FOX-IT

FOX files 2

FOX-IT.COM
SEPTEMBER 2011

MOBIELE PLATFORMS
Hoog gebruiksgemak, lage veiligheid

TRAINING OEKRAÏENSE VEILIGHEIDSDIENST
Wodka als wonderolie

DILEMMA: VRIJHEID VERSUS VEILIGHEID
De mening van Akerboom (NCTV) en Aerdts (BoF)

EXPERTISE CYBERCRIME

Succesvol Nederlands exportproduct

19

10

12

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
Hillcreek Pictures, Den Haag

Interviews en teksten
Sabel Communicatie, Den Haag

Met dank aan Hilton The Hague

Fox zoekt Foxers!

Economisch herstel of niet? De berichten zijn wisselend. In ieder geval gaat het met Fox-IT crescendo. We hebben natuurlijk best wat gemerkt van slinkende budgetten hier en daar, maar zijn de afgelopen jaren toch stevig doorgegroeid. We plukken duidelijk de vruchten van onze innovatiestrategie.

Op die gekozen weg willen we de komende jaren volop door. Samen met iedereen, die zijn eigen organisatie of de maatschappij in het algemeen weerbaarder wil maken tegen cyberdreigingen, gaan we graag op zoek naar technische, leading-edge innovatieve oplossingen. De mooiste vondsten, de innovatieve juweeltjes, willen we ook wereldwijd verkopen. Ons (korte) verleden toont aan, dat dit kan. Nu al worden producten van Fox over de hele wereld – van Japan tot de VS – ingezet om de maatschappij veiliger te maken. En dus kun je ons zo maar tegenkomen op een marineschip in India, zoals je verderop in dit magazine kunt lezen.

In onze innovatieve ambitie worden we geholpen doordat Nederland voorop loopt op het gebied van internet en cybercrime. Onze kennis op dit terrein is een exportproduct. In het artikel 'Made in Holland' gaan we in op een paar interessante recente 'Hollandsche' initiatieven. Dat soort initiatieven kunnen alleen maar bestaan dankzij mensen met bijzondere kwaliteiten. Op ons vakgebied zie je dat niet altijd af aan het CV. Met een knipoog hebben wij het weleens over het werven van digitale hangjongeren. Die kreet heeft inmiddels de nationale pers gehaald.

We groeien flink. We hebben die bijzondere mensen hard nodig. Ik hoop daarom dat jullie het me niet kwalijk nemen als ik dit directie intro ook nog een keer voor wat werving 'misbruik'...

CYBERCRIME - MONITORING - INTERNET - BOTNET - VULNERABILITIES - INTRUSION DETECTION - TCP/IP

Fox zoekt Foxers! Interesse? jobs.fox-it.com

Ton Wallast, directeur Fox-IT

ACTUEEL

Groeiende populariteit mobiele platforms vergroot veiligheidsrisico's

SMARTPHONE VERLOREN, GEHEIMEN OP STRAAT

Mobiele platforms zoals smartphones en tablets worden steeds populairder en dus interessanter voor cybercriminelen. Beveiliging is noodzakelijk maar mag het gebruiksgemak – dat mobiele platforms juist zo geliefd maakt – niet in de weg staan

‘Hoe veilig is open wifi bij Starbucks of een hotel?’

Blackberries, iPhones en andere smartphones zijn niet aan te slepen. En ook de populariteit van tablets, zoals de iPad, stijgt. Het gebruiksgemak van mobiele platforms is hoog en ze passen prima bij ‘Het Nieuwe Werken’. Alleen: hoe veilig zijn die platforms? ‘Cybercriminelen volgen het geld’, stelt Mark Koek, lead expert cybercrime bij Fox-IT. ‘Nu steeds meer mensen een smartphone hebben en meer bedrijven er apps voor maken, wordt het voor cybercriminelen interessanter om zich op mobiele platforms te richten. Wat het kwaadwillenden bovendien makkelijker maakt, is dat de meeste gebruikers zich niet bewust zijn van de veiligheidsrisico’s.’

KWAADWILLENDE APPS

‘Smartphones zijn eigenlijk computers die in je zak passen; ze hebben dezelfde veiligheidsrisico’s als computers’, stelt Koek. De besturingssystemen van smartphones kunnen net als die van computers lekken vertonen. Zoals bij een computer virussen via een onschuldig lijkende download binnen kunnen komen, zo kunnen ook goed uitziende apps met kwade bedoelingen zijn ontworpen. ‘Het kan gebeuren dat je een app installeert die ongewild je gesprekken afluistert.’

In vergelijking met computers hebben smartphones nog een ander risico. Koek: ‘Door hun formaat worden ze vaker vergeten en ze zijn makkelijker te stelen.’

> ‘Goed uitziende apps kunnen met kwade bedoelingen zijn ontworpen’

Een verloren of gestolen smartphone bevat een schat aan informatie. Koek: ‘Het is aan ons als beveiligers om gebruikers bewust te maken van de risico’s van mobiele platforms. Zo is het belangrijk dat mensen snel hun rekening blokkeren als ze hun smartphone kwijt zijn.’

MOBIEL BANKIEREN

Koek en zijn team deden op verzoek van een bank een audit van een iPhone-app voor online bankieren. Een bank wil voor zijn klanten natuurlijk een app die zo gebruiksvriendelijk mogelijk is, maar dat botst met beveiligingsaspecten. Wat bijvoorbeeld als mensen op een openbaar netwerk inloggen? Koek: ‘Met wie praat je? Als je bij Starbucks met je iPhone op een gratis netwerk inlogt, kan iemand zich voordoen als jouw bank en jouw gegevens stelen. Een zogenaamde man-in-the-middle aanval. De verificatie van de banksite moet dus op orde zijn.’

Bij de audit werd ook getest of de toegangscode voor bankverkeer op een ‘gevonden’ telefoon makkelijk te kraken was. ‘Dat is ons gelukt’, zegt Koek. ‘Je moet het dus zo lastig mogelijk maken om de informatie te vinden. Dat kan bijvoorbeeld door stukjes van het wachtwoord op verschillende plekken in het geheugen te zetten. Zo win je tijd, en dat geeft gebruikers de gelegenheid om contact op te nemen met hun bank.’

