Nieuwsbrief 2-2012

W.Bosgra ***Taakaccenthouder digitale criminaliteit***

Digitale nieuwsbrief verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer en kennis opdoen voor de opsporing van strafbare feiten gepleegd middels de computer. U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Deze nieuwsbrief zal met enige regelmaat in uw mailbox verschijnen.

Middels deze nieuwsbrief houden wij u op de hoogte van:

- onderwerpen die betrekking hebben op het veilig gebruik van de computer en het internet
- nieuws uit de media
- juridische vragen
- nieuwe technieken
- vele andere wetenswaardigheden

Computeralfabet:

http://www.joostvrinds.moerstaal.nl/alfabet/pagina6.html

Kwaadaardige software

Wormen

Een worm is een programma dat zichzelf verspreidt, bijvoorbeeld door een kopie van zichzelf op elke gedeelde harde schijf op hetzelfde netwerk te installeren. Een worm is daarnaast geprogrammeerd om een bepaalde actie uit te voeren, zoals het installeren van een achterdeur op geïnfecteerde systemen zodat die door de verspreider van de worm kunnen worden gecontroleerd.

Tegenwoordig verspreiden de meeste wormen zich door zichzelf als bijlage aan e-mail toe te voegen (die ze dan meestal zelf ook nog automatisch versturen). De ontvanger denkt dan een legitieme e-mail te krijgen, want de afzender van de mail is de eigenaar van de besmette computer. Hij zal dan snel geneigd zijn de bijlage te openen, waarna zijn PC ook geïnfecteerd raakt.

Het belangrijkste verschil tussen een virus en een worm is dat een worm zich zelfstandig verspreidt en een virus niet. Een virus verspreidt zich alleen wanneer de gebruiker een geïnfecteerd bestand of programma opent. Een worm kan zich al verspreiden als de computer alleen maar aan staat.

Als de actie van een worm schade oplevert, is de maker of verspreider strafbaar onder art. 350a lid 3. Een worm die alleen een achterdeur openzet, richt nog geen schade aan. Zo'n worm kan wel worden gezien als een hulpmiddel voor computervredebreuk (strafbaar volgens art. 139d lid 2 onder a).]

Virussen

Vaak worden de termen 'virus' en 'worm' door elkaar gebruikt. Een virus lijkt qua functionaliteit op een worm, maar verspreidt zichzelf niet autonoom. Een virus hecht zich aan een bestaand programma (of document) en kopieert zichzelf pas wanneer dat programma wordt uitgevoerd. Een virus kan zich ook hechten aan het besturingssysteem ("boot sector virus"), en wordt dan automatisch actief zodra de computer opstart.

Het maken en verspreiden van virussen is net als bij wormen strafbaar onder art. 350a lid 3.

Trojaanse paarden

en Trojaans paard is een programma met kwade bedoelingen dat zich voordoet als legitieme software. Een screensaver die stiekem alle bestanden uit de map "Mijn documenten" verstuurt naar een server, is een Trojaans Paard. Een ander voorbeeld is een programma dat wordt geadverteerd als een verbetering van Internet Explorer, maar tevens een stuk software installeert waarmee de computer op afstand te besturen is.

In tegenstelling tot virussen en wormen verspreidt Trojaanse paard-software zichzelf niet. Deze software wordt door gebruikers doorgegeven die niet doorhebben dat de software niet legitiem is.

Trojaans paard-software richt meestal hooguit indirect schade aan, bijvoorbeeld door andere software te installeren. Meestal zal dit hooguit kunnen worden gezien als een hulpmiddel voor computervredebreuk (art. 139d lid 2 onder a).

Rootkit

Een rootkit draait ongemerkt op de computer van het slachtoffer en verbergt bepaalde activiteiten die daarop plaatsvinden. Zo kan een rootkit bijvoorbeeld de aanwezigheid van een virus verhullen, door besmette bestanden te laten zien alsof ze dat niet zijn.

Een rootkit kan ook een achterdeur verborgen houden, waarmee een inbreker later gemakkelijk de computer binnen kan dringen of op afstand besturen.

Vaak worden rootkits als onderdeel van andere malware geïnstalleerd. Zo kan een Trojaans paard of een worm bijvoorbeeld een rootkit met zich meedragen en deze bij het slachtoffer installeren. Ze kunnen dan zelfs geprogrammeerd zijn om het verwijderen van die malware te detecteren en ongedaan te maken. Doordat rootkits vaak zeer moeilijk te verwijderen zijn, kunnen de hoge kosten van het opruimen worden gezien als schade. In dat geval is sprake van overtreding van art. 350a lid 3.

