Nieuwsbrief 3-2012

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:

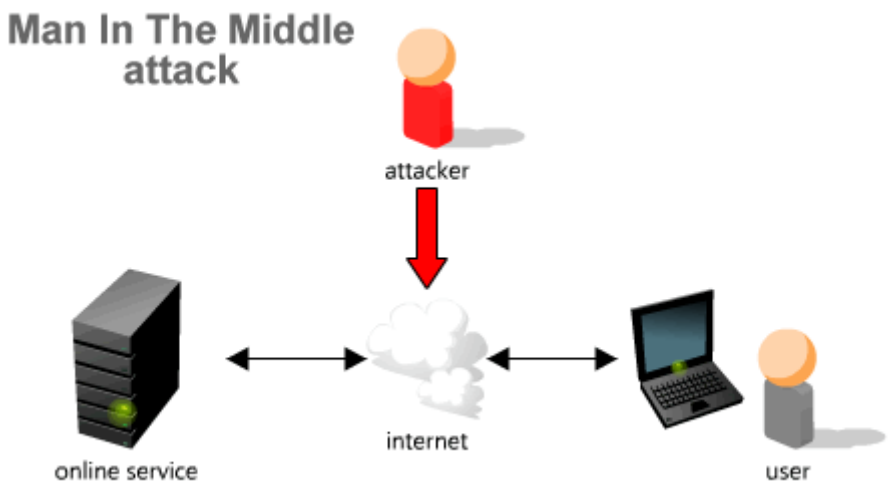
- onderwerpen die betrekking hebben op het veilig gebruik van de computer en het internet
- nieuws uit de media
- juridische vragen
- nieuwe technieken
- vele andere wetenswaardigheden

In deze editie o.a

Man in the Middle

“Ik was aan het internetbankieren, wilde een rekening betalen en voor dat ik het kon af knipogen was er een groot bedrag van mijn rekening afgeschreven middels een betaalopdracht die ik niet heb ingevoerd”.

Hoe kon dit gebeuren?



De rekeninghouder slachtoffer is geworden van malware, een illegaal geïnstalleerd programmaatje dat het voor criminelen mogelijk maakt om in de besmette computer te kijken en de pc zelfs over te nemen. Log je in op de website van de bank dan kan een crimineel dat zien en zelfs betaalopdrachten toevoegen zonder dat de rekeninghouder dat merkt. In jargon wordt deze methode een ***man-in-the-middle-aanval*** genoemd: de hacker plaatst zichzelf als het ware tussen de computer van de rekeninghouder en de site van de bank.

Het is een methode die de laatste tijd veel wordt toegepast. Veelal weet het slachtoffer niet op welke wijze de afschrijving heeft plaatsgevonden. U dus nu wel en kunt hem/haar dit mededelen.

ID-alert

Door het vele gebruik van social media (Facebook, Hyves enz.) is er van een ieder wel digitale informatie te vinden. Een bijkomend verschijnsel is misbruik van de door jou vermelde gegevens.

Wil jij jezelf beschermen tegen misbruik van je persoonlijke gegevens? Stel dan een ID-alert in, zodat je goed in de gaten kunt houden wat er over jou op internet verschijnt. Duikt er nieuwe informatie over jou op, dan weet je het meteen.

Hoe werkt het?

Een ID-alert is eigenlijk een intensieve zoekopdracht op internet naar nieuwe gegevens waarin jouw naam verschijnt. Zodra jouw naam ergens opduikt, krijg je een mailtje. Er zijn verschillende aanbieders waarbij je een ID-alert kunt aanmaken. Voorbeelden hiervan zijn Wieowie en Google. Zij kunnen je tevens laten zien wat er nu al over jou bekend is op internet. Beide diensten zijn gratis.

http://www.google.nl/alerts

http://wieowie.nl/registreer

Meldingsformulier identiteitsfraude:

http://www.overheid.nl/media/downloads/Meldingsformulier_Identiteitsfraude.pdf

Meldpunten

Meldpunt cybercrime

Het Meldpunt cybercrime van het Korps Landelijke Politie Diensten verwerkt alle meldingen die te maken hebben met:

kinderporno;

het seksueel benaderen van minderjarigen;

radicale en terroristische uitingen (afkomstig uit Nederland) op en via het internet.