ALGORITME GEKRAAKT

Mobiele telefoons zijn sowieso een veiligheidsrisico. ‘Het algoritme dat gesprekken en sms-jes versleutelt, is al een paar jaar geleden gekraakt’, vertelt Ronald Westerlaken, productmanager veilige telefonie bij Fox-IT. Gesprekken zijn daardoor af te luisteren. Hoe veilig toekomstige voice over IP communicatie wordt van nieuwe generatie smartphones, valt te betwijfelen. ‘De eerste zwakheden in GPRS zijn ook al gevonden. Veilig ben je pas echt als het gesprek of tekstbericht tussen twee telefoons volledig en goed versleuteld is. Dat is nu zeker niet het geval.”

De meeste beveiligingsproducten voor het versleutelen van de gesprekken of sms’jes op mobiele platforms kunnen volgens Westerlaken de toets der kritiek niet weerstaan. De kwaliteit laat vaak te wensen over en vooral softwareoplossingen zijn kwetsbaar omdat software vaak makkelijker te kraken is dan hardware. ‘Bovendien werken vele oplossingen niet met een open standaard. Dat maakt het moeilijker om telefoons van verschillende merken veilig met elkaar te laten communiceren.’ Met SNS is er een open standaard gekomen voor de civiele markt. SNS maakt het eenvoudig om platform- en netwerkonafhankelijke oplossingen te ontwikkelen, zoals SecuVOICE van Fox-IT (zie kader). Met SecuVOICE kun je veilig met elkaar communiceren, vanaf een vaste of mobiele telefoon.

MENS IS ZWAKKE SCHAKEL

Goede beveiliging van een mobiele telefoon blijft een uitdaging, maar vaak genoeg is de mens de zwakste schakel. Niemand vindt het leuk om een mobieltje van de baas dat na een paar minuten in een beveiligde stand schiet, steeds met een code te moeten ontgrendelen. Mensen zullen dan toch

AIVD GEEFT FIAT AAN VEILIG BELLEN

Beveiligd bellen met GSM’s tot het niveau ‘Departementaal Vertrouwelijk’ kan met het product SecuVOICE van Fox-IT. In april gaf de AIVD daar haar goedkeuring aan. Het hart van SecuVOICE vormt een speciale smartcard die de gebruiker in het slot van een mobiele telefoon steekt. De kaart bevat een cryptochip die alle gesprekken en sms’jes versleutelt.

even hun eigen mobieltje pakken, met alle risico's van dien. Niets menselijks is ook onze politici vreemd: dit voorjaar viel in een uitzending van Eén Vandaag te zien dat het geen probleem was om de voicemails van ministers en andere hoogwaardigheidsbeklederste beluisteren. De reden: de gebruikers hadden de pincode van hun voicemail op de algemeen bekende standaardinstelling laten staan. Pijnlijk was dat na de uitzending gebruikers wel de pincode hadden aangepast, maar dat sommigen daarvoor een te simpele code gebruikten. Zo wisten journalisten met een educated guess (door bijvoorbeeld een geboortedatum te gebruiken) alsnog in te breken in de voicemail.

'De meeste gebruikers zijn zich niet bewust van de veiligheidsrisico's'

Nieuwsuur wist daags daarna ook voicemailboxen van hoogwaardigheidsbeklederste kraken door de meegezonden nummerinformatie te manipuleren. Voor de gemiddelde hacker geen grote uitdaging. Vodafone, die alle mobiele telefoons voor de Rijksoverheid levert, reageerde met de mededeling dat er een afweging moet worden gemaakt tussen gebruiksgemak en beveiliging.

SPAGAAT

Dat is de spagaat waarin gebruikers en beveiligers zich bevinden. En dat probleem wordt alleen maar nijpender nu smartphones en tablets ook tijdens vergaderingen in boardrooms verschijnen. Handig, maar niemand wil toch dat de concurrent bedrijfsgeheimen af kan luisteren. Het is ook iets wat Peter van Zunderd bezighoudt. Hij is voorzitter van de Landelijke Operationele Staf (LOS) en oriënteert zich bij Fox-IT op de mogelijkheden van smartphones en tablets (zie kader). 'Bij een ramp zijn de eerste uren cruciaal. De leden van de staf die over heel Nederland verspreid zitten, moeten direct via een mobiele verbinding, liefst met video, met elkaar kunnen overleggen. Gebruiksgemak en continuïteit hebben in zo'n situatie voor ons prioriteit, dat moeten we afzetten tegen veiligheidsaspecten.'

GEBRUIKSVRIENDELIJKE BEVEILIGING

Gebruiksvriendelijke beveiliging heeft dus de toekomst. Een logische optie is monitoren. Monitoren richt zich niet op het mobiele platform zelf, maar op het dataverkeer tussen provider en gebruiker. Pas als er iets verdachts gebeurt, komt de beveiliging in actie. 'Het is niet zo dat we ál het dataverkeer monitoren, we letten op bepaalde karakteristieken', vertelt Eward Driehuis, expert van Fox-IT op het gebied van monitoring. 'Stel dat een gebruiker van een iPhone binnen een paar milliseconden van toestel verwisselt. Op zich kan een gebruiker een gesprek met een ander toestel voortzetten, maar het duurt even voordat hij een andere telefoon heeft gepakt en z'n SIM-kaart verwisseld. Zo'n snelle wisseling wordt door onze software van een rood vlaggetje voorzien want het betekent wellicht dat de telefoon overgenomen is. In combinatie met andere karakteristieken kan het aanleiding zijn om contact op te nemen met de provider.'

MONITOREN EN PRIVACY

Monitoren roept wel de vraag op of het geen bedreiging voor de privacy is. In mei dit jaar kwam KPN in opspraak omdat ze met Deep Packet Inspection van dataverkeer naging of gebruikers bepaalde apps gebruikten. Driehuis: 'Telecomproviders monitoren het telefoonverkeer al op een bepaald niveau omdat ze zo de beschikbaarheid van hun netwerk kunnen optimaliseren. Er zijn allerlei gradaties van monitoring. Wat wij doen, is kijken naar de vrachtwagens met post, niet naar de brieven. Slaat een vrachtwagen af naar bijvoorbeeld een Oost-Europees land waar veel cybercriminaliteit vandaan komt, dan trekken we aan de bel.

