Overwerk bij abuse teams

Ronald Eygendaal

De meeste security afdelingen bij de Internet Service Providers (ISP)'s hebben een abuse team. Deze abuse teams zien er op toe dat klanten zich aan de algemene voorwaarden van de Internet Service Provider houden en dus geen 'abuse' plegen. Met 'abuse' wordt bedoeld het uitvoeren van oneigenlijke en/of ongewenste acties op internet. Het gaat hierbij bijvoorbeeld om SPAM, virussen, hacken of mogelijke pogingen daartoe, illegale content, verspreiding van kinderporno, etc.

De abuse teams hebben, onder andere de verantwoordelijkheid om klanten bewust te maken hoe ze kunnen voorkomen dat ze zelf abuse plegen en hoe ze de overlast van anderen die dit doen kunnen beperken. Net als in de gewone wereld zijn er binnen de internetwereld normen en waarden, dit zijn de zogenaamde netiquette. Deze netiquette staan beschreven in internetvoorschriften, ook wel RFC's genoemd. Internet voorschrift RCF3013 gaat over de 'netiquette'. Overtreding van deze netiquette wordt vaak door medegebruikers afgestraft. Het overbrengen van deze netiquette wordt ook vaak gezien als een van de taken van een abuse team.

SPAM BESTRIJDING

Het woord SPAM komt van: Sending People A lot of Mail. SPAM, ook wel bulk e-mail genoemd, is het versturen van grote aantallen ongevraagde/ongewenste berichten (vaak van commerciële aard). De ontvangers van deze SPAM berichten zijn meestal personen die er waarschijnlijk anders niet voor zouden kiezen om dergelijke berichten te ontvangen. SPAM is maar zelden afkomstig van een fatsoenlijke en eerlijke adverteerder, integendeel 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-mail adressen te verzamelen en zelf SPAM te versturen.
- Aanbiedingen voor aandelen van onbekende startende ondernemingen.
- Dubieuze geneesmiddelen.
- Pyramidespelen.
- Kettingbrieven.
- Illegale software.

In de nieuwsgroepen worden regelmatig postings in veel groepen tegelijk gedaan, ook dit valt onder het begrip SPAM.

Een abuse team neemt maatregelen tegen klanten van desbetreffende ISP als die zich schuldig maken aan versturen van SPAM. Gedupeerde klanten kunnen bij het abuse team melden dat men SPAM heeft ontvangen. Indien de veroorzaker traceerbaar is, dan zal deze via zijn ISP tot de orde worden geroepen, en indien nodig, worden afgesloten van het internet. Eenheid en samenwerking tussen de abuse teams van verschillende ISP's is hiervoor noodzakelijk.

Vooral met mobiel internet kan het ontvangen van SPAM een hoop geld kosten, immers men betaald 'airtime' en krijgt er niets voor terug.

VIRUSSEN

Virussen kunnen veel schade aan een computer aanrichten. Een computervirus is een klein computerprogramma dat meestal een saboterende werking heeft. 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. Ook probeert het virus zichzelf te vermenigvuldigen. Veel virussen verspreiden zich via internet en besmetten op deze wijze andere op het internet aangesloten computers. Een aantal automatische virusscanners op internet sturen waarschuwingen naar onbewuste dan wel bewuste verspreiders van virussen. Tevens sturen deze systemen een kopie naar het abuse mail adres van de verzendende ISP.

Via het mailadres abuse@ komen de virusmeldingen dan binnen bij de abuse teams. 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.

Veel virussen verspreiden zich via internet en besmetten op deze wijze andere op het internet aangesloten computers.

Ook aan homepages van klanten hebben de abuse teams hun handen vol

HACKING

De definitie van Hacking is: het op een of andere wijze ongeoorloofd binnendringen in een computersysteem en/of netwerk. Het gaat dus om gevallen waarin iemand zich opzettelijk met een netwerk, een server of een bestand in verbinding stelt, als hij daarvoor geen toestemming heeft, of dat hij onopzettelijk de verbinding tot stand brengt, maar deze vrijwillig besluit te handhaven. Computerhuisvredebreuk, een mooi woord voor hacking, is een strafbaar delict. Als het abuse team een melding van hacking binnen krijgt dan zal men, indien nodig, passende maatregelen nemen. Vaak worden, in afwachting van een officieel verzoek, alvast forensische sporen zeker gesteld.

De meeste hacking risico's lopen de gebruikers van ADSL en kabel internet. GPRS netwerken werken met het 'allways online' principe en zijn daardoor net zo kwetsbaar voor hacking als een ADSL c.q. kabel internet aansluiting.

KINDERPORNO

De hoeveelheid meldingen over kinderporno is afgelopen jaar ongeveer met 30 tot 35 procent gestegen. Kinderpornografie is strafbaar gesteld in artikel 240b Wetboek van Strafrecht

In artikel 240b 1ste lid staat beschreven dat degene wordt bestraft die een afbeelding – of een gegevensdrager, bevattende een afbeelding – van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van zestien jaar nog niet heeft bereikt, is betrokken, verspreidt of openlijk tentoonstelt, vervaardigt, invoert, doorvoert of in voorraad heeft (lid 1).

De abuse teams van de Internet Service Providers ontvangen vanuit verschillende bronnen informatie over klanten met een dubieus gedrag. In de meeste gevallen wordt direct na de melding, de klant afgesloten. In een aantal gevallen worden, op verzoek van justitie, forensische sporen veilig gesteld.

Zorgelijk is de stijgende hoeveelheid meldingen en het feit dat de plegers van dit soort delicten inventiever worden en daardoor vaak niet strafbaar.

ILLEGALE CONTENT (INFORMATIE)

Hierbij moet worden gedacht aan schending van auteursrechten, merkenrecht, portretrecht, maar ook uitings- en verspreidingsdelicten. Een ISP die op zijn site een selectie geeft van content (informatie) van bepaalde klanten, toont zo betrokkenheid en is daardoor medeverantwoordelijk en dus strafbaar. Ook civiel rechtelijke is een ISP aanspreekbaar voor illegale content.

De snelle opkomst van ringtones en plaatjes voor de mobiele telefoons, welke gedownload kunnen worden van internet, hebben gezorgd voor meer meldingen van illegale content bij de Internet Service Providers. Ook aan homepages van klanten hebben de abuse teams hun handen vol, schijnbaar geldt nog steeds 'beter goed gejat dan slecht gemaakt'. In geval van het aantreffen van illegale content zal een abuse team gelijk tot afsluiting moeten overgaan, immers als de ISP dit niet doet, is hij strafbaar.

Een belangrijke taak van een abuse team is het verwijderen van illegale content op het 'stukje' internet waarvoor de ISP verantwoordelijk is.

BEREIKBAARHEID ABUSE TEAMS

In de internetvoorschriften, ook wel RFC's genoemd, zijn verplichtingen opgenomen dat Internet Service Providers de e-mail adressen abuse@, security@ en noc@ moeten implementeren in hun systemen. (RFC 2142). De branchevereniging van Nederlandse Internet Providers, het NLIP, geeft in aanvulling op RFC2142 haar leden het advies om ook het e-mail adres misbruik@ beschikbaar te maken voor de meldingen betreffende misbuik op internet.

BRONNEN

http://www.meldpunt.nl
http://spamcop.net/
http://www.nlip.nl
RFC 2142
RFC 3013
Netiquette Richtlijnen NLIP