Backdoor

Een achterdeur ("backdoor") is precies wat de naam aangeeft: een programma dat toegang biedt tot de computer waarop het is geïnstalleerd. Vaak wordt achterdeur-software of backdoors geïnstalleerd door wormen of Trojaanse paarden. Ze houden zich meestal verborgen door gebruik te maken van rootkit-technieken. Eén van de oudste voorbeelden is Back Orifice, maar tegenwoordig zijn er tientallen vergelijkbare software-pakketten.

Omdat achterdeuren worden gebruikt om binnen te dringen in andermans computer, zijn ze strafbaar als hulpmiddel voor computervredebreuk (art. 139d lid 2 onder a).

Via de achterdeur kan de computer op afstand worden bestuurd. Een veel gebruikte toepassing hiervan is het versturen van reclame-mail (spam). Ook kan hiermee bijvoorbeeld een verstikkingsaanval worden uitgevoerd. Als de aanvaller dit met veel computers tegelijk doet, is de aanval bijzonder lastig te stoppen voor het slachtoffer.

Een verzameling computers die voorzien zijn van achterdeuren wordt ook wel een botnet genoemd, omdat ze in wezen als een netwerk van willoze robots ingezet kunnen worden door de beheerder van de software. Vanwege het 'willoos' heten de computers soms ook wel zombies.

Een heel andere betekenis van "achterdeur" is "truc waarmee stiekem toegang tot een systeem te krijgen is". Een programmeur kan bijvoorbeeld een speciaal wachtwoord inbouwen in zijn software waarmee hij altijd in kan loggen of de beveiliging kan omzeilen. Ook dergelijke achterdeuren zijn strafbaar als hulpmiddel voor computervredebreuk (art. 139d lid 2 onder a).

Nepwaarschuwingen

Naast echte virussen, wormen en andere kwaadaardige software doen ook berichten over malware steeds vaker de ronde. Meestal zijn zulke berichten nep. Alhoewel het vervelend is om ze te krijgen, zijn dergelijke berichten niet strafbaar.

Dat zou wellicht anders worden wanneer de berichten proberen schade aan te richten. Een voorbeeld is de Teddybear hoax (Engelstalig) die mensen vertelt dat ze een bepaald bestand moeten weggooien omdat het een virus is. In werkelijkheid gaat het om een onderdeel van Windows.

PHISHING

Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website en ze daar — nietsvermoedend Bij phishing wordt dikwijls gebruikgemaakt van URL-spoofing. Dit is het nabootsen van de URL van bijvoorbeeld een bank, zodat de gebruiker denkt de echte site te bezoeken, terwijl de URL die van de bedrieger is.

Sinds het gebruik van het IDN-systeem (International Domain Name), waarbij niet-ASCII-tekens kunnen gebruikt worden in domeinnamen, kan phishing hiervan gebruikmaken door een echte domeinnaam na te bootsen met gelijkwaardige buitenlandse tekens, zodat de gebruiker niet merkt dat het adres niet klopt.

Zelfs met een gewone ASCII-URL kan bedrog gepleegd worden: zo lijkt het adres www.google.com, waarin de

kleine letter l vervangen is door een hoofdletter i (I), erg op www.google.com, en kan het er, afhankelijk van het lettertype, zelfs exact gelijk uitzien.

De meeste banken maken tegenwoordig gebruik van een Extended Validation Certificate, in moderne internetbrowsers wordt het eerste gedeelte van de adresbalk weergegeven met een groene achtergrond, zodat de gebruiker zeker weet dat hij op de echte pagina zit.

Meestal ontvangt het slachtoffer een mail waarin hem gevraagd wordt zijn account bij bijvoorbeeld een bank te checken en bevestigen. Ook wordt er wel gebruikgemaakt van instant messaging, soms wordt er telefonisch contact opgenomen. Fraudeurs maken veelvuldig gebruik van nepsites van financiële instellingen, eBay en PayPal. Phishing is moeilijk te achterhalen, internetters moeten vooral zelf alert zijn en nooit ingaan op een mailverzoek waarin gevraagd wordt persoonlijke (financiële) gegevens te geven; zoals bankrekeningnummer, pincode, BSN of creditcardgegevens. Het eerste geval van phishing dateert uit 1996.

