FOX-IT

FOX files 1

FOX-IT.COM
MAART 2011

SIOD TRAINING
Onderste steen boven

NATIONALE STRATEGIE
Polderen tegen cybercrime

AANVAL OP CRIMINELEN
Alle ballen op de spits

‘Doe altijd aangifte’

INTERVIEW MET OFFICIER VAN JUSTITIE, LODEWIJK VAN ZWIETEN

22


12


18


15


10


04

COLOFON

Redactieadres
Fox-IT Afdeling Marketing
Postbus 638
2600 AP Delft
015 - 284 79 99
015 - 284 79 90
marketing@fox-it.com
www.fox-it.com

Vormgeving
viervier, Rijswijk

Fotografie
Chris Bonis, Rotterdam
ANP Photo, Hollandse Hoogte

Interviews en teksten
Sabel Communicatie, Den Haag

COLUMN

Cybercrime, hot or not ?

Op het moment dat ik dit stuk schrijf krijg ik net de laatste update van ons Cybercrime symposium. Ik kan het bijna niet geloven: meer dan 220 inschrijvingen! De verwachting voor dit symposium lag initieel rond de 80 deelnemers, maar na bekendmaking schoten we meteen door 220 deelnemers! Wat is hier aan de hand?

Het onderwerp Cybercrime staat al jaren op onze agenda en nog geen jaar geleden dreigde het een buzzword te worden waarbij de aandacht van je luisteraars meteen wegebt als je er over begint. De mogelijkheden voor cyberfraude, spionage of oorlog zijn niet noemenswaardig toegenomen, technieken van cybercriminelen zijn ook niet noemenswaardig veranderd. Wat is er dan wel veranderd?

Het zit hem denk ik in twee zaken: echte aanvallen en strategische noodzaak. In de afgelopen periode hebben steeds meer organisaties en individuele burgers ondervonden dat hackers werkelijk serieuze financiele en maatschappelijke schade veroorzaken. Denk bijvoorbeeld aan de aanvallen tijdens de Wikileaks affaire, wereldwijde internetbankierfraude of het toenemend aantal spionagesporen in digitale netwerken. Het gaat nu niet alleen meer om de digitale brandalarmen en evacuatieplannen, maar om het uitrukken van de digitale brandweer en ambulance. De digitale criminelen worden gevonden en achter de fysieke tralies gezet.

Dan kom ik op het tweede punt: strategische noodzaak. Fox is de afgelopen periode vaak betrokken geweest bij acute digitale branden. We zien dat dan vaak ad hoc geschakeld wordt en regelmatig moet vertrouwd worden op vrijwilligerswerk. Ondanks alle risicosessies van de afgelopen jaren blijkt dat er nog een flinke slag moet worden gemaakt in de professionele inrichting voor de bescherming tegen cybercrime, er is behoefte aan een strategie. Eén voordeel hebben we nu wel, die strategie kan nu gemaakt worden met steeds meer ervaringsdeskundigen, die werkelijk een digitale brand kunnen blussen.

Menno van der Marel, directeur Fox-IT

ACTUEEL

De Nationale Cyber Security Strategie: een stap voorwaarts?

POLDEREN TEGEN CYBER CRIME

Stuxnet, Wikileaks, een gigantisch botnet en een kinderpornonetwerk. Stuk voor stuk drukken ze ons met de neus op hetzelfde feit: Nederland is nog niet optimaal geoutilleerd om de strijd aan te binden met cybercriminelen. Om daar verandering in te brengen, heeft het ministerie van Veiligheid en Justitie eind februari de Nationale Cyber Security Strategie gelanceerd. Wat houdt die strategie in en is het voor onze digitale veiligheid een stap in de goede richting? Ronald Prins, directeur en medeoprichter van Fox-IT, geeft zijn visie.

De Nationale Cyber Security Strategie moet Nederland weerbaarder maken tegen nieuwe risico’s van de digitale samenleving. Onze buurlanden hadden zo’n strategie al langer. Mogen we daaruit concluderen dat we ons tot nu toe dan niet konden beschermen tegen cybercriminelen? Nee, dat denk ik niet. Maar de incidenten met Wikileaks en Stuxnet laten wel zien dat serieuze verstoringen mogelijk zijn en dat Nederland alle zeilen moet bijzetten om aanvallen via internet de baas te blijven. De bescherming die we tot nu toe hadden, was in elk geval onvoldoende. Daarvoor kan ik drie reden aanwijzen.

ONVOLDOENDE BESCHERMING

De belangrijkste reden is dat we in Nederland te weinig structurele operationele slagkracht hebben. Bij elk incident kruipen experts van publieke- en private partijen bij elkaar om het probleem te onderzoeken en aan te pakken. Dat is effectief gebleken, maar het is niet voldoende om de digitale veiligheid in de toekomst te waarborgen. Daarnaast is er gebrek aan regie. Vanuit hun traditionele blikveld hebben een aantal ministeries en andere organisaties zoals I&V en NCTb al hun eigen verantwoordelijkheid genomen. Dat heeft geresulteerd in diverse partijen die zowel op tactisch als operationeel niveau hun eigen gang lijken te gaan.
Tot slot ontbreekt Situational Awareness. We weten niet goed met wat voor soort digitale aanvallen we te maken hebben. Ook hebben we weinig idee van de potentiële hacking- en verstoringsmogelijkheden van onze huidige vijanden.

BESTAANDE ORGANISATIES BETROKKEN BIJ CYBERSECURITY

- Ministerie van Defensie - DEFCert
- Militaire Inlichtingen- en Veiligheidsdienst - ?
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties - GOVCERT.NL
- Ministerie van Veiligheid en Justitie - KLPD/THTC, BDE’s, OM, ZM, NCTb
- Algemene Inlichtingen- en Veiligheidsdienst - NBV + ?
- Ministerie van Economie, Landbouw en Innovatie - TNO/CPNI.nl
- Private partijen - Fox-IT en diverse anderen

‘De Nederlandse strategie onderscheidt ons van het buitenland: een integrale aanpak door publieke en private partijen’

INTERNATIONALE INITIATIEVEN

Cybersecurity is voor vrijwel elk land relevant. Het is dan ook niet verbazingwekkend, dat bijvoorbeeld de Verenigde Staten en het Verenigd Koninkrijk al langer een beveiligingsstrategie hebben. Een aantal incidenten in de Amerika heeft Obama heel snel na zijn aantreden doen besluiten om alle overheidsinitiatieven op dit gebied in kaart te brengen. Zo werd er ingebroken in een defensienetwerk via een USB-stick en werden sleeperbots gevonden in het elektriciteitsnetwerk. De belangrijkste maatregel van Obama was de benoeming van een Cyber Czar, gepositioneerd in het Witte Huis. Deze functionaris geeft een gezicht aan cybersecurity en garan-deert dat het onderwerp hoog op de agenda blijft staan.

VS: FOCUS OP DEFENSIE EN SPIONAGE

De Amerikaanse cyberstrategie beschermt de nationale veiligheid en moet er zo voor zorgen dat het land blijft functioneren. Daarom is het beleid vooral gericht op digitale dreigingen in het defensie- en spionageveld, en minder op vormen van cybercriminaliteit waar vooral burgers en bedrijven last van hebben. Het beveiligingsbeleid van Washington werkt in hoofdlijnen drie doelen uit:

- Het realiseren van een eerste verdedigingslinie tegen de huidige dreigingen. Denk daarbij aan het continu monitoren van alle overheidsnetwerken. Later moeten daar ook kritische private partijen op aansluiten. Bovendien krijgen de Amerikanen een responsmogelijkheid; verdedigen door aan te vallen.
- Het opbouwen van een volledige verdedigingsomgeving. Een goede verdediging is alleen mogelijk door continu te analyseren waar de dreiging vandaan komt en waar de interesse van de vijand ligt. Dit wordt ook wel contra-inlichtingen genoemd. Dat Amerika dit serieus neemt, blijkt uit het feit dat ze zelfs apparatuur uit het buitenland wantrouwen.