Iedereen die cybercrime tegenkomt kan melding doen, via een online meldingsformulier. U geeft aan wat u heeft gezien, waar en wanneer u dit bent tegengekomen en wat uw eigen gegevens zijn. Het meldpunt beoordeelt alle meldingen die binnenkomen en stuurt de informatie door aan bijvoorbeeld de politie, het Openbaar Ministerie (OM) of de Algemene Inlichtingen en Veiligheidsdienst (AIVD). Een melding kan de basis zijn om actie te ondernemen.

Meldpunt Identiteitsfraude

Het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI) geeft voorlichting en advies over identiteitsfraude. U kunt bij het meldpunt terecht wanneer:

u vermoedt dat u slachtoffer bent van identiteitsfraude (het CMI geeft dan ondersteuning en advies);

de overheid uw persoonsgegevens niet goed heeft geregistreerd.

Om identiteitsfraude te melden moet u een meldingsformulier invullen en opsturen. U omschrijft wanneer u hebt ontdekt dat u mogelijk slachtoffer bent van identiteitsfraude, welke bewijzen u hiervoor hebt, wat de vermoedelijke schade is en of u weet wie de vermoedelijke dader is. Ook vult u uw persoonlijke gegevens in en vertelt u welke acties u hebt ondernomen.

Voor de melding van een fout in de registratie van persoonsgegevens gebruikt het CMI een apart meldingsformulier.

Serieuze behandeling melding

Het CMI zorgt ervoor dat de betrokken instanties de melding behandelen. Bij het CMI zijn onder andere de politie, marechaussee, de Immigratie- en Naturalisatiedienst en het Openbaar Ministerie aangesloten. Het meldpunt is een initiatief van de Nederlandse overheid.

Meldpunt Discriminatie Internet

Het Meldpunt Discriminatie Internet (MDI) verzamelt alle meldingen van uitingen van discriminatie op het internet. De organisatie richt zich voornamelijk op het Nederlandse deel van het Internet. Het kan gaan om discriminatie op basis van:

geloof;

afkomst;

seksuele voorkeur;

geslacht;

huidskleur;

en/of leeftijd.

Het MDI neemt alleen meldingen in behandeling die via de e-mail zijn verstuurd. Als de gemelde uiting strafbaar is, stuurt het MDI doorgaans een verzoek tot verwijdering. Wordt de uiting niet weggehaald, dan kan het meldpunt besluiten om aangifte te doen.

Meldpunt Kinderporno op Internet

Het Meldpunt Kinderporno op Internet zet zich in voor de bestrijding van seksueel kindermisbruik (kinderporno) via internet. Wanneer u vermoedt dat u afbeeldingen van seksueel kindermisbruik op internet bent tegengekomen, kunt u dit melden via de website van het meldpunt. Dit kan eventueel anoniem. Jongeren die online zijn lastiggevallen, kunnen dit melden bij www.helpwanted.nl. Dit is een onderdeel van het Meldpunt Kinderporno op Internet.

Het Meldpunt Kinderporno op Internet is een particuliere stichting, die wordt gefinancierd door het ministerie van Justitie, de Europese Commissie en sponsors. De organisatie werkt nauw samen met de politie.

Fraudehelpdesk

De Fraudehelpdesk wil zo veel mogelijk voorkomen dat mensen slachtoffer worden van fraude. Daarnaast helpt de helpdesk slachtoffers van fraude door te verwijzen naar de juiste instanties. De Fraudehelpdesk geeft onder andere tips hoe fraude is te voorkomen. Zo waarschuwt de Fraudehelpdesk om nooit via mail persoonlijke gegevens aan derden te geven. Zoals bankrekeningnummer, pasnummer, pincode of persoonsgegevens. Officiële instanties vragen nooit om deze gegevens. Wanneer dat toch gebeurt, is de kans op fraude groot.

Wetsartikelen voor computercriminaliteit in enge zin

(ruime zin: algehele benamingen / enge zin: specifieke verschijningsvormen)

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

. Artikel 138a WvSr: het binnendringen in een geautomatiseerd werk.

. Artikel 161 sexies WvSr: opzettelijk veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk of werk voor de telecommunicatie.

. Artikel 161 septies WvSr: stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie door schuld.