Hoe te herkennen

In een phishing-bericht vind je vaak de volgende elementen

- Er wordt gedreigd met gevolgen als je niet onmiddellijk gehoor geeft aan de mail.
- Je kan worden gevraagd om naar een bepaald nummer te bellen, waar je dan je gegevens moet doorgeven.
- Je kan worden gevraagd om op een link te klikken, die je dan naar een valse site leidt. Daar moet je je dan inloggen.
- Een veelgebruikte methode is dat de fraudeur een e-mail stuurt met een bijlage waarin een Keylogger zit verborgen. De mail functioneert dan als een Trojaans paard. Zodra de gebruiker de bijlage heeft geopend, wordt — op de achtergrond — de keylogger geactiveerd. Hierdoor kan de fraudeur via internet zien welke wachtwoorden de gebruiker gebruikt bij het inloggen bij zijn of haar bank.

— te laten inloggen met hun inlognaam en wachtwoord of hun creditcard-nummer. Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De slachtoffers worden vaak via e-mail naar deze valse website gelokt met daarin een link naar de (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren".

Een gelijkaardige vorm van oplichting werd uit analogie pharming genoemd. Beide methoden worden gebruikt voor identiteitsfraude.

- Tip 1 – Klik nooit op links, tik zelf de url in. Hierdoor weet je zeker dat je niet onderwater naar een andere website wordt gestuurd
- Tip 2 – Ziet de URL er raar uit? Maak hier dan geen gebruik van. Er bestaat een kans dat je met een phishing website te maken hebt
- Tip 3 – Grammatica of spelfouten komen vaak voor in phishing e-mails of op phishing websites. Wees hier alert op
- Tip 4 - Wees op je hoede wanneer er om je betalingsgegevens gevraagd wordt

Keyloggers

Een keylogger is een programma of een stuk hardware waarmee men de toetsaanslagen tot zelfs de muisbewegingen van een computergebruiker kan registreren.

Redenen voor het gebruik van keyloggers

Deze informatie kan worden gebruikt voor verscheidene doeleinden. Meestal probeert men via keyloggers persoonlijke informatie te stelen. Hierbij gaat het vaak om wachtwoorden en gebruikersnamen of creditcardnummers. Ook belangrijke en vertrouwelijke e-mails kunnen onderschept worden. Tegenwoordig worden keyloggers ook ingezet op de werkvloer. Op deze manier kunnen werkgevers hun werknemers controleren. Een keylogger kan er bijvoorbeeld voor zorgen dat er een lijst van alle bezochte websites wordt blootgelegd. Zo kan de werkgever nagaan of zijn werknemers wel degelijk aan het werk zijn.

Een keylogger kan ook dienst doen als back-up, namelijk als het computersysteem crasht. Deze functie van keyloggers is dan weer interessant voor grotere bedrijven waarbij crashes ernstige gevolgen kunnen hebben. Keyloggers kunnen reeds worden ondergebracht onder de noemer van spyware.

De werking van een keylogger

Het programma draait op de achtergrond waardoor de nietsvermoedende gebruiker geen last ondervindt of er ook maar iets van opmerkt. Een keylogger slaat zijn informatie op in een logfile. Deze kan via het internet bezorgd worden aan de opdrachtgever, bijvoorbeeld via e-mail. Je kunt het programma van een keylogger beveiligen door middel van een wachtwoord. Hierdoor kan enkel de opdrachtgever het programma gebruiken. Een keylogger kan aan een tijdschema worden onderworpen zodat de taken enkel uitgevoerd worden tijdens de uren dat de gebruiker meestal actief is. Naast de belangrijkste functies zijn keyloggers ook in staat om klembordtekst te loggen. Uitgebreidere keyloggersoftware kan ook regelmatig screen captures maken, waardoor gelogd wordt wat er op dat moment op het scherm te zien was.

Beveiligen tegen keyloggers

Software voor keyloggers staat niet standaard op een computer, maar wordt veelal geïnstalleerd door de hacker zelf, weliswaar via een omweg. Keyloggers kunnen doorgegeven worden via het installeren van software of via virussen en wormen. Vaak gebeurt dit zonder dat de gebruiker zich van kwaad opzet bewust is. Daarom is het voor gebruikers belangrijk de computer goed te beveiligen. Hier zijn enkele suggesties:

- Maak gebruik van de firewall. Keyloggers verspreiden hun informatie via het internet. Een firewall kan onbekende programma's die contact zoeken met het internet opmerken, om dan de gebruiker te waarschuwen.

- Installeer antivirussoftware en een programma dat spyware tegengaat. Deze zijn in staat om de aanwezigheid van keyloggers op te sporen. Eenmaal ze de aanwezigheid van keyloggers ontdekt hebben, kunnen ze ook gebruikt worden om deze keyloggers te verwijderen van de computer.