- Investeren in de toekomst. Meer opleiding en regie en herijking van onderzoek en ontwikkelingsprogramma's.

Ondanks de financiële crisis heeft de Amerikaanse overheid veel geld vrijgemaakt voor de aanpak van cybercrime. Voor het fiscale jaar 2011 bedraagt dit budget 3,6 mjrd dollar.

UK: SPECIALE VEILIGHEIDSDIENST

Het Verenigd Koninkrijk volgt Amerika in haar grootschalige aanpak. Naast de dreiging van andere staten en terroristen zien de Engelsen ook cybercrime als risico. Voor dat laatste gebied volgt later nog een specifieke strategie. De Nationale Recherche, de Serious Organised Crime Agency, draagt hiervoor de verantwoordelijkheid. Het belangrijkste initiatief van het Verenigd Koninkrijk is het inrichten van een multi-agency Cyber Security Operations Centre (CSOC). Deze operationele unit wordt ondergebracht bij de afluisterdienst GCHQ en heeft drie heldere taken:

- Verschaffen van situational awareness. Dit doet de unit onder andere door het internet in het Verenigd Koninkrijk permanent te monitoren.
- Analyseren van trends en dreigingsinschattingen maken. Zo brengt CSOC de mogelijkheden van eventuele aanvallers in kaart.
- Het technisch reageren bij een digitale aanval.

Behalve het beschermen van netwerken van de staat zelf, waarschuwt het CSOC via de Engelse veiligheidsdienst MI5 zelfs vitale bedrijven op het moment dat het CSOC vaststelt dat mogelijke spionage incidenten plaatsvinden. Het hele project wordt strategisch aangestuurd door de Office of Cyber Security (OCS) dat een plaatsje krijgt in the Cabinet Office, dus net als in de Verenigde Staten dicht bij de Prime Minister. Hoeveel geld de Engelsen hebben vrijgemaakt voor cybersecurity, is niet precies bekend. In ieder geval heeft het ministerie van Defensie ondanks alle bezuinigingen voor de komende vier jaar meer dan 500 miljoen Pond beschikbaar gesteld.

'We hebben weinig idee van de potentiële hacking- en verstoringsmogelijkheden van onze huidige vijanden'

NEDERLAND: ZES ACTIEPUNTEN

De basis van de Nederlandse strategie ligt in Kamervragen over de defensiebegroting eind 2008. De Kamer verbaasde zich erover dat nergens in de begroting een post was opgenomen voor de digitale veiligheid van Nederland, terwijl in veel omliggende landen dat wel gebeurde. De strategie die 'Den Haag' vervolgens ontwikkelde, kent zes actielijnen:

1. Integrale aanpak door publieke en private partijen.
2. Adequate en actuele dreigings- en risicoanalyses.
3. Versterken van de weerbaarheid tegen ICT-verstoring en cyberaanvallen.
4. Versterking responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren.
5. Intensivering opsporing en vervolging van cybercrime.
6. Stimuleren onderzoek en onderwijs.

De eerste hoofdlijn onderscheidt ons meteen van het buitenland: een integrale aanpak door publieke en private partijen. Ook in cyberspace gaan we samen polderen.

TWEE NIEUWE ORGANISATIES

Net als het Verenigd Koninkrijk krijgt Nederland twee nieuwe organisaties. Als eerste komt er een Cyber Security Raad, waarin vertegenwoordigers van publieke en private partijen de beveiligingsprioriteiten bepalen. Ten tweede komt er een Nationaal Cyber Security Centrum (NCSC). Het wordt een kennis- en expertisecentrum dat ondersteunt bij het aanpakken van incidenten. De dan opgeschaalde organisatie GOVCERT.NL gaat deel uitmaken van het centrum. Het NCSC treedt ook op bij digitale incidenten die de maatschappij kunnen ontwrichten. Dat doet het samen met cyberexperts van publieke en private organisaties. Of het NCSC ook diensten gaat bieden aan vitale sectoren zoals energiebedrijven en banken is nog onzeker. Misschien ligt daar wel een mooie taak voor marktpartijen die nauw samenwerken met het NCSC. Op dit moment monitort GOVCERT.NL al de netwerken van een aantal overheidsdeelnemers om incidenten in een vroeg stadium te ontdekken.

IMPULS HUIDIGE DIENSTEN

Verder beschrijft de strategie dat de AIVD, MIVD en Defensie hun eigen verantwoordelijkheden houden en zelfstandig zullen optreden. Hoe Defensie haar kennis beschikbaar kan stellen voor haar civiele taak, wordt nog onderzocht. Defensie krijgt in elk geval een eigen cybercentrum met daarin onder meer een Opleidings- en trainingscentrum (OTC). Net als de rest van de maatschappij is Defensie afhankelijk geworden van digitale systemen. Daarom wordt zelfs fors geïnvesteerd in offensieve capaciteiten om te voorkomen dat ons eigen leger niet kan optreden door digitale aanvallen. Daarnaast wordt het Programma Aanpak Cybercrime (PAC) versterkt. En het succesvolle Team High Tech Crime van de KLPD gaat uitbreiden naar zeventig mensen in 2014. Ze moeten minstens twintig zaken per jaar oplossen.

NEDERLANDSE AANPAK IS AFWIJKEND

Vergelijken we de Nederlandse cyberstrategie met die van onder ander de Verenigde Staten en het Verenigd Koninkrijk, dan vallen drie dingen op:

- De samenwerking tussen publieke en private partijen is een belangrijk onderdeel van onze strategie. Positief hieraan is dat de kennis en initiatieven van het bedrijfsleven niet verloren gaan. Een risico is dat de Nederlandse overheid geen duidelijke en sterke regie zal voeren. Terwijl het belang en de aard van de problematiek nadrukkelijk om die regie vraagt. Een ander risico is dat overleggen en compromissen een snelle besluitvorming bemoeilijken en onze slagkracht verminderen.
- Defensie en de inlichtingendiensten AIVD en MIVD blijven zelfstandig opereren. Vooral als het gaat om situational awareness werpt dit direct de cruciale vraag op hoe de organisaties voor structurele kennisdeling gaan zorgen. Immers, het Nationaal Cyber Security Centrum (OCSC) zal voor een goede dreigingsanalyse in grote mate van deze kennis afhankelijk zijn. Ook bestaat natuurlijk de kans dat mogelijke synergievoordelen niet worden benut.
- De concrete acties voor intensivering van de opsporing. Nu al is bekend dat succesvolle initiatieven voor bestrijding van cybercrime meer geld en menskracht krijgen. Dat is hoe dan ook een goede stap, want hoe strategisch we het probleem van cybersecurity ook benaderen, het succes hangt af van bevlogen professionals en hun initiatieven. Die geven we hiermee de ruimte en dat is een goede zaak.

CONCLUSIE: OVERHEID MOET KENNIS BUNDELEN

In onze analyse van de huidige Nederlandse situatie onderkenden we drie belangrijke aandachtspunten. Namelijk een gebrek aan structurele operationele slagkracht, regie en situational awareness. Het is nog geen uitgemaakte zaak dat de huidige cyberstrategie hier een adequaat antwoord op biedt. De crux is de rol van de overheid, zoals ook al blijkt uit de door haar gekozen titel voor deze strategie: 'Slagkracht door samenwerking'. Binnen de Nederlandse aanpak van cyberdreigingen blijven verantwoordelijkheden verspreid. Als de overheid er desondanks in slaagt kennis te bundelen, en leiding en richting te geven aan de verschillende initiatieven, dan kunnen we vol-doende slagkracht opbouwen. De nieuwe strategie is dan een goede eerste stap op weg naar een blijvend cyberveilig Nederland.

