R. Eygendaal 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 lastig gevallen. Voornamelijk vrouwen zijn het slachtoffer. Van de vrouwen ouder dan vijftien jaar heeft één op de twaalf regelmatig te maken met 'hijgers, dreigers en zwijgers', zo blijkt uit onderzoek van het CBS.

Cyberstalking en bestrijding

Stalking bestaat meestal uit het uiten van bedreigingen, niets zeggen, vloeken, schelden, hijgen of andere ongewenste uitingen. Bij de berichtendiensten zoals SMS en e-mail zijn het vaak discriminerende en angstaanjagende of soms hatelijke berichtjes. Vaak zijn het aanhoudende stromen van ongewenste telefoontjes en weet de ontvanger niet van wie deze afkomstig zijn. Voor de gedupeerden is het een vervelende en bedreigende ervaring en geeft het een gevoel 'in de gaten te worden gehouden'.

De daders moeten vaak in de relationele sfeer worden gezocht, bijvoorbeeld een afgewezen partner. Wie rechtbankzaken bijhoudt, staat er van te kijken in hoeveel gevallen ongewenste SMS-jes een rol spelen. Soms moeten de daders worden gezocht in bepaalde groepen of organisaties.

Management-summary

Stalking komt steeds meer voor via internet en berichtendiensten zoals SMS. Het is vaak moeilijk om te bewijzen wie de stalker is. Wat kan iemand doen wanneer hij of zij lastig wordt gevallen door een digitale stalker? In dit artikel worden tips gegeven. Ook wordt het nieuwe artikel in de Telecommunicatiewet uitgelegd, waarin de mogelijkheid is opgenomen om op te treden tegen telefoonterreur in openbare netwerken.

Nieuw nummer

De gedupeerde kan hooguit een nieuw telefoonnummer aanvragen. Dit kan enige tijd soulaas bieden, vooral als men een geheim nummer aanvraagt. De gedupeerde zal zijn nieuwe telefoonnummer uitsluitend in een zeer kleine kring bekend kunnen maken. Omdat de dader vaak in de relationele sfeer moet worden gezocht zal een nieuw telefoonnummer slechts 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 bij de netwerkaanbieder te klagen over de ongewenste berichten. Vaak heeft deze in de algemene voorwaarden regels opgenomen

* is werkzaam als senior Security consultant voor Protection Company

over misbruik van de diensten 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

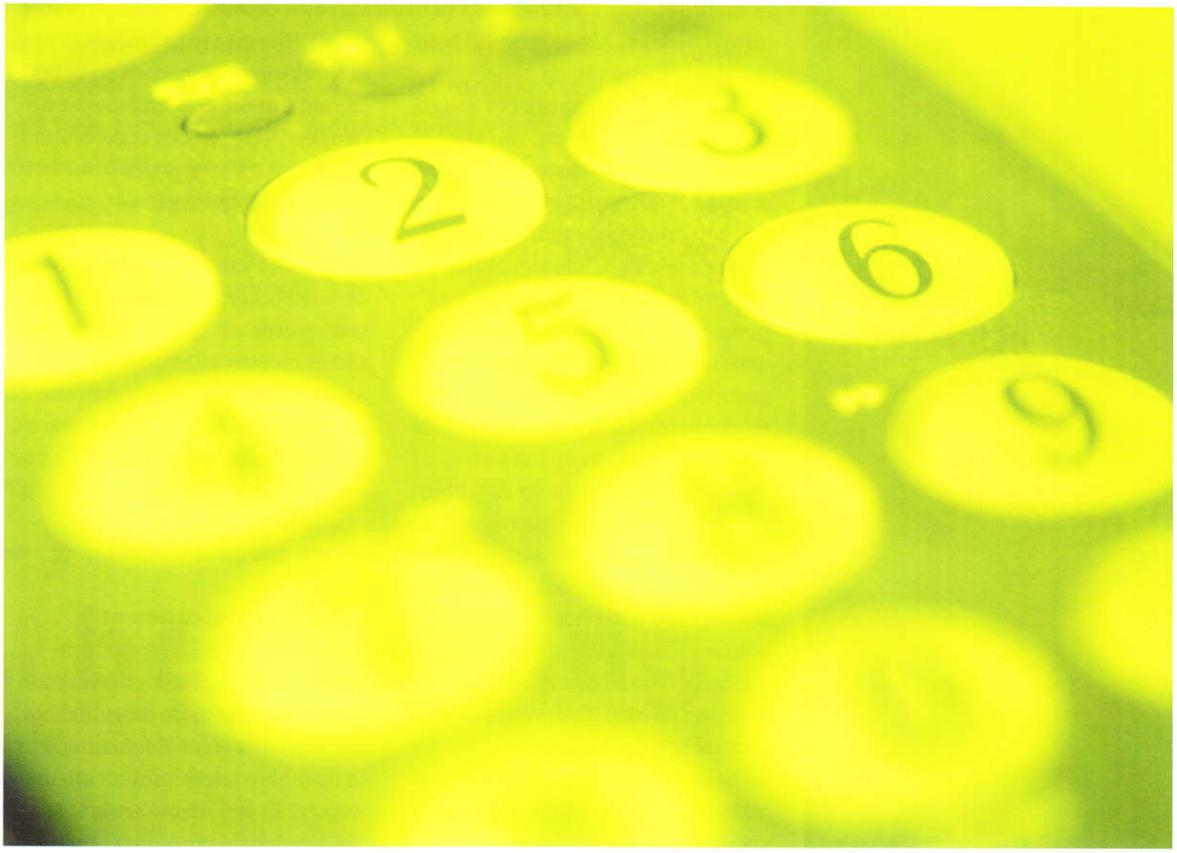
Tegen iemand die anderen 'digitaal'lastigvalt is moeilijk op te treden. De politie grijpt niet in zolang er niets gebeurd is en er geen aangifte is gedaan. Als de mogelijkheid tot identificatie van de beller bestaat, is het belangrijk om aangifte bij de politie te doen. Van elk strafbaar feit (hoe gering ook) moet aangifte worden gedaan!
Het bewijzen van stalking is een lastige zaak. Bij telefonie zal het slachtoffer zelf een lijst moeten bijhouden van de tijdstippen waarop 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 nummer van het toestel zien waarmee het bericht verstuurd is. De abonnee of gebruiker van dit nummer hoeft echter niet de verzender 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-berichten die via internet zijn verstuurd 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 beschikken over de functie 'malicious call trace'. Hiermee is het mogelijk om gesprekken op te nemen en te registeren. Om dit te doen moet er tijdens een gesprek een code worden ingetoetst.
Bij een telefoontje van een algemeen toestel moet eerst worden vastgesteld van welk telefoontoestel de telefoonterreur plaatsheeft. 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 hij met behulp van een statische observatie moeten worden geïdentificeerd.