LANDELIJKE OPERATIONELE STAF (LOS)

Het LOS is een 'slapende' organisatie die tot leven komt bij een grote ramp, zoals een overstroming, pandemie of terroristische aanslag. In het LOS zitten vertegenwoordigers van defensie, politie, brandweer, GGD en gemeenten. Ze geven multidisciplinair operationeel advies aan de regering.

'Gebruiksvriendelijke beveiliging heeft de toekomst'

'Spagaat tussen gebruiksvriendelijkheid en veiligheid'

Het grote voordeel van monitoren is dat de gebruiker deze vorm van beveiliging niet als last ervaart. Toch betekent dit niet dat monitoren andere vormen van beveiliging overbodig maakt. 'Een goede beveiliging werkt met lagen', stelt Driehuis. 'De provider moet zijn beveiliging op orde hebben. De gebruiker moet op zijn smartphone of tablet beveiliging toepassen, zich bewust zijn van de gevaren en zijn gedrag daar op aanpassen. Daarnaast kunnen wij het lijntje tussen provider en platform in de gaten houden.' ■

MARINESCHIP PERFECTE PLEK OM TE NETWERKEN

Indiase interesse voor **Fox DataDiode**

Op 24 mei ontvingen Fox-IT en de Indiase partner High-Tech Technologies lokale klanten op het luchtverdedigings- en commandofregat Hr. Ms. Tromp. In de haven van Bombay kreeg Fox-IT een uitgelezen kans om verder te werken aan de uitbreiding van het internationaal portfolio.

Fox-IT heeft een sterke focus op innovatie en wil blijven groeien. Ook in het buitenland. Met een groeiend partnernetwerk bereikt Fox-IT steeds meer landen. Samen met partner High-Tech Technologies (HTT) timmert Fox-IT hard aan de weg in India. HTTis trusted partner van de overheid, defensie en bedrijven die vitale infrastructuur in India beheren. Het bedrijf lijkt sterk op Fox-IT en is daarmee een prima partij voor de Indiase markt.

KANS

Op 24 mei kregen HTT en Fox-IT de kans om hoogwaardige contacten binnen de Indische marine, luchtmacht, Air Traffic Control, Indiase spoorwegen en Tata Power uit te nodigen op het marineschip Hr. MS. Tromp. In deze inspirerende hightech-omgeving toonde Fox-IT diverse crypto-oplossingen zoals de Fox DataDiode. Voor deze Fox-oplossing zijn goede vooruitzichten op de Indiase markt.

‘De Fox DataDiode wordt gecertificeerd voor de Indiase markt’

CERTIFICERING DATADIODE

Op verzoek van een aantal defensieklanten laat Fox-IT de Fox DataDiode certificeren door het Standardisation Testing and Quality Certification (STQC) directorate van het Indiase Department of Information Techology. Dit staat hen toe om de Fox DataDiode zonder verdere belemmeringen operationeel in te zetten. Deze nieuwe versie van de DataDiode wordt geëvalueerd op Common Criteria (ISO/IEC 15408) EAL4+. Dit wordt het tweede product dat het STQC certificeert. ■

De Hr. Ms. Tromp is één van de vier luchtverdedigings- en commandofregatten van de Nederlandse Marine. Opvallend is het STEALTH-design dat het fregat minder goed zichtbaar maakt voor vijandelijke radar. Het schip kwam dit jaar succesvol in actie tegen Somalische piraterij.

‘Samen met partner High-Tech Technologies (HTT) timmert Fox-IT hard aan de weg in India’

HIGH-TECH TECHNOLOGIES

High-Tech Technologies (HTT) houdt zich bezig met Cyber Forensics, Mobile Forensics en Network Forensics zoals beeldanalyse, password recovery, e-Discovery, steganografie, GPS forensics, Audio/Video forensics en producten voor het verzamelen van inlichtingen. Hierbij worden strategische samenwerkingsverbanden aangegaan. HTT beschikt over eigen oplossingen voor computer forensics en informatiebeveiliging. Meer informatie: http://htt.co.in

PRAKTIJK

Made in Holland

Nederland is internationaal voorbeeld bij bestrijding cybercrime

Kaas, tulpen en Delfts Blauw zijn onze klassieke exportproducten. Maar sinds kort hebben we er één bij: onze expertise in het bestrijden van cybercrime. Noodgedwongen hebben we die kennis en ervaring opgebouwd: Nederland is vaak het slachtoffer van cyberaanvallen. Internationale samenwerking is noodzakelijk, want cybercrime kent geen landsgrenzen.

In relatief korte tijd is Nederland één van de koplopers geworden bij de bestrijding van cybercrime. De kennis die we hebben opgedaan, delen we graag met andere landen. In deze Fox Files passeren twee voorbeelden de revue. Zo hebben het Team High Tech Crime (THTC) van het KLPD en Fox-IT een opleiding verzorgd voor medewerkers van de Oekraïense veiligheidsdienst SBU. En de Verenigde Staten maakten recent bij het oprollen van het Coreflood-botnet gebruik van de methode die Nederland vorig jaar toepaste bij de ontmanteling van het Bredolab. Het lijkt er dus op dat onze kennis over internetbeveiliging binnenkort in het rijtje van belangrijkste Nederlandse exportproducten staat.

TRAINING VOOR OEKRAÏENSE VEILIGHEIDSDIENST

Wodka als wonderolie

Veel cybercriminelen komen uit Rusland en Oekraïne. Alleen de lokale autoriteiten zijn bevoegd om deze criminelen op te pakken. Maar zij hebben een behoorlijke kennisachterstand op het gebied van cybercrime. Daarom kregen medewerkers van de Oekraïense veiligheidsdienst SBU training in het opsporen van digitale misdaad. Fox-IT verzorgde samen met het Team High Tech Crime en Team Digitaal en Internet van het KLPD een deel van deze training. Een goed voorbeeld van kennisdeling over de grens.

Pim Takkenberg, teamleider van het THTC, vertelt: ‘Veel cybercrime vindt zijn oorsprong in Oekraïne. Met onze training helpen we collega’s in Oekraïne om strafbare feiten te herkennen. Om maar een simpel voorbeeld te noemen: veel inwoners van Oekraïne hebben geen eigen bankrekening. Hierdoor weten ze niet hoe internetbankieren eruit ziet. Dat levert een achterstand op bij de opsporing van cybercrime.’