. Artikel 350a WvSr: het opzettelijk onbruikbaar maken en veranderen van gegevens.

. Artikel 350b WvSr: het onbruikbaar maken en veranderen van gegevens door schuld,

. Artikel 139c WvSr: het aftappen en/of opnemen van gegevens en

. Artikel 139d WvSr: het plaatsen van opname-, aftap- c.q. afluisterapparatuur.

Er zijn geen specifieke wetsartikelen om cybercrime in ruime zin aan te duiden. Voor de hoofddaad worden dezelfde wetsartikelen gebruikt als wanneer de criminele daad niet met ICT zou worden gepleegd.

Haatzaaien.

'Het zaaien van haat of het (opzettelijk) beledigen of discrimineren van een groep mensen wegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuele gerichtheid of hun lichamelijke, psychische of verstandelijke handicap, zonder een bijdrage te leveren aan het publieke debat, waarbij ICT essentieel is voor de uitvoering' .

Haatzaaien staat niet als zodanig in het wetboek.

Aande hand van de geformuleerde definitie kunnen echter de volgende wetsartikelen worden onderscheiden die delicten omschrijven welke vallen onder deze noemer:

. Artikel 147 WvSr: godslastering.

. Artikel 90quater WvSr: discriminatie.

. Artikel 137d WvSr: aanzetting tot discriminatie van een bevolkingsgroep.

. Artikel 137e WvSr: openbaarmaking discriminerende uitlatingen.

. Artikel 137f WvSr: deelname of steunen van discriminatie.

. Artikel 137g WvSr: discriminatie in ambt, beroep of bedrijf.

. Artikel 131 WvSr: opruiing.

Cyberstalking.

'Cyberstalking is de verzamelnaam voor het stelselmatig lastigvallen van een persoon door provocerende uitspraken te doen en/of berichten te plaatsen via online forums, bulletin boards en chatrooms, of de ander als het ware via spyware te bespioneren dan wel voortdurend ongevraagd e-mail en spam te sturen. Er is sprake van een verregaande inbreuk op de privacy van het slachtoffer' .

Relevante wetsartikelen zijn:

. Artikel 285b WvSr: belaging.

. Artikel 138a WvSr: computervredebreuk.

. Artikel 266 WvSr: belediging.

Grooming.

Grooming wordt door het particuliere Meldpunt Kinderpornografie op Internet (MKI) opgevat als het zich op internet anders voordoen (door een volwassene) met het doel om seksueel getinte contacten te leggen met kinderen. Deze contacten kunnen zowel virtueel (seksuele handelingen voor de webcam) als fysiek (een ontmoeting waarbij het kind daadwerkelijk seksueel misbruikt wordt) zijn . ***Op dit moment is grooming niet strafbaar***.

Grooming is echter wel opgenomen in het door Nederland ondertekende maar nog niet door Nederland geratificeerde EU-verdrag van Lanzarote van 25 oktober 2007, artikel 23 ('Solicitation of children for sexual purposes'), waarin landen zich verplichten om grooming strafbaar te stellen. Grooming is dan het door een volwassene via ICT leggen van contacten met een jongere met de intentie deze te ontmoeten voor het verrichten van seksuele

handelingen, gevolgd door het feitelijk geven van uitvoering aan het tot stand brengen van die ontmoeting. Dat is een aanzienlijk engere uitleg dan het MKI geeft, vooral omdat volgens het verdrag begonnen moet zijn met het realiseren van de ontmoeting ('material acts leading to such a meeting').

Spionage.

Spionage is het op illegale wijze, zonder toestemming verkrijgen van informatie door het gebruik van spionnen of andere middelen (Morris, 2004: 16). Met behulp van ogenschijnlijk onschuldige softwareapplicaties (spyware) kunnen computer- en telefoongegevens ongemerkt worden onderschept, afgeluisterd of bespioneerd.

Relevante wetsartikelen zijn:

. Artikel 138a WvSr: computervredebreuk.

. Artikel 139e WvSr: afluisteren, aftappen.

. Artikel 98 WvSr: misdrijven tegen de veiligheid van de staat.

. Artikel 273 WvSr: schenden van geheimen.

Handel in mensen of foute goederen.

