Overwerk bij abuse-teams

De meeste beveiligingsafdelingen van ISP's hebben een abuse-team dat er op toeziet dat klanten zich aan de aansluitvoorwaarden houden. Nu spam ook aan banden is gelegd, draaien de teams op volle toeren.

Door Ronald Eygendaal

Internetmisbruik, ook wel *abuse* genoemd, is het uitvoeren van oneigenlijke of ongewenste acties op het internet zoals het versturen van spam en virussen maar ook hacken, het publiceren van illegale content en de verspreiding van kinderporno. Abuse-teams houden toezicht op naleving van de contractuele voorwaarden maar maken klanten er tevens van bewust hoe ze misbruik kunnen voorkomen en hoe ze de overlast van misbruikers kunnen beperken.

Net als in de gewone wereld zijn er binnen de internetwereld normen en waarden. Deze netiquette staat beschreven in internetvoorschriften, ook wel *Requests for Comments* (RFC's) genoemd. Internetvoorschrift RFC3013 gaat over de netiquette. De branchevereniging voor de *Nederlandse Internet Providers* (NLIP) heeft daarbij aanvullende netiquette en beveiligingsvoorschriften voorgeschreven aan zijn leden. In de internetvoorschriften (RFC2142) is opgenomen dat ISP's de e-mail adressen abuse@ , security@ en noc@ in hun systemen moeten implementeren. De branchevereniging van Nederlandse Internet Providers (NLIP) geeft in aanvulling op RFC2142 haar leden het advies om ook het e-mailadres misbruik@ beschikbaar te maken voor de misbruikmeldingen op het internet.

Abuse-teams kunnen worden gezien als stadswachten van het internet.

Recent heeft het NLIP nog een van zijn leden publiekelijk gewaarschuwd en vervolgens geschorst om hij in strijd handelde met de aanvullende netiquette en beveiligingsvoorschriften. Ook worden overtreders van de netiquette vaak door mede internetgebruikers afgestraft. Abuse-teams kunnen dan ook worden gezien als de stadswachten van het internet.

Spam-bestrijding

Het versturen van grote aantallen ongevraagde en ongewenste berichten, vaak van commerciële aard wordt gedefinieerd als spam of bulk e-mail. Spam veroorzaakt meer ergernis dan elke andere vorm van reclame dan ook. Onderzoeksbureau Blauw Research deed in opdracht van internetprovider XS4ALL onderzoek naar spam en concludeerde onder andere dat 88 procent van de ondernemers en 85 procent van de consumenten voor een harde aanpak van spammers is.

Spam is maar zelden afkomstig van een fatsoenlijke en eerlijke adverteerder. De meeste berichten behoren tot een van de volgende categorieën:

- Advertenties voor pornografische sites.
- *Get rich quick* of *make money fast*-projecten.
- Aanbiedingen voor software om e-mailadressen te verzamelen en zelf spam te versturen.
- Aanbiedingen voor aandelen van onbekende startende ondernemingen.
- Dubieuze geneesmiddelen.
- Pyramidespelen.
- Kettingbrieven.
- Illegale software.

Klanten kunnen bij het abuse-team van hun ISP klagen over spam. Indien de veroorzaker traceerbaar is, zal deze via zijn ISP tot de orde worden geroepen en indien nodig van het internet worden afgesloten. Om hun werk goed te kunnen doen, moeten abuse-teams wereldwijd samenwerken. De veroorzakers van spam kunnen zich namelijk overal ter wereld bevinden.

Vaak wordt vergeten dat spam niet alleen irritatie oplevert, maar dat de ontvangers ervan ook financieel worden gedupeerd. Het binnenhalen en verwijderen van spam kost immers tijd en dus geld. Vooral met mobiel internet kan spam veel geld kosten omdat GPRS-gebruikers *airtime* betalen en daar niets voor terugkrijgen.