Ronald Prins, directeur Fox-IT


Ronald Prins

'Nederland moet alle zeilen bijzetten om aanvallen via internet de baas te blijven'

Op de website van Fox-IT kunt u de analyse van Fox-IT downloaden als pdf, inclusief een link naar de Nationale Cyber Security Strategie.
Reageren? Graag! Mail of bel naar Ronald Prins, prins@fox-it.com, @cryptoron, 015 - 284 79 99

MAATWERKTRAINING VOOR DE SIOD

‘Weten hoe je de onderste steen boven krijgt’

In het rechercheonderzoek van de Sociale Inlichtingen- en Opsporingsdienst (SIOD) vormen tegenwoordig niet de papieren ordners, maar de digitale opsporingsgegevens het drukpunt tijdens een verhoor. Om de juiste gegevens snel en veilig te kunnen blijven vinden, volgde het digitaal forensisch team van Jan Lutz een maatwerktraining voor onderzoek in een Microsoft-omgeving. ‘Als je niet regelmatig bijschoolt, beland je binnen twee jaar in een museum.’

De SIOD bestrijdt criminaliteit op het gebied van werk en inkomen, legt digitaal forensisch expert Lutz uit. ‘We jagen vooral op bedrijven die zich schuldig maken aan fraude, uitbuiting en mensenhandel. Mijn hoofdtaak is niet zozeer het vinden van sporen, maar het detecteren van bruikbare informatie. Als je bij grote ondernemingen en industrieën binnenvalt, ben je niet binnen een uurtje met een paar megabytes aan data klaar met een onderzoek. We zien al snel terabytes aan bestanden. En vind daar maar eens de juiste informatie in.’

FORENSISCHE PRAKTIJK

Het digitaal forensisch team van Lutz bezit de gouden combinatie van inzicht in computernetwerken en kennis van welke drukpunten een rechercheur nodig heeft in zijn verhoor. Om hun onderzoekskennis op hoog niveau te houden, volgden de zeven mannen van het team de maatwerktraining ‘digitaal forensisch onderzoek in een Microsoft-omgeving’ bij Fox-IT. Een feest der herkenning, vond Lutz. ‘Vier dagen met elkaar de diepte in; wij én de experts van Fox-IT. Geen uitgebreide verhalen over overbodige applicatiekennis – wat meestal zo’n negentig procent van basistrainingen vormt – maar juist de focus op die tien procent waar de gaten zitten. We hebben geleerd waar we informatie kunnen vinden en hoe we die er veilig uit kunnen halen.’

GEEN BRAVE ACCOUNTANTS

De experts van Fox-IT kenden volgens Lutz precies de weg die het SIOD-team nodig heeft om waardevolle informatie boven tafel te krijgen. ‘Ze weten hoe een systeem werkt en hoe je de onderste steen boven krijgt. Dat is voor ons essentieel. Wij hebben niets aan brave accountants die de regels kennen. Die zien de fraude namelijk niet en weten niet waar ze moeten zoeken.’ Lutz vond het extra leuk dat de trainers van Fox-IT ook genoten van de maatwerktraining: ‘Wij vertelden over onze praktijk, zij dachten direct mee vanuit hun expertise. Dat resulteerde in vier dagen op hoog niveau met elkaar sparren over oplossingen in de forensische praktijk.’

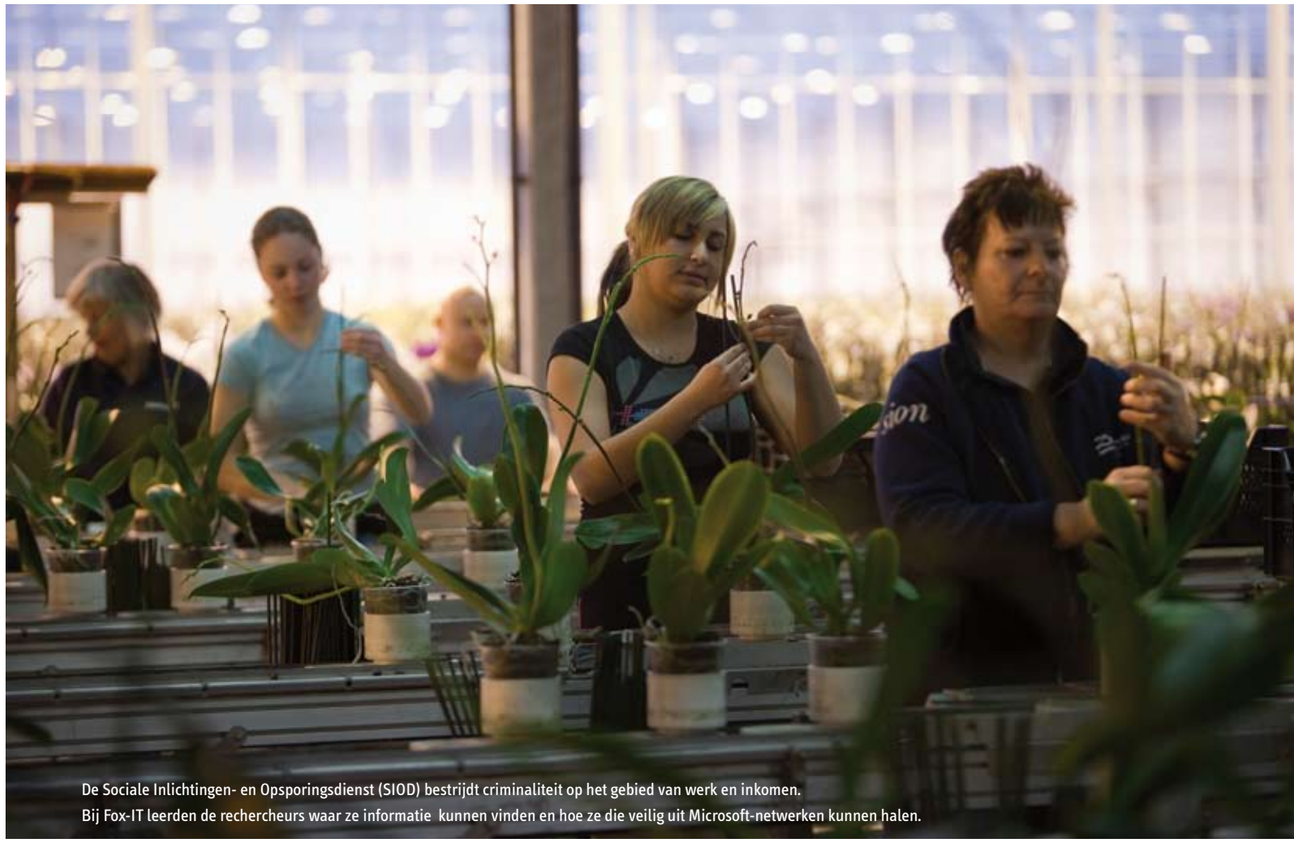
> ‘Vier dagen op hoog niveau met elkaar sparren over oplossingen in de forensische praktijk’

TECHNISCHE TIPS

Lutz en zijn team leerden ESX-technieken voor het emuleren van besturingssystemen, technieken om hot clones te produceren en SQL om selecties binnen records van databases veilig te stellen. ‘Het zijn voor ons handige en bruikbare technieken, zodat we niet elke terabyte hoeven mee te nemen, maar precies weten welke tweehonderd gigabyte we wél willen inpakken. Daarnaast kregen we in de training – juist door zo intensief samen te werken - veel praktische tips die soms prachtige eye-openers zijn. Een voorbeeld? In Microsoft Exchange 2003 moet je van tevoren bepaalde services uitzetten om EDB-bestanden te kunnen overnemen. Zet je die services niet uit, dan lukt het deels met bestaande tooling maar treedt toch dataverlies op. Dat moet je maar net weten.’

HANDS-ON-HACKING

Terwijl het forensisch team van de SIOD inmiddels de nieuwe kennis voorzichtig toepast in de praktijk – het kan zich niet veroorloven ‘zomaar’ gegevens kwijt te raken – zit de volgende maatwerktraining van Fox-IT alweer in de pijplijn: Hands-on-Hacking. Lutz heeft er zin in: ‘We willen nu eenmaal graag weten waar de kwetsbaarheden in systemen zitten. Als je weet met welke handelingen je gegevens uit Windows naar voren kunt toveren, kun je dat misschien ook binnen andere systemen, zoals Novell en Linux. En dat is uiteindelijk waarnaar we op zoek zijn: waardevolle gegevens die als bewijsvoering kunnen dienen in het primaire rechercheproces van de SIOD.’ ■



De Sociale Inlichtingen- en Opsporingsdienst (SIOD) bestrijdt criminaliteit op het gebied van werk en inkomen.
Bij Fox-IT leerden de rechercheurs waar ze informatie kunnen vinden en hoe ze die veilig uit Microsoft-netwerken kunnen halen.