- Tegenwoordig bestaat er specifieke software om keyloggers op te sporen. Dewasoft bracht eerder al twee tools op de markt die deze taak op zich nemen.

- Voorzichtig zijn bij het installeren van software die nieuw voor je is. Het kan zijn dat bij deze software een virus zit of bij de installatie ervan ook een keylogger wordt geïnstalleerd.

- Het is zeer belangrijk om je browser up-to-date te houden. Deze updates kunnen hun inbreng hebben in het veiliger surfen.

Hardware keylogger

Keyloggers bestaan niet alleen in de vorm van software, maar ze kunnen ook als hardware voorkomen. Het is een soort hulpstukje tussen de computer en de kabel van het toetsenbord. Deze keyloggers hoeven niet geïnstalleerd te worden via software en kunnen zelf ook niet opgemerkt worden door scanners. Ze hebben echter het nadeel dat ze waarneembaar zijn langs de buitenkant van de computer, maar voor mensen die niets kennen van computers en hardware is het zeer moeilijk om een keylogger op te merken.

Formaten

Een hardware keylogger beschikt over een flashgeheugen. Dit kan variëren van 2MB tot 2GB. Een keylogger met een geheugencapaciteit van 2MB stemt ongeveer overeen met 1.000.000 toetsaanslagen. Keyloggers zijn verkrijgbaar in verschillende formaten:

- USB-aansluiting
- PS/2-aansluiting
- Men kan ze ook via een chip installeren in het toetsenbord zelf.

Extra functies en varianten

Keyloggers kennen heel wat varianten. Zo zijn er keyloggers met of zonder extra software. Deze software kan helpen om de instellingen te wijzigen naar de voorkeur van de gebruiker. Andere extra opties zijn bijvoorbeeld de timerfunctie en wifi. Door de timerfunctie kan de keylogger bijhouden op welke datum en welk uur de gebruiker iets getypt heeft. Wifi-keyloggers zijn heel wat duurder omdat zij hun informatie rechtstreeks kunnen doorsturen via het internet naar de opdrachtgever.

Wireless keylogger

Naast hardware keyloggers bestaan sinds kort ook in wireless keyloggers. Het geheel bestaat uit een kabel van het toetsenbord naar de computer van de gebruiker, de transmitter, en een ontvanger. In die transmitter zit een ingebouwde draadloze verbinding met de ontvanger. De opdrachtgever beschikt zelf over die ontvanger. Zo kan de transmitter alle verwerkte informatie doorsturen naar de ontvanger.

Het grote voordeel is dat eenmaal de transmitter geïnstalleerd is, de opdrachtgever zich niet meer moet vertonen aan de computer van de gebruiker. Uiteraard werkt een draadloze verbinding maar vanaf een bepaalde afstand. De maximale afstand kan ongeveer 50 meter bedragen.

Met computers die iemand niet zelf beheert moet voorzichtig worden omgegaan. Een computer in een internetcafé zou bijvoorbeeld door een (vorige) gebruiker besmet kunnen zijn met een keylogger. Het kan dan nog steeds zo zijn dat er een antivirusprogramma actief is, maar dat alle meldingen met betrekking tot de keylogger handmatig uitgezet zijn.

Toekomst van de keylogger

Keyloggers zijn legaal verkrijgbaar en worden dus gebruikt voor verschillende doeleinden. Tegenwoordig gaan mensen al zo ver om hun kinderen te controleren terwijl ze surfen op het net. Buiten de voordelen die keyloggers bieden, moet men toch nadenken over de gevolgen die ze met zich mee kunnen brengen. Aangezien keyloggers legaal zijn, zou het kunnen dat over enkele jaren een keylogger standaard wordt ingebouwd in een toetsenbord

DNS aanval (vervolg op nieuwsbrief 1)

Het uitvoeren van een denial of service aanval (of in mooi Nederlands ***een verstikkingsaanval***) is sinds 1 september 2006 ook strafbaar. Op het belemmeren van de toegang tot of het gebruik van een systeem door daaraan gegevens aan te bieden of toe te zenden staat maximaal 1 jaar cel of geldboete van 16.750 euro (art. 138b).

Bij een dergelijke aanval worden zo veel gegevens verstuurd naar een systeem dat dit systeem niet meer in staat is normaal te functioneren. Voorbeelden zijn het massaal sturen van nepverzoeken naar Websites, iemands mailbox volstoppen met tienduizenden e-mailberichten (of juist met een paar hele grote berichten - een "e-mail bom"), of het zo vaak opvragen van een webpagina dat de server dit niet meer aankan.