Malicious code

Virussen, trojans en worms zijn allemaal voorbeelden van malicious code ofwel kwaadaardige software. Malicious code is vaak geschreven om de veiligheid van systemen in gevaar te brengen. Een computervirus is een klein computerprogramma met een saboterende werking. Een groot aantal virussen verbergt zichzelf in andere programma's om vanuit daar ongezien de juiste werking van de software en het computersysteem te saboteren. Daarbij proberen de virussen zichzelf te vermenigvuldigen. Ander computerongedierte is de zogenaamde worm die zich op dezelfde manier als een virus verspreidt en vermenigvul-

Ronald Eygendaal *is werkzaam als Senior Security Consultant voor Protection Company, heeft meer dan 10 jaar ervaring in beveiliging en informatiebeveiliging, is voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland en lid van het International Advisory Board van de International Foundation for Protection Officers. (ronaldeygendaal@protectioncompany.com)*

digt. Het verschil tussen worms en virussen is dat worms zich van computer naar computer verspreiden totdat ze het volledige systeem besmetten in plaats van zich van bestand naar bestand te verspreiden. Worms kopiëren zichzelf van de ene naar de andere computer via e-mail, ICQ of GPRS. Omdat wormen geen menselijke tussenkomst nodig hebben om zich te vermenigvuldigen, kunnen ze zich veel sneller verspreiden dan computervirussen.

Veel malicious code verspreidt zich via het internet en besmet op deze wijze andere op het internet aangesloten computers. Sommige programma's, trojans genoemd, doen alsof ze een bepaalde nuttige en door de gebruiker gewenste taak verrichten, maar saboteren vervolgens de computer. Een goed voorbeeld van trojans is spyware. Sommige ISP's hebben een virusscan-functionaliteit in hun dienstverlening en sturen waarschuwingen naar onbewuste en bewuste verspreiders van virussen. Tevens sturen deze systemen een kopie naar het abuse mailadres van de verzendende ISP. Zo gauw het abuse-team deze melding ontvangt, informeert het team de verspreider. Vervolgens kan deze actie ondernemen om het virus op zijn computer te verwijderen.

Ook virusscanners in de bedrijfsnetwerken kunnen besmette of verdachte e-mail weigeren, opschonen en soms zelfs daarna accepteren. Vaak sturen dit soort systemen ook waarschuwingen naar verzenders van besmette of verdachte e-mail en soms ook naar het abuse-adres van de versturende ISP. Het abuse-team van de versturende ISP kan dan actie ondernemen. Er zijn zelfs ISP's die *spyware scanning* als dienst aanbieden.

Hacking en poortscanning

Hacking is het op een wederrechtelijke manier binnendringen in een computersysteem of netwerk. Hackers trachten vaak gegevens te kopiëren, te wijzigen of te vernietigen. Ook proberen hackers zich ongeoorloofd toegang te verschaffen tot besloten systemen om websites opzettelijk te beschadigen of om zonder betaling toegang te krijgen tot abonneediensten. Computerhuisvredebreuk, zoals hacking ook wel wordt genoemd, is een strafbaar delict.

Spam kan al gauw oplopen tot honderden bulk-e-mailtjes per dag.

Als het abuse-team een melding van hacking binnenkrijgt dan zal het passende maatregelen nemen. Vaak worden in afwachting van een officieel verzoek alvast forensische sporen zeker gesteld. Poortscanning is een methodiek om te ontdekken welke poort op een computersysteem openstaat zodat deze open poort kan worden gebruikt om binnen te dringen.

De ontvangers van mobiele spam worden financieel gedupeerd omdat ze airtime betalen en daar niets voor terugkrijgen.

Bij het gebruik van een firewall, mits goed geconfigureerd, zal een dergelijke poging tot inbraak op niets uitlopen. Poortscanning is een minder belangrijke vorm van hacking en vormt slechts zelden een gevaar. Overigens wordt dit soort aanvallen wel gedetecteerd door een firewall. Vaak is in de logfile van de firewall het scannende IP-adres terug te vinden. Poortscanning als zodanig is niet strafbaar, maar in de meeste aansluitvoorwaarden van ISP's zijn wel regels over poortscanning opgenomen. Op basis van deze regels kunnen abuse-teams tot actie overgaan en hardnekkige poortscanners uit het ISP-netwerk weren. De meeste hacking-risico's lopen de gebruikers van ADSL en kabelinternet. GPRS-netwerken werken met het *allways online*-principe en zijn daardoor net zo kwetsbaar voor hacking als een ADSL- of kabelinternet-aansluiting. Een firewall is dan ook een must bij het gebruik van dit soort netwerkverbindingen.