Telecommunicatiewet

Recentelijk is de Telecommunicatiewet aangepast (kamerstuk 28 962) en bestaat er de mogelijkheid om te treden tegen telefoonterreur in openbare telecommunicatie netwerken. In een nieuw artikel, 11.11 TW 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.
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 wordt niet gesproken over berichtendiensten zoals e-mail. Daarnaast zal de uitvoering van het artikel nog de nodige problemen geven.
Lidsgewijs zijn er de volgende punten van aandacht in de Telecommunicatiewet. Eerste lid: nummer-



weergave geblokkeerd. Dit gaat over situaties waarbij hinderlijke of kwaadwillige oproepen plaatshebben vanaf een telefoonaansluiting waarvan de nummerweergave geblokkeerd is. Door alsnog de gegevens van de oproepende abonnee te achterhalen (via de aanbieders van telecommunicatiediensten), kan de ontvanger van de gesprekken civiele- of strafrechtelijke stappen ondernemen. Echter, zodra er sprake is van oproepen vanaf anonieme prepaid mobieltjes, oproepen vanuit telefooncellen, openbare gelegenheden, bedrijven en het buitenland komen we, met 11.11 TW in de problemen.

Schriftelijk

In deze situatie is de daadwerkelijke fysieke beller niet gemakkelijk te achterhalen. Helaas is men in deze situatie aangewezen op hulp van derden (bijvoorbeeld het bedrijf waar de hinderlijke of kwaadwillige oproepen vandaan komen). Vaak zal men aangewezen zijn op een, door het ministerie van Justitie erkend, particulier rechercheburo welke door middel van een statische observatie de dader kan achterhalen. Hoewel de algemene voorwaarden van de aanbieders van telecommunicatiediensten mogelijkheden bieden om klanten af te sluiten bij dit soort wangedrag is het maar de vraag of de belangen van gedupeerden voldoende gewaarborgd zijn. De kans bestaat dat aanbieders van telecommunicatiediensten hun commerciële belangen prefereren boven de belangen van gedupeerden, helaas regelt 11.11 TW hier niets over.
Volgens het tweede lid van artikel 11.11 TW heeft de gedupeerde een aantal verplichtingen. Zo zal de gedupeerde 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 maatschappelijke 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. 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 te bewijzen dat de persoon op wiens naam het telefoonnummer staat, ook daadwerkelijk degene is die heeft gebeld.
Uiteindelijk zal de aanbieder van de telecommunicatiediensten moeten vaststellen of er sprake is van hinderlijke of kwaadwillige oproepen. Om dit te doen zal de aanbieder van de telecommunicatiedien-

sten een onderzoek en analyse van de verkeersgegevens moeten uitvoeren. Opgemerkt moet worden dat een aanbieder van de telecommunicatiediensten slechts kan beoordelen of er sprake is van hinderlijke of kwaadwillige oproepen op basis van subjectieve informatie van de gedupeerde (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 wettelijke eisen ten aanzien van opleiding, betrouwbaarheid personeel (screening), uniformering en legitimering.

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

Bestrijding

De recente wijziging in de Telecommunicatiewet kan worden gezien als een verdere invulling van de wetgeving rond het begrip stalking. Het positieve is dat, nadat de aanbieders van telecommunicatiediensten hun onderzoek hebben voltooid, de belaagde een klacht kan indienen zoals gesteld in artikel 285b van het Wetboek van Strafrecht. Het is alleen jammer dat in de Europese richtlijn 2002/58/EG (betreffende privacy en elektronische communicatie) niet wordt gesproken over berichtendiensten. Het is noodzakelijk om onderzoeken die een onrechtmatige inbreuk vormen op het recht op eerbiediging van de persoonlijke levenssfeer verder te reguleren. Voorkomen moet worden dat onderzoeken onevenredig en ongeoorloofd tegen mogelijke stalkers worden uitgevoerd. Een controlemechanisme zoals onder andere aanwezig in de Wet particuliere beveiligingsorganisaties en recherchebureaus is geen overbodige luxe.

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 hebben plaatsgevonden 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.