Het belemmeren moet wel opzettelijk gebeuren. Wanneer een populaire website een link legt naar iemands site, die de massale toename in bezoekers vervolgens niet aankan, is er geen sprake van een verstikkingsaanval.

Voorbeelden van verstikkingsaanvallen

Verstikking van websites

Een verstikkingsaanval wordt meestal uitgevoerd tegen Websites. Daarbij wordt de site gebombardeerd met verzoeken om webpagina's, of worden juist grote bestanden op die site zeer vaak opgevraagd. Al deze verzoeken belemmeren het versturen van legitiem opgevraagde webpagina's.

Verstikking van mailboxen

Ook kan een verstikkingsaanval uitgevoerd worden door het versturen van extreem grote aantallen e-mails, of juist e-mails met zeer grote bijlagen. Dit verstopt de mailbox van de ontvanger, en belemmert daarmee dus het gebruik van de e-mail dienst.

Verstikken door claimen systeembronnen

Veel verstikkingsaanvallen gebeuren door zo veel mogelijk gegevens te versturen, zodat de ontvanger daar onder bezwijkt. Een andere mogelijkheid is het belemmeren van het systeem door zo veel mogelijk systeembronnen te claimen. Een gebruiker kan bijvoorbeeld alle vrije ruimte reserveren op een netwerkschijf, waardoor anderen daar geen bestanden meer op kunnen slaan.

- Verstikken van netwerk

- Verstikkingsaanvallen zijn vaak gericht tegen één specifieke computer. Ze kunnen ook tegen een heel netwerk tegelijk gericht worden, bijvoorbeeld door de router aan te vallen zodat geen enkele computer op dat netwerk meer verkeer kan zenden of ontvangen. Zo werden in 2002

verstikkingsaanvallen uitgevoerd tegen de root DNS servers, waardoor in potentie heel Internet platgelegd had kunnen worden.

Willoos meedoen

Het is ook mogelijk dat de aanvaller de computers op het netwerk van het slachtoffer zelf mee laat doen aan de aanval. Het Internet- protocol kent bijvoorbeeld een speciaal bericht dat neerkomt op "bent u daar nog" (het "ping" bericht). Een computer die dat bericht ontvangt, zal een bevestiging sturen naar de afzender (dat heet dan natuurlijk het "pong" bericht). Ook hebben netwerken vaak een adres (het broadcast adres) waarmee alle computers op een netwerk te bereiken zijn. Een ping-bericht naar dat adres zorgt dus voor antwoorden van alle computers tegelijk. Dat vaak herhalen kan het netwerk al aardig verstoppen.

Misbruiken van protocol

Ook kan misbruik worden gemaakt van een netwerkprotocol. Een voorbeeld is wat heet een SYN-flood. Om een verbinding tot stand te brengen tussen twee computers op Internet, stuurt de eerste computer een verzoek naar de tweede. Deze bevestigt dat de verbinding gemaakt kan worden, waarna de eerste computer een laatste bericht stuurt waarmee de verbinding feitelijk tot stand komt. De verstikkingsaanval berust nu simpelweg in het feit dat dit laatste bericht nooit wordt verstuurd, zodat de tweede computer computer gedurende een lange tijd blijft wachten. Ondertussen kan hij geen andere verbindingen meer accepteren. Daarmee wordt de toegang tot het systeem belemmerd.

Programmabommen

Bij een verstikkingsaanval moet het gaan om belemmeren door het versturen van gegevens of verzoeken. De goede werking van een systeem kan ook worden belemmerd door een programma te draaien dat het systeem overbelast. Zulke programma's heten ook wel logische bommen.

Een bekend voorbeeld is de zogeheten forkbom: dit programma doet niets anders dan kopieën van zichzelf opstarten tot het systeem geen enkel ander programma meer kan opstarten. Ook kan een programma continu op volle kracht steeds dezelfde rekenoperatie uitvoeren, waardoor het alle processorkracht claimt. Hierdoor kunnen andere programma's veel minder goed functioneren.

Dergelijke activiteiten zouden wellicht als verstikkingsaanval kunnen worden gezien, wanneer het installeren (uploaden) van dit programma gezien wordt als het versturen van gegevens. Ook kunnen ze worden vervolgd als het opzettelijk vernielen, beschadigen of onbruikbaar maken van een computer- of communicatiesysteem (art. 161sexies lid 1).