Kinderporno

De hoeveelheid meldingen over kinderporno is het afgelopen jaar ongeveer met 30 tot 35 procent gestegen. Kinderporno is strafbaar gesteld in artikel 240b van het Wetboek van strafrecht. Volgens artikel 240b eerste lid wordt degene bestraft die een afbeelding of een gegevensdrager met een afbeelding van een seksuele gedraging verspreidt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert of in voorraad heeft waarbij iemand is betrokken die de leeftijd van zestien jaar nog niet heeft bereikt.

Nederland kent net zoals de meeste beschaafde landen een meldpunt kinderporno. Abuse-teams van de ISP's ontvangen regelmatig vanuit al dan niet anonieme bronnen informatie over klanten met een dubieus gedrag. In de meeste gevallen wordt de verspreider van dit materiaal direct afgesloten nadat belastend materiaal is aangetroffen. In een aantal gevallen worden, veelal op verzoek van justitie, forensische sporen veiliggesteld. Een zorgelijke ontwikkeling is de stijgende hoeveelheid meldingen van kinderporno en het feit dat de plegers van dit soort delicten inventiever worden en daardoor vaak niet kunnen worden gestraft.

Illegale content

Het is in Nederland verboden om bepaalde content digitaal te publiceren. Hierbij moet worden gedacht aan schending van auteursrechten, merkenrecht en portretrecht, maar ook aan uitings- en verspreidingsdelicten. Een ISP die op zijn site een selectie geeft van illegale content van klanten, toont zo betrokkenheid bij de content en is daardoor medeverantwoordelijk en dus strafbaar.

Dit is het zogenaamde *mère conduit*. Ook civielrechtelijk is een ISP aanspreekbaar voor illegale content.
Het spreekt voor zich dat het downloaden van illegaal materiaal zoals software, muziek en films in Nederland verboden is. Auteursrechtenorganisaties zoals Stichting Brein trachten downloaders te traceren en civielrechtelijk aan te pakken en de misgelopen inkomsten te verhalen. In het kader van de aansprakelijkheidketen is het voor ISP's van belang dat abuse-teams snel optreden tegen vermeende downloaders van illegaal materiaal.
Ook de snelle opkomst van ringtones en plaatjes voor de mobiele telefoons die van het internet kunnen worden gedownload, hebben gezorgd voor meer meldingen van illegale content bij de ISP's. De abuse-teams hebben hun handen vol aan de homepages van klanten. Blijkbaar geldt nog steeds het credo *beter goed gejat dan slecht gemaakt.* Wanneer een abuse-team illegale content aantreft, zal het gelijk tot afsluiting moeten overgaan. Bij nalatigheid is de ISP immers strafbaar.

Chat en IRC

De meeste Chat en *Internet Relay Chat* (IRC)-kanalen hebben een abuse operator die erop toeziet dat chatters verschoont blijven van scheldkanonnades en uitspraken die niet conform de normen en waarden of zelfs discriminerend zijn. Soms is een simpele waarschuwing van de operator of het abuse-team voldoende, soms is aansluitend een *timekickban* nodig van 5 minuten om de gemoederen te laten afkoelen.
Een van de problemen met chat en IRC is dat niemand te vertrouwen is, omdat een chatter nooit weet of de persoon aan de andere kant de waarheid spreekt. Gebruikers van chat en IRC wordt dan ook geadviseerd nooit zomaar een telefoonnummer of een huisadres af te geven. De operators zien er op toe dat gebruikers onenigheden niet in een chat- of IRC-kanaal uitvechten, maar privé een en ander uitpraten. ■

Abuse-teams van de ISP's ontvangen regelmatig informatie over klanten met een dubieus gedrag.