Meer weten over maatwerktrainingen?
Neem contact op met de afdeling Trainingen, 015 - 284 79 08

TRIAGETOOLS EN DATADIODE IN CRIMINALITEITSBESTRIJDING

Fox-IT en de SIOD kennen elkaar ook buiten de trainingen. Zo zoeken de partijen samen naar digitale triagetools: tools die ervoor zorgen dat je niet meer alle computers hoeft mee te nemen, maar precies diegene waar het om gaat. Ook op het gebied van hardware is de SIOD geïnteresseerd in door Fox-IT ontwikkelde toepassingen, zoals de datadiode, die het hoogst haalbare veiligheidspredicaat heeft gekregen. Met de diode kan informatie veilig een en dezelfde kant op stromen binnen het SIOD-onderzoekssysteem. Informatie is tegenwoordig de ruggengraat van de organisatie en niemand wil dat deze op straat komt te liggen.

‘Doe altijd aangifte’

OFFICIER VAN JUSTITIE LODEWIJK VAN ZWIETEN OVER HET TOPSEGMENT VAN CYBERCRIME

INTERVIEW

‘Criminaliteit waarbij informatie- en communicatietechnologie (ICT) een doorslaggevende rol speelt’. Dat is de definitie van cybercrime waar Lodewijk van Zwieten mee werkt. De Landelijke Officier van Justitie voor Cybercrime hanteert daarbij een extra onderscheid: ‘In de ruime zin van het woord gaat het om ‘oude criminaliteit’ via nieuwe middelen. In enge zin is ICT niet alleen middel, maar ook doel. Denk aan hacken: crimineel gedrag gericht op of tegen ICT-middelen.’

Bij het Landelijk Parket van het Openbaar Ministerie (OM) werkt Van Zwieten in wat hij ‘het topsegment’ noemt: ‘Zware, georganiseerde cybercrime, ofwel high tech crime.’ De Officier leidt opsporingsonderzoeken bij de Nationale Recherche en bepaalt welke zaken zijn team aanpakt. ‘Dit laatste coördineer ik ook landelijk: hoe zorgen we dat we op dezelfde manier keuzes maken voor bepaalde zaken? En ik adviseer het OM over het voorkomen en aanpakken van cybercrime.’

BASALE RISICO’S

De meest voorkomende risico’s zijn heel basaal. ‘Jan met de Pet heeft misschien zijn virusscanner niet bijgewerkt of zijn firewall niet aan gezet.’ Maar Van Zwieten waarschuwt consumenten ook voor een ander type gevaar: ‘Niet iedereen realiseert zich dat Twitter, Hyves en Facebook niet alleen door vrienden worden gelezen, maar ook door mensen die actief zoeken naar berichten over vakanties en dergelijke om daar identiteitsfraude mee te plegen of je huis leeg te halen als je er niet bent. Daarnaast kan persoonlijke informatie die je op sites achterlaat een eigen leven gaan leiden. Veel internetdiensten houden bovendien gegevens bij van jouw internetgebruik.’

‘Stelregel in cybercrime is dat de eindgebruiker de zwakste schakel is’

BESTAANSRECHT

Voor bedrijven is één van de risico’s imagoschade: mensen gaan er met de goede naam vandoor. ‘Ondernemingen zijn daarnaast steeds vaker van internet afhankelijk voor elektronisch betalingsverkeer. Natuurlijk wil je als bedrijf deze voorzieningen bieden omdat klanten die willen, maar als je online betalen eenvoudig en breed toegankelijk maakt, dan kun je bijna automatisch niet voor optimale veiligheid kiezen.’ Die afweging heeft tot gevolg dat ondernemers

CYBERCRIME SYMPOSIUM 2011

Officier van Justitie Lodewijk van Zwieten sprak op 8 februari op het Cybercrime Symposium 2011, georganiseerd door Fox-IT. Tijdens dit symposium wierp hij, met verschillende sprekers en samen met bezoekers, een blik in de toekomst hoe cybercrime zich ontwikkelt. Aan de hand van onder meer technische tracks en prikkelende sprekers konden aanwezigen op een effectieve manier de gevaren van cybercrime leren (h)erkennen. Ook kregen zij tips en trucs over hoe zich tegen cybercrime te wapenen. Meer informatie over het symposium vindt u op **http://bit.ly/foxcc**.

een deel van de verantwoordelijkheid voor goede beveiliging bij de klant leggen. 'En stelregel in cybercrime is dat de eindgebruiker de zwakste schakel is.' Daarnaast zijn er verschillende niveaus waarop je beveiliging lekken kan vertonen. 'Ook het hostingbedrijf waar je webshop draait, moet zijn zaakjes op orde hebben. En wat te denken van afspraken met je bank en met je sitebouwer? Vanuit het oogpunt van security zijn dit allemaal risico's.' Als je serieus bent en internetverkoop je nering is, adviseert Van Zwieten bovendien om de beveiliging van je systemen periodiek te laten testen. "Dat is niet goedkoop, maar het gaat om je bestaansrecht."

'Bescherming van de openbare orde is online hetzelfde als in het fysieke domein'

SAMENWERKING OVER DE GRENS

'Digitale criminaliteit kun je niet zien. En als je het ontdekt, is het vaak al te laat: geld of gegevens zijn weg, net als sporen naar de dader', legt Van Zwieten uit. 'Een cybercrimineel die zich in het topsegment beweegt en een beetje zijn best doet, is niet eenvoudig op te sporen en te pakken.
Eén van de problemen hierbij is dat de bevoegdheid van de Nederlandse politie bij de grens ophoudt. En voor het plegen van een misdrijf in ons land hoeft de crimineel ook niet eens in Nederland te zijn geweest. Maar gelukkig gebeurt samenwerking over de grens steeds meer en steeds beter. Net als overigens de samenwerking met bedrijven en organisaties in publiekprivate vorm.'

DOE ALTIJD AANGIFTE

Het OM heeft behoefte aan veel meer informatie. Van Zwieten benadrukt het belang van aangifte doen, ook door bedrijven. Voor vitale sectoren en infrastructuren moet er misschien zelfs een speciale meldingsplicht komen, pleit de Officier.
'Nu doen bedrijven vaak geen aangifte uit angst voor imagoschade, of de ondernemer is bang dat klanten niet langer elektronisch zaken willen doen. Maar die angsten zijn ongegrond. Het delen van informatie over incidenten is uiteindelijk beter voor de business. En vanuit opsporingsperspectief biedt een aangifte waardevolle informatie over de aard, vorm en omvang van de criminaliteit.'

ZELFREDZAAMHEID

Onze economische belangen zijn direct gediend wanneer bedrijven zelf een aanval kunnen stoppen. Van Zwieten 'We moeten organisaties dus niet belemmeren in hun pogingen om cybercriminaliteit tegen te gaan of er rekening mee te houden. Maar als bedrijf moet je ook weer niet zwichten voor criminelen die data in gijzeling houden, of voor een denial-of-serviceaanval, of zelfs maar verliezen ten gevolge van cybercrime incalculeren. Dan sla je door. Bovendien schrik je een crimineel niet af en wordt de kans juist groter dat die nog eens toeslaat.'