Specialisten van het KLPD en Fox-IT ontwikkelden een uitgebreid trainingsprogramma en vertrokken naar Oekraïne.

SPOREN ZOEKEN

Vanuit Fox-IT was onder andere forensisch IT-expert Christian Prickaerts bij het project betrokken. Hij geeft regelmatig training over cybercrime aan de politie, Openbaar Ministerie, hogescholen of bedrijven.

‘Veel inwoners van Oekraïne hebben geen eigen bankrekening en weten niet hoe internetbankieren eruit ziet’

En nu dus ook aan crimefighters in Oekraïne. Prickaerts: ‘De training besloeg in totaal drie weken. In de eerste week kregen de medewerkers algemene informatie over dreigingen in de financiële wereld en phishing. Wij verzorgden het technische onderdeel van de training in de tweede en de derde week. Aan de hand van cases leerden we de medewerkers hoe ze een digitaal forensisch onderzoek kunnen uitvoeren. We maakten hiervoor gebruik van open-source software en hadden zelfs een mobiel leslokaal naar Kiev gebracht.’
De medewerkers van Fox-IT en KLPD lieten eerst zien hoe je op de laptop van een slachtoffer zoekt naar informatie over de herkomst en werking van een virus, zodat je

TEAM HIGH TECH CRIME

Het Team High Tech Crime (THTC) is onderdeel van de dienst Nationale Recherche van het KLPD. Het team richt zich op de bestrijding van zware, georganiseerde vormen van cybercrime. Teamleider Pim Takkenberg: ‘Bestrijden staat in dit geval voor een combinatie van opsporen en tegenhouden. Dit laatste houdt in dat we barrières opwerpen om strafbaar gedrag in de toekomst te voorkomen.’
Bij de start in 2007 richtte het THTC zich voornamelijk op zaakgericht opsporen. ‘We gingen gewoon een zaak onderzoeken in de hoop hem op te lossen. Het nadeel van deze methode was dat veel sporen ondertussen al waren verdwenen.’ In 2008 maakte het team de overstap naar meer persoonsgerelateerd opsporen. ‘Door meer te focussen op groepen en organisaties, loop je minder achter de feiten aan.’ Sinds 2009 legt het THTC steeds meer de nadruk op fenomeengerelateerd opsporen: het team brengt fenomenen zoals botnets in kaart en probeert zo de cybercrime effectief en integraal aan te pakken.

Over grenzen gaan letterlijk en figuurlijk

COREFLOOD-BOTNET OPGEROLD ALS BREDOLAB

Ook zonder directe betrokkenheid vormt Nederland een voorbeeld voor andere landen. De Verenigde Staten hebben onlangs het Coreflood-botnet opgerold, waarvoor de methode is gebruikt die Nederland vorig jaar al toepaste om het Bredolab neer te halen. Het Team High Tech Crime en Fox-IT namen bij de ontmanteling van het Bredolab zelf de controle over het botnet over. Een aanpak die ter discussie staat, maar wel doeltreffend is.

SAMENWERKING MET OEKRAÏNE

De training aan medewerkers van de SBU was een samenwerking tussen Fox-IT, het KLPD en de Nederlandse Vereniging van Banken. Deze training kwam voort uit een beperkt landenprogramma voor Oekraïne: een niet-operationele samenwerking van het KLPD met collega's in Oekraïne, waarbij kennis delen, kennis halen en een netwerk opbouwen centraal staan.
De Dienst Internationale Politiesamenwerking (IPOL) van het KLPD gaf in 2009 de aanzet voor de samenwerking. IPOL adviseerde de stuurgroep internationale samenwerking (STIPS) om met een beperkt landenprogramma in te stemmen, omdat er operationele en politieprofessionele belangen met Oekraïne zijn. De training in de aanpak van cybercrime was een van de eerste projecten met Oekraïne.

uiteindelijk de computer van de verdachte traceert. Vervolgens legden ze uit hoe je naar sporen zoekt op de computer van de verdachte. Zijn de creditcardgegevens van het slachtoffer in de computer opgeslagen? Of is de broncode van het virus er misschien te vinden?

WEDERZIJDS BEGRIP

Het doel van de training was de medewerkers leren om zelfstandig onderzoek te doen naar cybercrime. In hoeverre de trainers daarin zijn geslaagd, is nog niet duidelijk. Het niveau van de cursisten liep nogal uiteen, aldus Prickaerts. 'Sommigen leerden heel snel en konden de kennis ook in andere situaties toepassen. Anderen hadden er meer moeite mee.'
Maar het ging de betrokken organisaties niet alleen om de pure overdracht van kennis. 'Zo'n training zorgt ook voor wederzijds begrip', vertelt Takkenberg. 'We kregen inzicht hoe ze in Oekraïne werken en andersom. Dat is van belang als we internationaal willen samenwerken bij de aanpak van cybercriminaliteit.' 'We hebben echt aan onze relatie gewerkt', vult Prickaerts aan. 'Onze Oekraïense collega's lieten meerdere malen hun waardering blijken en waren heel gastvrij. Ze nodigden ons bijvoorbeeld uit voor officiële diners, waarbij naar goed traditioneel Oekraïens gebruik de wodka rijkelijk vloeide. We hebben tijdens die weken belangrijke contacten gelegd.' Wodka dus als wonderolie.

INTERNATIONAAL NETWERK

Die goede relatie is misschien nog wel het belangrijkste. De opbouw van een internationale netwerk is essentieel om cybercrime integraal aan te pakken. Takkenberg: 'Het internet kent geen grenzen. Bij cybercrime zijn vaak meerdere landen betrokken. Zo komt het regelmatig voor dat criminelen uit Rusland of Oekraïne gebruikmaken van de Nederlandse infrastructuur om uiteindelijk in de VS toe te slaan. Willen we cybercrime echt aanpakken, dan moeten we samenwerken.'

