker als we dit in het contrast zetten van inbreuk op privacy versus vergunning gebonden particulier recherchewerk.

CONCLUSIE

De recente wijziging in de Telecommunicatiewet kan worden gezien als een verdere invulling van de bestrijding van de wetgeving rond het begrip 'stalking'.

Het positieve is dat, nadat de telecomoperator zijn onderzoek heeft voltooid, de belaagde een klacht kan 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 Telecommunicatiewet artikel 11.11, welke een onrechtmatige inbreuk vormt op het recht op eerbiediging van de persoonlijke levenssfeer is, in een democratische samenleving, noodzakelijk. Voorkomen moet worden dat onderzoeken onevenredig en ongeoorloofd tegen mogelijke stalkers worden uitgevoerd. Een controlemechanisme zoals onder andere aanwezig is binnen de 'Wet particuliere beveiligingsorganisaties en recherchebureaus', is geen overbodige luxe.