Verschijningsvormen:

drugs, geneesmiddelen, vuurwapens en explosieven, mensenhandel- en smokkel, heling.

Kenmerkend bij deze vormen van cybercrime is dat de handel plaatsvindt op of middels ICT (bijvoorbeeld marktplaats) en dat de betrokken partijen weten dat het gaat om illegale handel.

Relevante artikelen zijn:

. Artikel 273a WvSr mensenhandel.

. Artikel 441a WvSr heling.

. Artikel 416 WvSr opzetheling.

. Artikel 417 WvSr opzetheling (gewoonte).

. Artikel 273a WvSr mensenhandel.

. Artikel 274 WvSr slavenhandel.

. Artikel 2 Wwm: wet wapens en munitie

. Artikel 31 Wwm: overdragen van wapens of munitie

. Artikel 2 Ow: opiumwet

. Artikel 3 Ow: opiumwet

. Artikel 3b Ow: opiumwet

Kinderpornografie.

Kinderpornografie is in Nederland strafbaar gesteld in artikel 240b Wetboek van Strafrecht. Kinderpornografie is volgens dit artikel iedere afbeelding - of gegevensdrager die een afbeelding bevat - van een seksuele gedraging waarbij iemand, die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar betrokken is'. Zowel het verspreiden, tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren als in bezit hebben ervan is in Nederland strafbaar. In Nederland is het enkel kijken naar kinderpornografie niet strafbaar.

Softwarepiraterij.

Bij piraterij gaat het feitelijk om illegale handel van allerhande 'cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden' . De nadruk ligt volgens het KLPD veelal bij eindgebruikers, internetpiraten en vervalsers, en in mindere mate bij gebruikers van licenties (bijvoorbeeld bedrijven) en computerverkopers. In alle gevallen is piraterij echter strafbaar en valt het onder meer onder het Wetboek van Strafrecht, de Auteurswet en de Merkenwet.

Relevante artikelen uit het wetboek van strafrecht zijn:

. Artikel 337 WvSr: handel goederen vervalste merken.

. Artikel 328 WvSr: oneerlijke mededinging.

. Artikel 441a WvSr: heling.

. Artikel 1 AW: auteurswet

. Artikel 31 AW: opzettelijk inbreuk op auteursrecht

. Artikel 31a AW: voorwerp met daarop een inbreuk op auteursrecht

. Artikel 31b AW: beroep maken van inbreuk op auteursrecht

Illegale kansspelen.

'Volgens de Wet op de kansspelen (Wok) is er in Nederland een verbod op het aanbieden, propageren en gebruikmaken van kansspelen waarvoor geen vergunning is verleend. Illegale kansspelen en gokken op het internet (bijvoorbeeld het online casino) is één van de groeiindustrieën op internet' .

Relevante wetsartikelen zijn:

. Artikel 1 Wks: wet op de kansspelen

. Artikel 1a Wks: piramidespelen.

Uitspraak 29 februari 2012:

Buitenlandse goksites moeten in Nederland op zwart. Dat is het finale verdict van de Hoge Raad in de langlopende zaak tussen Lotto en Ladbrokes. Volgens de uitspraak moeten websites en telefoondiensten van grote internationale gokbedrijven voor Nederlanders worden geblokkeerd. De zaak was in 2002 aangespannen door De Lotto. Het aanbieden van kansspelen door Ladbrokes was ‘oneerlijke concurrentie’, vond De Lotto, in Nederland monopolist bij het organiseren en aanbieden van kansspelen. De zaak ging langs alle denkbare rechters. In 2003 oordeelde de rechter in kort geding al dat de sites van Ladbrokes voor Nederlanders ‘op zwart’ moesten, in 2010 werd dat door het Europese Hof nog eens bevestigd. Nu heeft uiteindelijk de Hoge Raad ook geoordeeld dat het via internet aanbieden van gokmogelijkheden aan Nederlanders in strijd met de wet is.

E-fraude.

'De essentie van fraude is steeds dezelfde: mensen eigenen zich middels bedrog geld of vermogensbestanddelen toe waarop ze geen recht hebben en tasten daardoor de rechten van anderen aan. Er zijn verschillende begrippen in omloop om de cybervorm van fraude te beschrijven, zoals fraude in e-commerce en internetfraude . 'Bij deze vorm van fraude wordt het internet gebruikt om op oneigenlijke wijze gelden, goederen en diensten te

verkrijgen zonder daarvoor te betalen of tegenprestaties te leveren' .