'Het doel van de training was de medewerkers leren om zelfstandig onderzoek te doen naar cybercrime'

Botnets vormen een grote bedreiging op het internet. Het Team High Tech Crime (THTC), Govcert.nl, Leaseweb, het NFI en Fox-IT werkten samen om het botnet Bredolab op te rollen. Hiervoor zochten ze de grenzen van de wet op. Ze moesten wel. Ze gebruikten vernieuwende technieken waarover nog geen wetgeving of jurisprudentie bestaat. Pim Takkenberg, Teamleider van THTC: 'We denken out-of-the-box en bevinden ons daarbij soms op de grens van het toelaatbare.'

EIGEN SOFTWARECLIENT

De verdachten binnen het Bredolab-onderzoek maakten gebruik van minimaal 143 servers en veroorzaakten sinds juli 2009 ten minste 30 miljoen computerinfecties. Om het botnet neer te halen, maakte het KLPD gebruik van het botnet zelf. Het installeerde er een eigen softwareclient op die werd geüpload naar alle op dat moment besmette computers binnen het botnet. De software zorgde voor waarschuwingsberichten op het scherm van de gebruikers zodra zij hun computer aanzetten. Zo kon het KLPD het netwerk neerhalen en ervoor zorgen dat in Armenië het 27-jarige brein achter het Bredolab werd gearresteerd.

DIGITALE ZAAKWAARNEMING

Deze methode deed behoorlijk wat stof opwaaien. De politie zou de wet hebben overtreden door op het botnet in te breken. Het zou niet toegestaan zijn om computers van anderen over te nemen met eigen botcliënts. Het Openbaar Ministerie (OM) ontkrachtte deze kritieken. Politie en justitie waren niet in overtreding bij de ontmanteling van het Bredolab. Het is weliswaar verboden om in een andere computer binnen te dringen, behalve als dat gebeurt om schade te beperken. En dat was volgens het OM van toepassing. We kunnen hier als het ware spreken van zogenaamde legitieme digitale zaakwaarneming.

VERNIEUWENDE AANPAK

Nederlandse cybercrime-experts wisselen geregeld kennis uit met collega's in de VS. Takkenberg: 'In ons Team High Tech Crime zitten permanent liaisons van de FBI en de USSS (United States Secret Service). Dat is vrij uniek. Het zegt wat over de expertise die we in Nederland hebben opgebouwd voor de bestrijding van cybercrime. Zij zitten niet alleen in ons team om operationele zaakgegevens uit te wisselen, maar ook om van onze vernieuwende aanpak te leren.'
Een goed voorbeeld daarvan was in maart te zien. De VS hebben toen het Coreflood-botnet ontmanteld, waarbij ze dezelfde methode gebruikten als hiervoor beschreven. 'In de rechtbankdocumentatie wordt zelfs verwezen naar onze Nederlandse methodiek', vertelt Takkenberg. Het Coreflood-botnet omvatte meer dan twee miljoen computers en zou gebruikt zijn om meer dan 100 miljoen dollar te stelen. Het Amerikaanse ministerie van Justitie vroeg toestemming aan een federale rechter om het botnet over te nemen en hierop eigen software te installeren. Door gebruik te maken van de Nederlandse methodiek, konden de VS een botnet dat al tien jaar actief was eindelijk uitschakelen. ■

'In ons Team High Tech Crime zitten permanent liaisons van de FBI en de USSS'

NATIONALE CYBER SECURITY STRATEGIE

In februari presenteerde het kabinet de Nationale Cyber Security Strategie (NCSS). Deze strategie moet zorgen voor een integrale aanpak van cybercrime. In Nederland, en daarbuiten. Omdat veel dreigingen een grensoverschrijdend karakter hebben, is internationale samenwerking essentieel. Bijzonder aan de NCSS is dat publieke en private partijen met elkaar samenwerken. Ook Fox-IT speelde een rol bij de totstandkoming van de NCSS (zie Fox Files maart 2011).

Vrijheid versus veiligheid

3 EXPERTS, 3 MENINGEN

Voor criminelen is internet een grote speeltuin. De vrijheid is enorm. Er is geen internationale internetpolitie of een internationaal internetstrafhof. Criminelen zien internet als een handig hulpmiddel of een plek die uitnodigt tot nieuwe misdaad. Wetgeving, vrijwel altijd op nationaal niveau, hobbelt achter de feiten aan. Terwijl het grote publiek steeds vaker wordt geconfronteerd met de gevolgen van cybercrime – van het hacken van persoonsgegevens en identiteitsfraude tot slecht gespelde phishingmails.

De maatschappij realiseert zich steeds meer dat cybercrime een probleem is. Maar op welke manier moet je ingrijpen? En hoe ver ga je daarin? Wet- en regelgeving kunnen inbreuk maken op de privacy en de vrijheid beperken die van internet zo'n uniek en innovatief medium maakt.

In deze editie van Fox Files belichten we het thema internetvrijheid en veiligheid van drie kanten. Willemijn Aerdts van Burgerrechtenbeweging Bits of Freedom vindt dat we eerst moeten onderzoeken wat de aard en omvang van cybersecurity is, voor we nieuwe bevoegdheden toestaan. Erik Akerboom, Nationaal Coördinator Terrorismebestrijding en Veiligheid en co-voorzitter van de Cyber Security Raad, kiest voor een pragmatische benadering: zo min mogelijk bureaucratie en samenwerking met marktpartijen. Fox-IT-directeur, Ronald Prins, benadrukt tot slot hoe belangrijk het is om cyberdreigingen op tijd te signaleren. Hij vindt het geen probleem als de overheid daarvoor wat meer op internet rondsnuffelt.

OPINIE

WILLEMIJN AERDTS OVER VRIJHEID EN VEILIGHEID

‘Eerst helderheid verkrijgen over aard en omvang van cybersecurity’

Bits of Freedom is een beweging die opkomt voor digitale burgerrechten. De beweging analyseert nieuwe ontwikkelingen, informeert hierover, lobbyt en voert campagne. Centraal staan communicatievrijheid en bescherming van de privacy op het internet.