Spam en verstikking

Het versturen van ongewenste e-mail (spam) is op zichzelf nog geen verstikkingsaanval. Pas wanneer het ontvangende systeem in de werking wordt belemmerd, kan er sprake zijn van een verstikkingsaanval. Grofweg dus pas wanneer de mailserver bezwijkt onder de aangeboden mail.

In 2002 organiseerde een producent van vitaminepreparaten een e-mail actie waarbij binnen zes maanden meer dan 600 miljoen(!) e-mails werden verstuurd naar politici in de Tweede Kamer. Oftewel meer dan 30 per seconde. De servers van het parlement konden dit niet aan. Hiervoor moest

hij een schadevergoeding betalen. Met de huidige wet computercriminaliteit had dit vervolgd kunnen worden als een verstikkingsaanval.

Het versturen van spam aan natuurlijke personen is overigens wel verboden onder artikel 11.7 van de Telecommunicatiewet. Zie o.a. de uitspraak van de Hoge Raad inzake Ab.Fab/XS4All.

Gedistribueerde verstikking

Een verstikkingsaanval kan worden gepleegd vanaf één enkele computer, maar dat is niet zo effectief omdat de meeste computers slechts een beperkte hoeveelheid gegevens kunnen versturen. Bovendien is dan de aanvaller natuurlijk snel terug te traceren. Vandaar dat de zogeheten distributed denial of service (DDoS) aanval de laatste jaren steeds populairder is geworden. Hierbij worden tientallen of honderden computers (in fraaie Internet-terminologie "zombies") tegelijk ingezet om gegevens te versturen naar het slachtoffer.

Een veel gehoorde vraag is of het door computers van derden laten versturen van gegevens valt onder strafbare verstikking. Artikel 138b spreekt alleen van het "aanbieden of versturen" van gegevens. Bij een DDoS-aanval verstuurt de dader wel degelijk gegevens naar het slachtoffer, alleen gebruikt hij andermans computers om dit te doen. Daarmee is dus ook de gedistribueerde verstikkingsaanval verboden volgens dit artikel.

Internet-providers

Dit wetsartikel is met name gericht tegen aanvallen op gebruikers (personen en bedrijven) van netwerken. Wanneer een Internet-provider slachtoffer is van een verstikkingsaanval, kan dat ook gerekend worden onder het verhinderen of bemoeilijken van een openbare telecommunicatiedienst (art. 161sexies). Wanneer dat leidt tot "gemeen gevaar voor de verlening van diensten" kan de aanvaller tot maximaal zes (in plaats van één) jaar cel veroordeeld worden. Zo vond de rechtbank dat een denial-of-service aanval tegen de sites van overheid.nl en geenstijl.nl onder bemoeilijken van een openbare telecommunicatiedienst viel

Effectiviteit van de aanval

Er moet wel sprake zijn van een echte belemmering, een "aanval" waarbij een marginaal aantal pakketjes gegevens worden verstuurd is niet strafbaar. Het is echter niet nodig dat de toegang of het functioneren volledig wordt geblokkeerd. Ook een gedeeltelijke blokkade valt al onder dit wetsartikel. Wordt naast (of door) het belemmeren van de toegang ook schade aan het systeem toegebracht, dan valt dat onder de algemene bepalingen van vernielen van gegevens.

Hulpmiddelen

Net als software en andere hulpmiddelen voor computervredebreuk zijn ook hulpmiddelen voor verstikkingsaanvallen verboden. Het maken, vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van dergelijke software is een strafbaar feit (art. 139d lid 2 onder a). Hierop staat een jaar cel (of een boete van 16.750 euro).

De hulpmiddelen moeten wel specifiek gemaakt zijn voor verstikkingsaanvallen. In theorie kun je met een gewoon e-mail programma mailbommen versturen, daarmee is dat programma nog geen

verboden hulpmiddel geworden. Ook een Linux-programma als "ping" kan gebruikt (misbruikt?) worden bij een verstikkingsaanval maar is daarmee nog niet verboden.

POLITIEMETHODES VOOR BEWIJS

De politie heeft diverse methode tot haar beschikking om digitaal bewijsmateriaal te verzamelen. Naast onderzoek van in beslag genomen opslagmedia (zoals harde schijven) kan zij ook de provider een tap laten leggen en persoonsgegevens vorderen.