Bij internetfraude wordt er al snel gedacht aan oplichtingen via verkoopsites op internet zoals marktplaats en e-bay. Wij gebruiken de term 'e-fraude' als overkoepelende term. E-fraude is bedrog met als oogmerk het behalen van financieel gewin waarbij ICT essentieel is voor de uitvoering. Fraude staat niet als zodanig in de wet genoemd. Relevante wetsartikelen uit het wetboek van strafrecht zijn:

. Artikel 326 WvSr: oplichting.

. Artikel 225 WvSr: valsheid in geschrifte.

. Artikel 310 WvSr: diefstal.

. Artikel 321 WvSr: verduistering.

. Artikel 416 WvSr: heling.

Cyberafpersen.

Afpersen is het verkrijgen van geld of goederen van een persoon of organisatie door middel van dreiging en/of geweld . Afpersen gebeurt sinds mensenheugenis, denk bijvoorbeeld aan betalen van protectiegelden aan de maffia of betalen van losgeld voor een ontvoerde. Cyberafpersing is: dreigen met het vernietigen of onbruikbaar maken van computergegevens of het dreigen met het via ICT openbaren van smaad, smaadschrift of een geheim, in beide gevallen met als doel financieel gewin.

De middelen die voor cyberafpersen worden gebruikt, zijn technologisch, zoals het creëren van botnets, uitvoeren van DDoS-aanvallen, defacing van websites en het stelen van digitale informatie uit digitale systemen. Cyberafpersing combineert het binnendringen in computers, de vernietiging en wijziging van data, social engineering, en het bang maken van slachtoffers .

Relevante artikelen in het Wetboek van Strafrecht zijn:

. Artikel 317 WvSr: afpersing.

. Artikel 318 WvSr: afdreiging.

. Artikel 138a WvSr: computervredebreuk.

. Artikel 161 sexies WvSr: opzettelijk veroorzaken van stoornis in de gang of in de

werking van een geautomatiseerd werk of werk voor de telecommunicatie.

. Artikel 161 septies WvSr: stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie door schuld.

. Artikel 350a WvSr: het opzettelijk onbruikbaar maken en veranderen van gegevens.

. Artikel 350b WvSr: het onbruikbaar maken en veranderen van gegevens door schuld.

Hacken.

Er is sprake van hacken indien iemand zich opzettelijk en op ongeautoriseerde wijze toegang verschaft tot ICT. Aan de hand van artikel 138a Sr (computervredebreuk) definiëren wij hacken als het opzettelijk binnendringen in een geautomatiseerd werk, waarbij er enige beveiliging is doorbroken of waarbij de toegang is verkregen door een technische ingreep, valse signalen/sleutel of het aannemen van een valse hoedanigheid. Uit de literatuur is af te leiden dat een hackpoging doorgaans voldoet aan drie criteria: het is ongeoorloofd, eenvoudig maar doordacht, en het getuigt van een hoge mate van technische onderlegdheid en expertise.

Sinds de invoering van de Wet Computercriminaliteit I, in maart 1993, kent Nederland wetgeving op het gebied van hacken. Op dit moment is in de wet niet alleen het inbreken in een computer strafbaar gesteld, maar bijvoorbeeld ook het vastleggen of vernielen van gegevens. Voor relevante wetsartikelen: zie cybercrime in enge zin.

Hacktivisme/cyberterrorisme.

ICT-storing door manipulatie van data en systemen. Hacktivisme staat voor het hacken van computersystemen uit politiek gemotiveerde, activistische overwegingen. Wanneer ICTsystemen die vitale infrastructuren aansturen (bijvoorbeeld transportsystemen, besturingssystemen in de chemische sector of belangrijke crisis- en informatiediensten) om politieke redenen worden aangetast om grootschalige maatschappelijke ontwrichting te veroorzaken, spreken we van een cyberterroristische aanval .

Van cyberterrorisme zijn in elk geval in Nederland geen voorbeelden bekend . Voor relevante wetsartikelen: zie cybercrime in enge zin.

SECURE COMPUTING