1. Private partijen moeten zich niet met cybersecurity bemoeien.
Aan publiek-private samenwerking op veiligheidsgebied kleven nadelen. We noemen vooral het gebrek aan transparantie; op het functioneren van overheidsinstanties kan het parlement een bepaalde controle uitoefenen, dat ligt moeilijker bij private partijen. Als blijkt dat de overheid structureel kennis over digitale opsporing mist, dan moet de overheid daar zelf iets aan doen en niet een derde partij voor deze taak inhuren. Je ziet dat aan de organisatie die zich bezighoudt met de OV-chipkaart, het parlement zegt nu: ‘Maak daar een organisatie van waar de overheid controle over heeft.’ De nadruk op zelfregulering en publiek-private samenwerking vormt een gevaar voor de parlementaire democratie en onze internetvrijheid.

2. Het ontwikkelen van offensieve capaciteiten voor ordehandhaving in het cyberdomein is noodzakelijk.
Deels voldoen traditionele opsporingsmethoden nog. Voor je nieuwe bevoegdheden gaat toestaan, moet je eerst helderheid krijgen over de aard en omvang van cybersecurity. Wat is cybersecurity precies? Hoe groot is het probleem? Wat kan er met de bestaande opsporingsmethoden? Wie mag wat doen? Daar moet eerst onafhankelijk onderzoek naar worden gedaan. Een gebrek aan nuance over cybersecurity doet meer kwaad dan goed.

3. De traditionele aanpak van misdaad en vervolging is niet meer adequaat door het vervagen van de landsgrenzen in het cyberdomein. Als een cybercrimineel vanuit de Russische stad Chelyabinsk een computer in Nederland hackt, moet de Nederlandse jurisdictie gelden.
Dit klinkt in eerste instantie aantrekkelijk maar wat als, bij wijze van spreken, China computers in Nederland gaat onderzoeken? Traditioneel wordt ervoor gekozen de bevoegdheden van de politie binnen de eigen landsgrenzen te houden. Ook om jezelf te beschermen. Er is een aantal verdragen die samenwerking tussen landen mogelijk maakt. Desgewenst kan Nederland die aanpassen.

4. Bescherming van privacy is niet nodig als je toch niks te verbergen hebt.
Daar zijn we het niet mee eens en dat geldt voor steeds meer Nederlanders. Met de groei van het internet groeit het bewustzijn dat we op onze privacy moeten letten. Iedereen kent wel verhalen, variërend van identiteitsfraude tot Facebookfoto’s die een probleem vormen bij een sollicitatie of promotie. Uit informatie die we van Hyves ontvingen, blijkt dat bijna 90 procent van de jongeren zijn privacy-instellingen aanpast.

5. Je mag in sommige gevallen best de vrijheid een klein beetje inperken als daarmee de veiligheid enorm wordt vergroot.
De meeste grondrechten zijn niet absoluut. Je moet een afweging maken, maar dat moet wel volgens strakke regels. Het Europees Verdrag voor de Rechten van de Mens besteedt daar veel aandacht aan en wijst op noodzakelijkheid en proportionaliteit als je rechten wil inperken. Neem de bewaarplicht. Wordt door alle telefoon- en internetgegevens te bewaren de veiligheid enorm vergroot? Tot nu toe heeft geen enkel land aan kunnen tonen dat het opslaan van gegevens leidt tot een stijging van de opsporingspercentages. Op de vraag van de Europese Commissie of landen iets aan het bewaren hadden, is onvolledig of helemaal niet gereageerd. Inmiddels is de bewaarplicht voor internetgegevens teruggebracht naar zes maanden. Wij pleiten ervoor de bewaarplicht helemaal af te schaffen.

6. Cybercrime is breder dan het internet. Eigenlijk is er geen verschil meer tussen gewone misdaad en cybercrime.
Er is inderdaad geen verschil als je het bekijkt vanuit de grondrechten: die gelden altijd. Er is wel verschil in handhaving, omdat die semi-geautomatiseerd plaats kan vinden. Daardoor moet extra worden gewaakt voor het onnodig en disproportioneel schenden van grondrechten.

ERIK AKERBOOM OVER VRIJHEID EN VEILIGHEID

‘Privacy is voor mij geen obstakel, maar een vertrekpunt’

Erik Akerboom, vooral bekend als Nationaal Coördinator Terrorismebestrijding en Veiligheid, is ook co-voorzitter van de net opgerichte Cyber Security Raad. Deze raad adviseert de regering over digitale veiligheid. Hoe denkt hij over vrijheid en veiligheid?

1. Private partijen moeten zich niet met cybersecurity bemoeien.
Ik geloof in publiek-private samenwerking. Als je cybersecurity alleen een zaak van de overheid maakt, dan is de opbrengst van je acties beperkt. Want de wereld van de ICT is veel sneller, veel minder orthodox maar bovenal voor 90 procent in handen van private partijen. Amerikanen en Canadezen die bij ons op bezoek komen, vinden het reuze interessant zoals wij samenwerking zoeken met private partijen. Nederland ontwikkelt zich dankzij die aanpak tot gidsland op het gebied van cybersecurity.
De vraag is wel: in hoeverre is het toetsbaar wat private partijen doen? Er moet een kader zijn voor hoe partijen met gevoelige informatie omgaan. Je moet duidelijke afspraken maken én je aan die afspraken houden. Overigens zijn er goede ervaringen in het samenwerken tussen private partijen en de overheid op het gebied van veiligheid. Denk aan de beveiliging op Schiphol of de inzet van forensische accountants.

2. Het ontwikkelen van offensieve capaciteiten voor ordehandhaving in het cyberdomein is noodzakelijk.
We moeten in ieder geval toe naar een ander concept van cyberbeveiliging. Bij cloudcomputing heeft het bouwen van firewalls niet zoveel zin meer. Je moet eigenlijk het internetverkeer gaan monitoren. Dat is nogal een opdracht om te doen zonder dat je goede afspraken maakt om privacy te borgen. Je moet aan de voorkant afspreken hoe je dat aan wil pakken en daarna toetsen of het gebeurt zoals is afgesproken. Wat je niet moet doen, is daar een enorme bureaucratie voor optuigen, want dat beperkt.