ROL VAN DE OVERHEID

De overheid heeft in eerste instantie de taak om cybercriminaliteit op te sporen en daders te vervolgen. Daarnaast is voorlichting belangrijk: wat kunnen burgers en ondernemingen zelf doen om de risico's te beperken. Van Zwieten: 'Digitale beveiliging laten we in principe aan de markt over. De overheid schept wel kaders waarbinnen die markt kan werken: beperkend in de vorm van voorschriften, maar ook door marktpartijen gelijke kansen te bieden.
Bescherming van de openbare of rechtsorde is online hetzelfde als in het normale, fysieke domein: doe je auto op slot, doe je deur op het nachtslot.' ■

Fox DetACT for Online Banking **dringt fraude internetbankieren terug**

Cybercriminelen frauderen met banktransacties op het Internet. Nederlandse banken gebruiken sinds kort een systeem waarmee frauduleuze online transacties tijdig worden gedetecteerd en tegengehouden. Dit systeem - Fox DetACT for Online Banking - draagt in belangrijke mate bij aan het vertrouwen van consumenten in online bankieren en de filosofie van Care Free Banking.

Wil je pinnen, blijkt je rekening geplunderd... Fox-IT monitort dagelijks miljoenen transacties waardoor banken fraude voor kunnen zijn en consumenten blijven vertrouwen in elektronisch bankieren.

Internetbankieren is van alledag en niet meer weg te denken. Maar is het ook veilig? Consumenten denken van wel. Met versleutelde https-verbindingen, tan-codes, tokens en andere maatregelen beveiligen banken hun online bankverkeer. Cybercriminelen hebben hun methoden echter aangepast en omzeilen deze maatregelen. Met phishing en malware richten zij zich op de nietsvermoedende consument, wiens pc, laptop, iPad of smartphone maar moeilijk is te beveiligen.

COMMUNICATIE MONITOREN

Voor het beveiligingsprobleem bij internetbankieren heeft Fox-IT een oplossing: Fox DetACT for Online Banking (Detection of Active Cyber Threats). Deze oplossing heeft bij een aantal Nederlandse banken haar kracht al bewezen. DetACT-OB monitort het transactieverkeer tussen de bank en de consument. Dat gebeurt in de websystemen van de bank. Precies dáár, waar de informatie van de versleutelde verbindingen met de consument binnenkomt, volgt DetACT-OB

Care Free Banking is cruciaal voor het succes van de online strategie van banken

TRANSACTIEINFORMATIE VERSNIPPERD

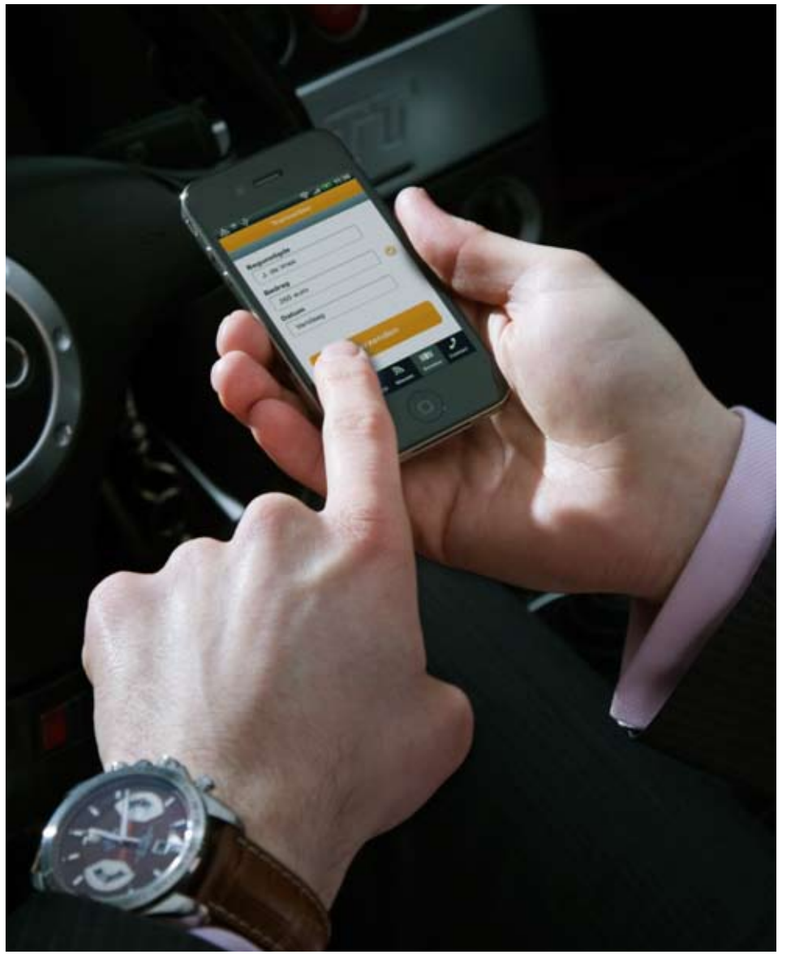
Online banking kan nog beter worden beveiligd tegen cybercriminaliteit. Niet aan de zijde van het onder vuur liggende en onvertrouwde platform van de consument, maar in het domein waarover de bank wél controle heeft, haar eigen infrastructuur. Vooral uit de TCP/IP-communicatie is veel bruikbare informatie te halen over de computer van de gebruiker, zoals zijn IP-adres of schermresolutie. Minder bruikbaar is de 'uitgeklede' informatie die de backoffices van de banken gebruiken. Daar staan de gegevens bovendien verspreid over veel verschillende systemen, applicaties en databases, van verschillende afdelingen, met verschillende eigenaren. Dan wordt het bijna onmogelijk om snel informatie te verzamelen, te analyseren en te reageren. En juist die snelheid is essentieel; in het huidige betalingsverkeer - ook internationaal - is binnen enkele minuten geld op te nemen, via bijvoorbeeld een pinautomaat, en daardoor niet meer terug te boeken.

COMMUNICATIE ANALYSEREN EN DETECTEREN

Bij online banking bevat de TCP/IP-communicatie een schat aan gegevens. Daarom tapt DetACT-OB juist die data af en analyseert die realtime. DetACT-OB zoekt op basis van tientallen kenmerken naar afwijkingen die (kunnen) duiden op fraude. Dat kunnen allerlei kenmerken zijn. Denk aan veranderingen in besturingssysteem, schermresolutie, browser of IP-adres. Ook de handelingssnelheid kan verraden of een mens van vlees en bloed bezig is, of een geautomatiseerd 'bot' of virus. DetACT-OB houdt elke afwijking tegen het licht en geeft direct een signaal wanneer het een transactie als 'frauduleus' bestempelt.

CASE STUDY: PHISHINGAANVAL AFGESLAGEN

Een Nederlandse bank kreeg in mei 2010 te maken met phishing-aanvallen. Fraudeurs lokten klanten via e-mailwaarschuwingen naar nepsites en belden ze op om inloggegevens te ontfutselen. Met de gegevens plunderden ze de rekeningen en het geld sluisden de fraudeurs weg naar money mules. De bank vroeg aan Fox-IT om DetACT-OB in te zetten. Direct al detecteerde het systeen een groot aantal malafide transacties. Het totaalbedrag van de geblokkeerde overboekingen was in de eerste week al hoger dan de kosten voor een volledig jaar Fox DetACT-OB. Ontmoedigd door het gebrek aan succes gaven de cybercriminelen uiteindelijk de aanvallen op en verlegden hun aandacht naar andere instellingen.



ANALYSE: MODUS OPERANDI EN VERGAARDE INTERNET INTELLIGENCE

Kern van DetACT-OB is een goede analyse van de rijke communicatiedata tussen de consumenten en de banksystemen.
Die analyse gebeurt op drie manieren:

1. **Op basis van bekende modus operandi**
   Hierbij gebruikt het systeem kennis over bekende online bankfraudescenario's. Loopt de communicatie altijd via een bepaald land of dezelfde bank? En wat is de gebruikelijke combinatie van IP-adres en User Agent, wat is de gebruikelijke schermresolutie? Dergelijke kenmerken vormen het DNA van fraudescenario's.
2. **Op basis van intelligence-onderzoek**
   Fox-IT infiltreert in de digitale onderwereld om te weten wat er speelt. Signalen voor dreigende frauduleuze acties kunnen bijvoorbeeld komen uit code van malware: hoe is die geschreven en welke kenmerken zitten daarin die eventueel te detecteren zijn in de online banktransacties?
3. **Op basis van slimme, lerende ICT**
   DetACT-OB detecteert opvallend gedrag op basis van dynamisch opgebouwde profielen. Het systeem leert met de tijd wat 'gewoon' gedrag is en zoekt op basis daarvan afwijkingen die kunnen wijzen op fraude.
   Deze analysetechniek is volop in ontwikkeling, maar heeft al interessante resultaten laten zien.