Het gebruik van elektronische systemen laat veel sporen na. Deze kunnen worden gebruikt als bewijsmateriaal bij een strafrechtelijk onderzoek. De politie heeft diverse methode tot haar beschikking om dergelijk bewijsmateriaal te verzamelen. Zo kunnen harde schijven in beslag worden genomen, of kan de eigenaar worden bevolen een kopie hiervan ter beschikking te stellen. De eigenaar kan tevens worden verplicht versleutelde bestanden te ontcijferen. De verdachte is echter niet verplicht tot het afgeven van een kopie van een bestand, of het ontcijferen van een versleuteld bestand. Daarnaast kan een Internet provider worden gedwongen al het Internet verkeer van een verdachte op te nemen, zodat de politie zijn e-mail, chats en website-bezoeken kan natrekken.

Bestandsbeheer

De politie mag, naast fysieke zaken zoals documenten, ook elektronische gegevens in beslag nemen.

Bewijsmateriaal tegen een verdachte kan bijvoorbeeld worden verzameld bij een huiszoeking. Hierbij mogen niet alleen maar tastbare zaken meegenomen worden. Ook elektronische gegevens kunnen "in beslag" worden genomen. Art. 125i Wetboek van Strafvordering bepaalt dat de rechter-commissaris het bevel kan geven dat hem toegang moet worden gegeven tot elektronische gegevens, of dat hiervan een kopie wordt gemaakt die dan op het gerechtelijk lab nader onderzocht kan worden.

Dit bevel mag niet worden gegeven aan de verdachte. Deze is immers niet verplicht mee te werken aan zijn eigen veroordeling en hoeft dus geen bewijs tegen zichzelf beschikbaar te stellen. De politie kan natuurlijk wel simpelweg de PC van een verdachte in beslag nemen, zodat diens harde schijf op het bureau rustig uitgeplozen kan worden op belastende informatie. Ook CD-ROM's en andere opslagmedia kunnen worden gekopieerd of meegenomen.

Het bureau Digitale Expertise van de politie onderzoekt vervolgens de in beslag genomen opslagmedia. Een bekend programma dat hierbij gebruikt wordt, heet EnCase. Dit programma kan bijvoorbeeld achterhalen op welk moment de verdachte bepaalde bestanden voor het laatst heeft geopend en wat hij heeft weggegooid. EnCase kan alle gewiste bestanden weer tevoorschijn halen. Zo'n analyse is echter niet blindelings te vertrouwen. Stel, er wordt een aantal gewist kinderpornofoto's teruggevonden. Heeft de verdachte die nu direct na ontvangst weggegooid omdat hij daar niets mee te maken wil hebben? Of heeft hij ze een dag voor de huiszoeking gewist na de datum van zijn PC op een aantal maanden eerder te hebben gezet? In beide gevallen zal EnCase aangeven dat de bestanden enkele maanden geleden zijn weggegooid.

Wachtwoorden achterhalen

Als informatie versleuteld is, kan de politie daar weinig mee zonder het juiste wachtwoord. Een verdachte mag niet worden bevolen dit wachtwoord te onthullen. Als anderen, zoals de provider of systeembeheerder, het wachtwoord toevallig weten, moeten ze het wel afgeven.

Wachtwoord raden

Om ongeauthoriseerde toegang tot een computersysteem te voorkomen, wordt meestal gebruik gemaakt van wachtwoorden. Ook elektronische bestanden kunnen worden beveiligd. Deze bestanden worden dan met behulp van een wachtwoord versleuteld (encryptie), waardoor ze onleesbaar zijn voor iedereen die het wachtwoord niet kent. Dat is althans de theorie.

In de praktijk blijkt dat mensen vaak gemakkelijk te raden wachtwoorden kiezen, zoals hun trouwdatum, een favoriet vakantieoord of de voornamen van hun kinderen. Ook zijn veel encryptie-programma's niet zo goed als de reclame suggereert. Voor bijna alle commerciële encryptie-programma's (inclusief de wachtwoord-beveiliging van Microsoft Word, Winzip en de 3Com Palm handcomputers) zijn kraakprogramma's beschikbaar die binnen enkele minuten het wachtwoord weten te raden of zelfs zonder het wachtwoord het oorspronkelijke bestand kunnen achterhalen.

Met zo'n kraakprogramma is het dus voor de politie erg eenvoudig om versleutelde bestanden te ontcijferen. Ook kunnen ze bij een huiszoeking natuurlijk de papiertjes in beslag nemen waar de wachtwoorden op geschreven staan.