3. De traditionele aanpak van misdaad en vervolging is niet meer adequaat door het vervagen van de landsgrenzen in het cyberdomein. Als een cybercrimineel vanuit de Russische stad Chelyabinsk een computer in Nederland hackt, moet de Nederlandse jurisdictie gelden.
Het is een van de dingen die de Cyber Security Raad in beeld wil brengen. Het is een interessant idee. In Oostenrijk gebeurt dat al. Je kunt zo handelen zonder direct de hele wereld over te moeten met rechtshulpverzoeken. In cybersecurityzaken moet je snel kunnen reageren. Een internationaal verdrag over deze materie gaat lang duren. Uiteindelijk wil je een verdrag, maar in de tussentijd moet er een Nederlandse oplossing komen. In de huidige situatie moeten we ons in ieder geval aan de spelregels houden, juist op het punt van jurisdictie.

4. Bescherming van privacy is niet nodig als je toch niks te verbergen hebt.
We weten uit de fysieke wereld dat anonimiteit de schuilplaats van het kwaad is. Het is goed als je criminaliteit uit de anonimiteit haalt. Aan de andere kant is anonimiteit een garantie dat internet maximaal zijn rol vervult; kijk naar wat er nu in het Midden Oosten gebeurt met de Arabische lente. Als er indicaties zijn dat er strafbare feiten plaatsvinden, dan moet je de anonimiteit echter wel opheffen.

5. Je mag in sommige gevallen best de vrijheid een klein beetje inperken als daarmee de veiligheid enorm wordt vergroot.
Bij de aanpak van cybercrime is privacy voor mij geen obstakel, maar een vertrekpunt. De Raad en de overheid moeten duidelijke ideeën ontwikkelen over privacy en waar de grenzen liggen. Iedere maatregel die de privacy beperkt, moet aan een duidelijk veiligheidsdoel verbonden zijn en worden getoetst. Als je zegt: dit doen we om het internet veilig te houden, dan moet je je ook echt daartoe beperken. Je moet goed nadenken over de balans. Hoe ver ga je voor veiligheid? Niet alles is te voorkomen, er zullen altijd risico’s blijven. In het verkeer bestaat ook de kans dat je door een auto wordt geschept, toch gaan we dagelijks de straat op.

6. Cybercrime is breder dan het internet. Eigenlijk is er geen verschil meer tussen gewone misdaad en cybercrime.
Het gaat niet om nieuwe fenomenen. Het gaat om bestaande vormen van criminaliteit, onveiligheid en dreiging in een ander medium: internet. In dat medium gaat alles wél sneller. Bovendien zijn de actieradius en de schaal groter. De vraag is: hoe dam je die dreigingen in? Het kan niet blijven zoals het is. Samen met bijvoorbeeld providers moeten we kijken naar de bedreigingen en risico’s en die vertalen in maatregelen. Dat vereist een transparante aanpak, maar niet een waarbij we alles dichtregelen, want dat verhoudt zich niet met de dynamiek van de internetwereld. Een goed voorbeeld vind ik de Notice-and-takedown procedure voor het verwijderen van onrechtmatige inhoud op het internet. In andere landen bestaat in dat opzicht veel meer spanning tussen overheid en providers. De in samenspraak met marktpartijen opgestelde gedragscode heeft voorkomen dat er bij ons een heel strafrechtelijk systeem werd opgetuigd.

DE CYBER SECURITY RAAD

De Cyber Security Raad werd op 30 juni van dit jaar opgericht. De Raad geeft de regering en private partijen gevraagd en ongevraagd adviezen over ontwikkelingen op het gebied van digitale veiligheid. Als eerste zal de Raad de dreiging in kaart brengen en een inschatting maken van de schade die cybercrime de samenleving toebrengt. Ook wil de Raad plannen opstellen voor een beter gecoördineerde gezamenlijke respons bij een mogelijke cyberaanval of grootschalige hack. Privacyvraagstukken en de vrijheid van meningsuiting en informatievergaring heeft de Raad hoog op de agenda staan.

RONALD PRINS OVER VRIJHEID EN VEILIGHEID

‘Ik vind het belangrijk dat de overheid over mijn privacy waakt’

Ronald Prins, directeur van Fox-IT, werkt regelmatig samen met de overheid aan cybersecurity-projecten en heeft een eigen kijk op digitale vrijheid en veiligheid.

1. Private partijen moeten zich niet met cybersecurity bemoeien.
Ik denk dat de overheid zelf meer digitale slagkracht nodig heeft. Private partijen moeten geen unieke rol in de opsporing krijgen, maar de overheid kan ze wel heel goed inzetten om nieuwe onderzoekstechnieken te ontwikkelen. Daarnaast blijkt de overloopfunctie erg praktisch bij onverwachtse digitale incidenten. Een private partij kan dan snel bijspringen om het incident te verhelpen. Het is voor de overheid soms lastig om de goede mensen te vinden en aan zich te binden. De samenwerking tussen private en publieke opsporing geeft de overheid ook een beter idee over het type medewerkers dat ze nodig heeft.

2. Het ontwikkelen van offensieve capaciteiten voor ordehandhaving in het cyberdomein is noodzakelijk.
In de Defensiecontext hebben we zeker offensieve capaciteit nodig om een aanval af te kunnen slaan. Maar het is nog belangrijker dat de overheid investeert in een ‘operationeel dreigingsbeeld’. Hiermee bedoel ik niet dat we opnieuw moeten onderzoeken of er wel een cyberdreiging is, maar dat we hem op tijd signaleren. Op dit moment blijft heel veel cyberellende onopgemerkt. We hebben geen idee hoeveel informatie wegstroomt door digitale spionage of hoeveel privacygevoelige gegevens worden gestolen. Hier is duidelijk sprake van een kip-eiprobleem. Zonder monitoring weten we niet hoe het zit. We weten ook niet of de door de overheid geïntroduceerde privacyrisico’s gerechtvaardigd zijn. Maar we kunnen het ons ook niet veroorloven om ze te negeren.