SNEL REAGEREN IS CRUCIAAL

Voor enkele Nederlandse grootbanken scant, analyseert en detecteert Fox-IT met DetACT-OB miljoenen banktransacties per dag. Met elke bank heeft de beveiligingsspecialist afspraken gemaakt over de wijze en snelheid waarop wordt gereageerd wanneer

Snelle reactie is noodzakelijk om criminelen te pakken

DetACT-OB mogelijk frauduleuze transacties detecteert. Snelle reactie is noodzakelijk om criminelen te pakken. DetACT-OB voorziet daarom bijvoorbeeld in geautomatiseerde interfacing met banksystemen. Hierdoor kan het systeem direct een overboeking blokkeren of in quarantaine plaatsen. De praktijk heeft geleerd dat dit de terugverdientijd van de cybercriminelen zo aantast, dat ze een ander doelwit kiezen.

CONSUMENT BEHOUDT VERTROUWEN

Met DetACT-OB heeft Fox-IT een unieke dienst in huis, die banken in staat stelt om haar klanten veilig online te laten bankieren, zonder ze te belasten met extra beveiligingsmaatregelen. Dit dringt niet alleen de online bankfraude terug, maar houdt tegelijk het consumentenvertrouwen in online banking overeind. En dat - Care Free Banking - is cruciaal voor het succes van de online strategie van banken. ■

Meer informatie: Jeroen Herlaar,
Fox-IT business unit manager Cybercrime
t: 015-284 79 99, e: herlaar@fox-it.com

ACTUEEL

Samenwerking met MatrikonOPC

Waterdichte beveiliging

Fox-IT en MatrikonOPC hebben de handen ineengeslagen. MatrikonOPC is wereldwijd een belangrijke speler in de industriële automatisering. Door de samenwerking bewijst de Fox DataDiode zijn diensten ook in industriële omgevingen.

Onze samenleving raakt ernstig ontregeld wanneer een virus of hack bijvoorbeeld de ICT van een waterzuiveringsinstallatie ontregelt. Beveiliging van industriële processen is dus essentieel.

Olieraffinaderijen, waterzuiveringsinstallaties en openbaar vervoerbedrijven zijn van vitaal belang voor de samenleving. De processen die deze bedrijven draaiende houden, moeten continu doorgaan en uiteraard goed zijn beveiligd. Een goed voorbeeld is de brand in november 2010 bij een verkeersleidingpost van ProRail in Utrecht, waardoor het treinverkeer in Nederland grotendeels lam kwam te liggen. Dit was een ongeluk, maar wat als hackers of een virus doelbewust essentiële bedrijfsprocessen verstoren?

FYSIEK SCHEIDEN VAN NETWERKEN

Een firewall om cyberaanvallen af te weren is onvoldoende. Een meer rigoureuze oplossing is noodzakelijk: het fysiek scheiden van de vitale proces- en controlenetwerken van andere bedrijfsnetwerken zoals intra- en internet. Maar deze scheiding van netwerken levert ook problemen op. Want voor een optimale bedrijfsvoering moet informatie worden uitgewisseld tussen de beide netwerken. Denk aan productieoverzichten, just-in-time leveringen of realtime facturering.

AIR GAP IS OMSLACHTIG

De fysieke scheiding, de zogenoemde air gap, wordt meestal overbrugd doordat iemand met een usb-stick of cd de benodigde informatie van het proces- en controlenetwerk overbrengt naar het andere bedrijfsnetwerk. Dat is omslachtig en tijdrovend. Bovendien is het ook niet eens honderd procent veilig, want een usb-stick kan ook geïnfecteerd zijn met een worm als Stuxnet.

FOX DATADIODE: EENRICHTINGSVERKEER

Een praktische oplossing voor dit probleem biedt de Fox DataDiode. De Fox DataDiode wordt tussen een vitaal proces- of controlenetwerk en een ander netwerk geplaatst. De diode zorgt dat informatie maar één kant op kan: informatie uit het vitale netwerk kan bijvoorbeeld wel naar het bedrijfsnetwerk gaan, maar de weg andersom is afgesloten. Dat is fysiek onmogelijk gemaakt. Hackers, virussen en wormen kunnen zo onmogelijk de vitale netwerken bereiken en aantasten.

GROTERE TOEPASSINGSMOGELIJKHEDEN

Veiligheidsdiensten, het leger, politie en andere overheidsinstanties met geheime informatie passen de Fox DataDiode al met succes toe. Fox-IT ziet voor het product ook in andere maatschappelijke sectoren toepassingsmogelijkheden, vooral in de industriële sector waar continuïteit van de bedrijfsprocessen voorop staat. Daarvoor is wel een speciale manier nodig om de Fox DataDiode te laten communiceren met de specifieke software en apparatuur in de proces- en controleomgevingen van industrieën.

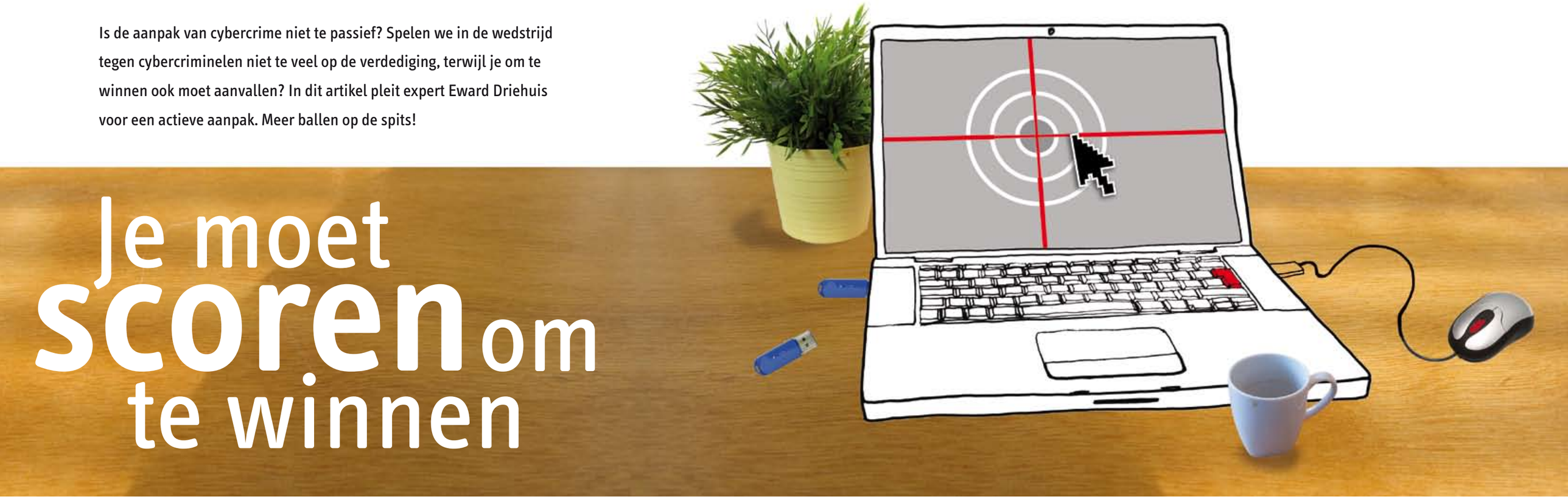
AANSLUITING BIJ OPC PROTOCOL

De samenwerking tussen Fox-IT en MatrikonOPC maakt dit mogelijk. MatrikonOPC heeft een uitstekende staat van dienst in de industrie, de transport- en de energiesector. De oplossingen van het Canadese bedrijf maken gebruik van het softwareprotocol OPC, de standaard in deze industrieën. De software van MatrikonOPC sluit niet alleen perfect aan op de wensen van Fox-IT, hij ondersteunt bovendien een enorme diversiteit aan proces- en controlesystemen. En dat maakt het inpassen van de Fox DataDiode in industriële systemen een stuk eenvoudiger. ■