Bevel tot afgeven wachtwoord

Daarnaast biedt het Wetboek van Strafvordering de mogelijkheid om de persoon die het wachtwoord weet te bevelen het wachtwoord af te geven dan wel toegang te geven tot het beveiligde systeem of bestand (art. 125k eerste lid). Een Internet provider kan dus verplicht worden de politie toegang te geven tot bestanden van een klant die op hun server staan. De systeembeheerder van een bedrijfsnetwerk kan eveneens worden verplicht om beveiligde gegevens van een medewerker te ontcijferen, bijvoorbeeld in het kader van een fraude-onderzoek. Binnen bedrijven worden bestanden namelijk vaak zodanig versleuteld dat de systeembeheerder ze altijd kan ontcijferen, voor het geval de betreffende medewerker onder de tram loopt of (wat vaker voorkomt) zijn wachtwoord is vergeten. Ook dit bevel mag niet worden gegeven aan de verdachte zelf (art. 125k, zesde lid).

Aftappen van communicatie

De politie mag vrijwel alle elektronische communicatie aftappen en opnemen.

Een andere manier om bewijs te verzamelen tegen een verdachte is het aftappen van zijn elektronische communicatie. Op grond van de Telecommunicatiewet kan de politie, maar ook opsporingsdiensten zoals de AIVD, met een gerechtelijk bevel eisen dat een Internet-provider naam en adres van een abonnee aan hen bekendmaakt. Ook kunnen ze eisen dat alle e-mail van deze abonnee wordt gekopieerd naar een speciale mailbox of zelfs dat al zijn gesprekken via MSN Messenger of ICQ opgenomen worden. Voor mobiele telefonie is opnemen van alle gesprekken en vastleggen wie wanneer met wie belde mogelijk.

Uit dergelijke opnames kan bijvoorbeeld blijken dat de verdachte regelmatig kinderporno ontvangt per e-mail of via een file sharing programma, of bezig is met het kraken van beveiligde computersystemen. Op basis hiervan kan dan een huiszoekingsbevel worden verkregen zodat de harde schijf van de verdachte in beslag kan worden genomen en geanalyseerd.

Ook is het mogelijk om met een dergelijke tap wachtwoorden te achterhalen. Veel mensen gebruiken namelijk hetzelfde wachtwoord op diverse verschillende systemen. Het wachtwoord van het inbelaccount of de POP3 mailserver is dus een goede kandidaat bij het raden van het wachtwoord van de versleutelde bestanden. Daarnaast is het ook goed mogelijk dat mensen via e-mail of de chat wachtwoorden aan elkaar doorgeven. Dit gebeurt met name bij hackers die hun vriendjes toegang willen geven tot systemen die zij zojuist gekraakt hebben.

Taps zijn helemaal nuttig bij Web-gebaseerde e-mail diensten als Hotmail of Yahoo!. Alle informatie wordt zonder versleuteling via een enkele server verstuurd, waardoor het perfect mogelijk is mee te lezen met alle verzonden en ontvangen mailtjes. Een groot probleem bij dergelijke taps is dat op deze manier bijzonder veel informatie opgeslagen wordt. Het kan maanden, zoniet jaren duren voordat dit allemaal ontcijferd en geanalyseerd is. Immers, elke e-mail (inclusief alle spam en reclame), en elke letter uit elke chat, en alle tekst en afbeeldingen van elke bezochte webpagina wordt op deze manier opgenomen.

Waarde van bewijs

Elektronische sporen mogen dan makkelijk te vinden zijn, het is ook makkelijk om ze te vervalsen. De datum van een bestand is eenvoudig te wijzigen, en met een beetje kennis is het mogelijk om een perfecte vervalsing van een e-mail of een logbestand te maken. En natuurlijk is het ook mogelijk dat iemand ingebroken heeft op de computer van een ander, en langs die weg het bewijsmateriaal op die computer heeft geïnstalleerd. De waarde van dergelijk bewijs is dan ook moeilijk in te schatten.

De rechter zal op basis van de omstandigheden van het geval moeten kijken hoeveel waarde hij hecht aan het bewijs. Als bijvoorbeeld logbestanden van diverse Internet providers overeenstemmen met gegevens die van de PC van de verdachte zijn gehaald, dan is het redelijk om te veronderstellen dat deze gegevens juist zijn. Echter, een e-mail die in geen enkel systeem terug te vinden is behalve op de computer van degene die aangifte deed is al een stuk twijfelachtiger.

De mogelijkheid om bij een Internet provider een tap te laten uitvoeren is daarom erg waardevol. Dit gebeurt namelijk met een aparte, verzegelde computer, waardoor het vrijwel zeker is dat de opgeslagen gegevens authentiek zijn.

Het in nieuwsbrief 1 aangekondigd onderdeel Cloud Computing is ivm de lengte van deze nieuwsbrief doorgeschoven naar nieuwsbrief 3