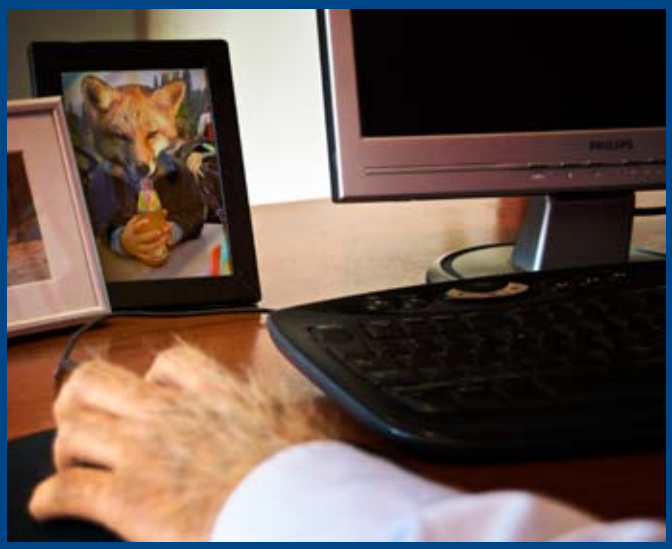
3. De traditionele aanpak van misdaad en vervolging is niet meer adequaat door het vervagen van de landsgrenzen in het cyberdomein. Als een cybercrimineel vanuit de Russische stad Chelyabinsk een computer in Nederland hackt, moet de Nederlandse jurisdictie gelden.
We moeten met een cyberbril onze wetgeving opnieuw doorlichten. Natuurlijk moet de Nederlandse politie niet lukraak hacken in het buitenland om een zaak rond te krijgen. Maar bij delicten die niet op een andere manier op te lossen zijn, moet het misschien wel worden toegestaan. Als voorbeeld noem ik de hidden services binnen het TOR-netwerk. Een TOR (The Onion Router) is een open netwerk voor anonieme communicatie. Daar kan verboden content op staan, zoals kinderporno, terwijl we niet eens weten in welk land zo’n server staat. Waar meld je je dan met een rechtshulpverzoek? Andere bevoegdheden van de overheid mogen juist wel worden ingeperkt. Als de politie nu bij mij een huiszoeking doet en alle computers meeneemt, heeft ze twintig jaar historie in handen. Twintig jaar geleden bewaarden we niet zo veel en was een huiszoeking misschien veel minder ingrijpend dan nu.

4. Bescherming van privacy is niet nodig als je toch niks te verbergen hebt.
Dat is te kort door de bocht. Iedereen heeft wat te verbergen. Er is veel meer op internet vastgelegd dan veel mensen denken. Het internet vergeet niets en het risico op privacy-inbreuken wordt alleen maar groter. Daarom is het steeds belangrijker om al die privacygevoelige gegevens te beschermen.

5. Je mag in sommige gevallen best de vrijheid een klein beetje inperken als daarmee de veiligheid enorm wordt vergroot.
Dat is de beroemde virtuele tegenstelling. Ik vind het juist belangrijk dat de overheid waakt over mijn privacy. Ik wil niet dat die vergaarbak van twintig jaar gegevens op straat komt te liggen. Als het daarvoor nodig is dat de overheid meer rondsnuffelt op het internet, vind ik dat prima. Vanzelfsprekend moet de overheid dat heel zorgvuldig doen en hier transparant over zijn. Het lijkt mij een goed idee om een internetprivacywaakhond in het leven te roepen. Die kan dan niet alleen de overheid op de vingers tikken, maar ook bedrijven die onzorgvuldig met de gegevens van hun klanten omgaan.

6. Cybercrime is breder dan het internet. Eigenlijk is er geen verschil meer tussen gewone misdaad en cybercrime.
Juridisch gezien zijn het misschien allemaal dezelfde delicten. Maar de impact is heel anders. Bij cybercrime kunnen een paar individuen veel meer schade veroorzaken dan bij ‘gewone’ misdaad. Verder hebben we online nog een heel ander normbesef dan offline. Op straat heeft de politieman een pistool en dus een geweldsmonopolie. Maar online zijn we feitelijk allemaal even sterk en wordt de strijd tussen de good guys en bad guys op een andere manier gevoerd. ■

Weetjes en **nieuwtjes**



Fox zoekt Foxers!

- Security Analyst Cybercrime
- Software Developer Cybercrime
- Senior Security Expert Audits
- Software Developer - Forensics
- Medewerker SIB (Support-Implementatie-Beheer)
- Linux beheerder met Windows affiniteit
- HR Business Partner
- Senior Accountmanager / Salesmanager
- Medewerkers Security Monitoring (parttime)

Kijk op jobs.fox-it.com

Events

6 september	Expertmeeting: 'Aanpak fraude in online bankieren'
20 t/m 23 september	NATO IA Symposium
5 oktober	Crypto Klantendag
11 t/m 13 oktober	ISS World Training Americas
12 oktober	Security Congres
3 t/m 4 november	InfoSecurity
8 november	Energy & Utility Cyber Security Summit
1 december	NIDV Symposium en Tentoonstelling

Bundeskriminalamt nieuwe partner Fox-IT

De Bundeskriminalamt (BKA) in Duitsland is een nieuwe partner van Fox-IT. In nauwe samenwerking met de recherchediensten van de individuele deelstaten, de Landeskriminalämter (LKA), coördineert de dienst de misdaadbestrijding op nationaal niveau en verricht onderzoek in criminele zaken met een internationaal karakter. Daarnaast is de dienst verantwoordelijk voor de bescherming van de federale gezagsdragers en vertegenwoordigt de Duitse Bondsrepubliek bij Interpol. De BKA gebruikt FoxReplay Analyst bij het uitvoeren van forensische onderzoeken.

TRAININGSKALENDER

14 t/m 16 september	Digitaal Forensisch Onderzoek – SQL
27 t/m 30 september	Digitaal Forensisch Onderzoek – Microsoft omgeving
10 t/m 13 oktober	Rechercheren op het Internet – Basis
31 okt t/m 1 nov	NVB Masterclass - Digitaal Forensisch Onderzoek (besloten)
3 t/m 4 november	SSR – Maatwerktraining 1e sessie
3 t/m 4 november	Rechercheren op het Internet – Vervolgtraining
7 t/m 8 november	IRN Basic training
9 t/m 11 november	IRN Advanced training
14 t/m 15 november	NVB Masterclass – Digitaal Forensisch Onderzoek (besloten)
16 t/m 17 november	Rechercheren op het Internet – Ken uw klant
17 t/m 18 november	SSR - Maatwerktraining 2e sessie
21 t/m 22 november	Digitaal Forensisch Onderzoek – De Essentie
23 t/m 25 november	FoxReplay Gebruikerstraining – Basis
28 t/m 30 november	ROI – Persoonsgericht zoeken

Meer informatie: www.fox-it.com