OVER MATRIKONOPC

Matrikon, met het hoofdkantoor in het Canadese Edmonton en sinds 2010 onderdeel van Honeywell, is gespecialiseerd in technologie voor productiebeheer, optimalisatie van operationele processen en assetbewaking op industriële locaties in de sectoren olie en gas, chemie, energie en raffinage. Het bedrijfsonderdeel MatrikonOPC richt zich op 'open connectivity' in proces control, gebaseerd op de OPC standaard. Met kantoren in Noord-Amerika, Europa, Azië-Pacific en het Midden-Oosten biedt MatrikonOPC lokale aanwezigheid op een wereldwijde schaal.
Meer informatie op ww.matrikonopc.com

Is de aanpak van cybercrime niet te passief? Spelen we in de wedstrijd tegen cybercriminelen niet te veel op de verdediging, terwijl je om te winnen ook moet aanvallen? In dit artikel pleit expert Eward Driehuis voor een actieve aanpak. Meer ballen op de spits!



Je moet **scoren** om te winnen

Cybercriminaliteit is er in alle soorten en maten en komt steeds vaker voor. In de eerste helft van 2010 stonden vijfhonderd mensen verbouwereerd voor het PIN-apparaat. Het scherm vertelde dat hun 'saldo ontoereikend' was, terwijl eerder op de dag pinnen voor een nieuwe aankoop geen enkel probleem was. Pas na paniekerige telefoontjes kwamen deze mensen erachter dat ze slachtoffer waren van cybercriminaliteit. Later in het jaar zagen we de stijgende populariteit van de DDoS-aanval. Links en rechts werden bedrijven en overheden geconfronteerd met massale 'aanvallen' op publieke servers. Deze aanvallen bestaan uit normaal internetverkeer, maar dan in een grote hoeveelheid en tegelijkertijd. Daar zijn veel servers, internetlijnen en firewalls niet tegen bestand; ze gaan plat.

DIGILANTES

DDoS-aanvallen die recentelijk het nieuws haalden, waren die van digilantes, digitale vigilantes (een vigilante is iemand die het systeem negeert en het recht in eigen hand neemt), die sympathiseerden met Wikileaks-voorman Julian Assange. Deze digilantes richtten zich in gecoördineerde acties op organisaties die volgens hen Wikileaks tegenwerkten. Mastercard, Visa en PayPal gingen plat, maar ook ons eigen Openbaar Ministerie werd het slachtoffer. Zonder het zelf te weten, hebben veel mensen meegewerkt aan dergelijke DDoS-aanvallen. Door gebrekkige beveiliging waren hun computers geïnfecteerd en onderdeel van een botnet. Schimmige personen, soms duizenden kilometers ver weg, zetten heimelijk andermans computer naar hun hand. Dergelijke botnets bieden criminelen veel mogelijkheden: identiteitsdiefstal, spammen, bankrekeningen plunderen, informatie stelen, gegevens gijzelen. En vooral: veel geld verdienen.

> 'Wij zijn team blauw, zij zijn team rood. Eén van ons gaat winnen, en zij mogen het niet zijn'

VERDEDIGING WORDT RATRACE

Wie wordt aangevallen, schiet in de verdediging. Dat was ook precies de eerste reactie op cyberaanvallen. Extra firewalls, IDS'en, anti DDoS-machines, end-point security abonnementen... we kochten ze per kilo. Miljoenen rekenden we af en we leunden tevreden achterover om naar ons gloednieuwe dashboard te kijken.

Maar het duurde niet lang of er verschenen rode lampjes. De cybercriminelen hadden niet stil gezeten. Beter en professioneler georganiseerd gingen ze verder. Ze hadden tijd, geld, mankracht en teststraten om hun nieuwe aanvallen te testen. Onze firewalls, IDS'en en virusscanners bleken zij ook te hebben. En daar konden ze mooi hun criminele programma's op testen. Een ratrace ontstond. Nieuwe aanvallen, nieuwe verdedigingen, nieuwe problemen en nieuwe kosten.

ALLEEN KEEPERS

We zijn vooral aan het verdedigen. Kennelijk ervaren we het als normaal om ons aan te passen aan ongewenst, asociaal of crimineel gedrag. We stellen een team van alleen keepers op tegen een team van spitsen. Hoe dat afloopt, laat zich raden. In de sport moet de verdediging honderd procent van de tijd pieken, terwijl de aanvaller maar één geniaal moment nodig heeft.

We kunnen ons goal volstapelen met keepers, maar iemand vindt altijd een manier om de bal er in te friemelen. Gelukkig zijn er mensen die anders naar cybercriminaliteit kijken. Mensen die een puur verdedigende instelling wel als een probleem zien en die de uitdaging willen aangaan. Bijvoorbeeld Lodewijk van Zwieten van het Openbaar Ministerie heeft gezegd dat we moeten nadenken over terugslaan. Hij heeft de daad bij het woord gevoegd door twee digilantes te verrassen met een bezoek. Ook rolde hij met de High Tech Crime unit van de politie een groot botnet, Bredolab, op.

TACTIEK VERANDEREN

De uitdaging is erachter zien te komen hoe cybercriminelen de bal in het doel willen krijgen. Daarvoor moeten we ze bestuderen. Hun tools onder de loep nemen. Hun communicatie bekijken. Als we weten wat ze volgende maand gaan doen, worden we er niet meer door verrast. We bouwen onze tactiek om hun acties heen. Ken je tegenstander.
We moeten het spel dus op een andere manier gaan spelen. Wij zijn team blauw, zij zijn team rood. Eén van ons gaat winnen, en zij mogen het niet zijn. Wij moeten de bal erin schieten. Over de middenlijn stappen, waar hun verdediging op ons wacht.
Er omheen, één-tweetjes, tactiek toepassen die we eerder hebben ontwikkeld. Want als je het spel wilt spelen, moet je aanvallen, anders rest als enige optie verliezen. ■

Eward Driehuis werkt bij de Business Unit Cybercrime
Reageren op zijn mening? Graag!
06-43 82 45 29 of
driehuis@fox-it.com

E-DISCOVERY

Wie wist wanneer wat?

Veranderende omstandigheden vereisen slimmere onderzoekstechnieken. Corporate securities, advocatenkantoren, bedrijfsjuristen, overheden of interne onderzoeksafdelingen: ze hebben allemaal te maken met steeds groter wordende hoeveelheden informatie die ze in korte tijd moeten doorzoeken. Met een beperkt budget en weinig resources, maar wel snel en zorgvuldig. Tegenwoordig kunt u dergelijke E-Discovery zelf doen.

E-Discovery - digitaal onderzoek - begint vaak met het controleren van harde schijven en mailboxen. Het is van belang dat men documenten en informatieverzamelingen snel en secuur kan veiligstellen, dat men door een snelle analyse direct inzicht krijgt in een onderzoek en dat een review op alleen de relevante documenten gedaan wordt. Doorgaans zijn voor zo'n onderzoek IT- en forensisch experts nodig en high end apparatuur. Sinds kort kan - spreekwoordelijk - een kind de was doen. Dankzij een samenwerking tussen Fox-IT en Clearwell, aanbieder van 's werelds meest geavanceerde E-Discovery software.

DOORZOEK NU ZELF ALLE DATA

Met de software van Clearwell Systems zijn complete forensische onderzoeken te doen en kunnen organisaties nu ook zelf grote hoeveelheden data snel doorzoeken.
De te onderzoeken data wordt desgewenst door Fox-IT veiliggesteld en ingeladen in Clearwell. Via een beveiligde verbinding kunt u als jurist, bedrijfsrechercheur of veiligheidsmedewerker zelf onderzoek uitvoeren op de data. Via de gemakkelijke interface is het zoeken naar personen, e-mails, bijlagen en andere documenten eenvoudig. U ziet direct verbanden en betrokkenen bij bepaalde conversaties. Hierdoor kunt u snel en efficiënt de belangrijkste informatie verzamelen en uw onderzoek afronden.
'Met Clearwell krijgt de gebruiker de beschikking over zeer geavanceerde zoektechnologie die zich in de praktijk bewezen heeft', aldus Hans Henseler, managing partner van Fox-IT Forensics en lector E-Discovery aan de Hogeschool van Amsterdam.

Juristen, bedrijfsrechercheurs of veiligheidsmedewerkers kunnen zelf onderzoek uitvoeren op data

VOORDELEN

Enkele voordelen van deze E-Discovery oplossing zijn:

- Inzicht en overzicht in een onderzoek binnen uren in plaats van weken;
- Versnelde verwerking van documenten, zodat gebruikers direct inzicht krijgen in de feiten van de zaak. Dit levert een tijdsbesparing tot 80% op;
- Het zoeken binnen het E-Discovery proces wordt transparant. Resultaat: een verdedigbaar E-Discovery proces;
- Interactieve analyse van de data. Resultaat: kleinere datasets met alleen relevante informatie;
- Het realtime volgen van de voortgang van het onderzoek, met complete rapportages.

AL BEWEZEN KRACHT

De samenwerking tussen Fox-IT en Clearwell Systems heeft zich al verschillende keren bewezen. Onder andere bij het advocatenkantoor Wijn & Stael en verzekeraar Unive (zie kaders). De toepassingsmogelijkheden en -markten zijn zeer breed. Bent u geïnteresseerd in de mogelijkheden van Clearwell neem dan contact op met Steffen Moorrees (moorrees@fox-it.com) senior onderzoeker bij Fox-IT Forensics. ■

WIJN & STAEL ADVOCATEN: FAILLISSEMENTSONDERZOEK

Tijdens een faillissementsonderzoek schakelde Wijn & Stael advocaten Fox-IT in om via Clearwell een grote hoeveelheid e-mailboxen te doorzoeken. Het doel was om duidelijk te krijgen wie, wanneer, welke beslissing nam, gebaseerd op haar of hem bekende feiten. Advocate Joyce Snijder: 'Over het algemeen lopen advocaten niet voorop als het gaat om IT-ontwikkelingen. Maar wij hebben gezien dat door het inzetten van techniek bij grote hoeveelheden informatie het onderzoek grondig en snel uitgevoerd kan worden. Het is bijna een onmogelijke opgave om met traditionele hulpmiddelen alle e-mail en attachments doorzoekbaar te maken, duplicaten eruit te halen en e-mailconversaties te groeperen op een tijdslijn.'
Omdat na de initiële zoekslag de documenten stuk voor stuk bekeken kunnen worden, is het van belang dat deze hoeveelheid informatie zo klein mogelijk is. Clearwell biedt veel verschillende mogelijkheden om alleen de relevante documenten over te houden. "Hierdoor konden we het onderzoek sneller uitvoeren", vertelt Snijder. 'Bij een eventueel volgend onderzoek zouden we Clearwell breder willen inzetten om zo automatisch een dossier van de zaak op te bouwen.'

AFDELING VEILIGHEIDSZAKEN VAN UNIVÉ VOERT INTERNE ONDERZOEKEN SNELLER UIT

Tijdens een onderzoek waarbij elektronische informatie verwerkt, geanalyseerd en doorzocht moest worden, maakte Bureau Interne Zaken van Univé gebruik van Clearwell. '
De door Fox-IT geleverde ondersteuning en E-Discovery oplossing waren zeer professioneel. Univé overweegt bij toekomstige onderzoeken hier vaker gebruik van te maken, met naar verwachting een nog sneller en keurig gedocumenteerd onderzoeksresultaat.', aldus Paul Engelsman, teammanager Bureau Interne Zaken. Behalve de tijdswinst en bijkomende kostenbesparing bracht het de verzekeraar de volgende voordelen:

- Op basis van voortschrijdend inzicht direct, realtime, zoekvragen aanpassen en verfijnen;
- Overzichtelijke tijdslijnen creëren met alleen de relevante informatie;
- Zelf kunnen inschatten/bepalen welke documenten belangrijk zijn. Niet afhankelijk zijn van derden die de bedrijfscultuur en materie niet kennen;
- Het is een intuïtief programma. Het is beveiligd en van afstand online te benaderen;
- Duidelijke en overzichtelijke rapportages. Elk document krijgt een eigen ID en is eenvoudig te traceren.

Weetjes en nieuwtjes

Sneak Preview voor Fox Tracks Inspector

Fox-IT heeft op 17 februari de eerste betaversie van Fox Tracks Inspector (FTI) getoond aan tactische en digitaal rechercheurs van de politie en opsporingsdiensten. Dit gebeurde tijdens een exclusieve sneak preview. De nieuwe forensische tool analyseert binnen een paar minuten digitaal bewijsmateriaal, zoals inloggegevens, e-mails, documenten en internethistorie. FTI maakt een duidelijk overzicht van belangrijke informatie, waarmee u snel kunnen bepalen welk bewijsmateriaal u verder uitgebreid moet onderzoeken.
Versie 1.0 van FTI is in juni beschikbaar; dan start ook de eerste pilot. Naar verwachting is in oktober 2011 versie 2.0 klaar en volgen er meer pilots.

Meer weten of wilt u een demonstratie van de Fox Tracks Inspector?
Neem dan contact op met Product Manager FTI - Marco de Moulin via 015-284 79 99 of demoulin@fox-it.com.

MOBIKEY:

Overal veilig en flexibel werken

Ook voor wie met vertrouwelijke informatie omgaat, is Het Nieuwe Werken mogelijk. Dankzij MobiKEY. Met deze speciale usb-stick kunt u vanaf elke Windows-pc ter wereld werken alsof u werkt op uw eigen (bedrijfs)computer. Zo kunt u in een hotel, internetcafé of thuis bestanden openen, e-mailen en internetten, zonder uw laptop of pc mee te nemen. Zolang uw eigen bedrijfscomputer maar aanstaat. De MobiKEY maakt de beveiligde verbinding, werkt altijd en laat geen informatie achter op de computer die u gebruikt.
Meer weten over de MobiKEY? Neem contact op met productmanager, Ronald Westerlaken via 015-284 79 99 of westerlaken@fox-it.com.

Events

15 t/m 16 maart	e-Crime Congress 2011 - London
23 maart	AFCEA luncheon - Mons
5 april	Expert Meeting Clearwell - Amsterdam
19 t/m 21 april	InfoSecurity Europe 2011 - London
17 t/m 20 mei	Hack in the Box - Amsterdam
26 mei	TechNet Europe 2011 - Bratislava
14 t/m 16 juni	ISS World Europe - Praag

TRAININGSKALENDER

Datum	Training
24 t/m 25 maart	Rechercheren op het Internet
29 t/m 31 maart	Digitaal Forensisch Onderzoek - SQL
29 t/m 31 maart	IRN advanced training - besloten
4 t/m 7 april	Rechercheren op het Internet
4 t/m 15 april	Training International Law Enforcement
18 t/m 19 april	Rechercheren op het Internet - Basis
16 t/m 17 mei	IRN Basis training
18 t/m 20 mei	IRN Advanced training

Datum	Training
6 t/m 8 juni	FoxReplay Gebruikerstraining - Basis
9 t/m 10 juni	SSR – Maatwerktraining 1e sessie
23 t/m 24 juni	SSR - Maatwerktraining 2e sessie
27 t/m 30 juni	Digitaal Forensisch Onderzoek - Microsoft
27 t/m 30 september	Digitaal Forensisch Onderzoek - Microsoft
3 t/m 4 november	SSR – Maatwerktraining 1e sessie
17 t/m 18 november	SSR – Maatwerktraining 2e sessie

Meer informatie www.fox-it.com