Fox-IT

NIEUWS

Maart 2003

Trends in Forensisch IT Onderzoek

Managed Security Monitoring met Plato

Europese partner van Sourcefire!

POB-nummer en goedkeuring CBP-melding

SafeBoot

Even voorstellen...

Nieuwe Opleiding Security & Hacking

Nieuwe PKI oplossingen

Fox-IT Forensic IT Experts B.V.

Haagweg 137

2281 AG Rijswijk

Telefoon: 070 - 336 99 99

Fax: 070 - 336 99 90

E-mail: fox@fox-it.com

www.fox-it.com

Trends in Forensisch IT Onderzoek

Wat zijn de trends in forensisch IT onderzoek? Welke tools worden gebruikt? Leidt een forensisch onderzoek tot vervolging? Fox-IT heeft een onderzoek gehouden om na te gaan of andere forensische IT onderzoekers wereldwijd, dezelfde toename van het aantal onderzoeken waarnemen en of dezelfde tools worden gebruikt. De geënquêteerden zijn vooral forensische onderzoekers, security managers en researchers.

In vergelijking met een jaar geleden, zien de meeste geënquêteerden een groei in het aantal forensische IT onderzoeken. 73% Van de ondervraagden verwacht dat de groei zal doorzetten.

Het onderscheppen van netwerkverkeer is een erg belangrijke techniek voor forensische IT onderzoekers. Meer dan 67% van de ondervraagden hebben bewijzen gevonden door netwerkverkeer te onderscheppen. Andere (digitale) bronnen die gebruikt zijn, zijn de mobiele telefoon, PABX, Fax en PDA. Na het onderscheppen van het netwerkverkeer is de meest gebruikte digitale bron de PDA. De tool voor forensisch IT onderzoek waar het meest mee gewerkt wordt is Encase. Een andere populaire tool is DD.

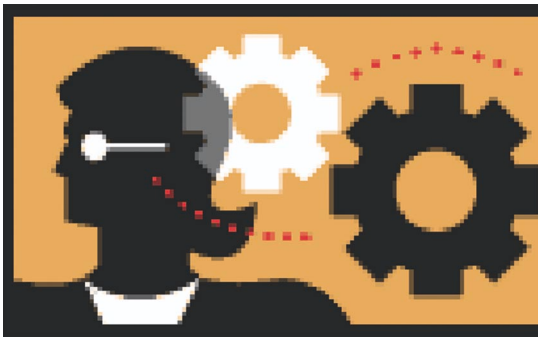
De resultaten van het onderzoek geven duidelijk aan dat forensisch IT onderzoek steeds vaker wordt uitgevoerd. In het Engelstalige rapport over dit onderzoek staan meer resultaten vermeld, www.fox-it.com/survey.

Managed Security Monitoring met Plato

Per 1 januari van dit jaar is een grote stap gemaakt door de lancering van Plato, dat onderdeel is van Fox-IT Managed Security Monitoring.

Plato is het expert systeem dat alle meldingen van de sensoren, die bij onze klanten staan, verwerkt. Deze sensoren geven meldingen door van verdacht netwerkverkeer aan het Fox-IT Security Operations Center (SOC). Het Plato systeem verwerkt deze individuele meldingen en genereert zonodig Meta-Alerts. Op basis van deze Meta-Alerts beslissen de medewerkers van het Security Operations Center of het noodzakelijk is deze door te spelen aan de klant. Op deze manier is het SOC in staat om u alleen te waarschuwen wanneer het echt nodig is.

Plato beschikt over een aantal eigenschappen die normaliter niet in networkbased IDS terug te vinden is: dit zijn onder andere host-based IDS, traffic analysis en IDS evasion detection. Daarnaast kunnen betere analyses gemaakt worden door het combineren van informatie van verschillende sensoren en van meerdere klanten. Deze opgedane kennis wordt op haar beurt weer aan het Plato expert systeem toegevoegd.



Managed Security Monitoring is een belangrijke dienst voor onze klanten. Bescherming tegen hackpogingen en ander ongeoorloofd gebruik wordt steeds belangrijker. Dit belang heeft Fox-IT onderkend en daarom wordt veel energie in het continu verbeteren van deze service gestoken. Een aantal van onze nieuwe medewerkers werken aan de verdere ontwikkeling van het Plato systeem. Zo kunnen we onze voorsprong behouden en zeer alert reageren op nieuwe gevaren van het Internet.

Fox-IT Europese partner van Sourcefire!

Fox-IT is op het gebied van Intrusion Detection Services een partnerschip aangegaan met Sourcefire Inc. Sourcefire is opgericht door de makers van het open source IDS-systeem Snort, een systeem dat door security experts als superieur bestempeld wordt. Fox-IT en Sourcefire zijn twee bedrijven die elkaar goed aanvullen en door samenwerking de stijgende vraag naar betere netwerkbeveiligingsproducten goed aankunnen.

Sourcefire is in Europa op zoek naar sterke partners op het gebied van security en IDS systemen. “Sourcefire Intrusion Detection System provides the most effective network intrusion detection available, however many companies may not have the resources required to make the most of the information. Skilled intrusion detection analysts can help optimize the rule set, analyze the logs and provide a suggested course of action when an attack is detected. The security experts from Fox-IT have significant experience deploying snort sensors and are among the highest skilled analysts available,” zei Martin Roesch, oprichter en technisch directeur van Sourcefire.

Sourcefire wil met Fox-IT een sterke support leveren voor de Sourcefire producten en een goede concurrentiepositie innemen. “The European way is different, we need strong partners in Europe to deliver high value local support to our customers and Fox-IT has the people who can deliver that!” aldus Allen Male, Vice President International Sales.
Fox-IT kan via Sourcefire hun service met betrekking tot Intrusion Detection en Security Monitoring nog verder verbeteren. Door middel van Sourcefire kan Fox-IT IDS producten met een nog betere performance en een zeer goede service aanbieden gecombineerd met lagere beheerskosten. Hierdoor laten we de concurrentie ver achter ons. Daarnaast is het voor ons van groot belang met een goed product in zee te gaan. Tests van zowel onafhankelijke instituten als Fox-IT wijzen uit dat IDS van Sourcefire veruit het beste product is.

Fox-IT verkrijgt POB-nummer en goedkeuring CBP-melding

Fox-IT heeft als eerste forensisch IT bedrijf in Nederland een goedkeuring van het College Bescherming Persoonsgegevens (CBP) gekregen voor haar melding. Sinds 1 september 2001 is ieder bedrijf dat persoonsgebonden informatie vastlegt, verplicht hiervan een melding te doen bij het CBP, de voormalige Registratiekamer. Tot 1 september 2002 gold een overgangstermijn, sindsdien is deze wettelijke eis verplicht gesteld.

Het uitvoeren van forensisch onderzoek komen de onderzoekers van Fox-IT vaak persoonsgebonden informatie tegen. Hoe hiermee wordt omgegaan, staat in de melding van Fox-IT bij het CBP. Deze melding is openbaar en te vinden op de website van het CBP: www.cbpweb.nl. Klik op ‘Openbare registers’ bovenin en vervolgens aan de linker kant op ‘Register meldingen’, ‘Zoeken’ en zoek naar meldingsnummer 1080379 of de naam ‘Fox’.

Naast de goedkeuring van het CBP voor de forensische werkwijze van Fox-IT, is door het Ministerie van Justitie tevens een POB-nummer (824) toegekend. Hiermee is Fox-IT een erkende Particuliere Beveiligingsorganisatie en Recherchebureau. In de praktijk betekent dit dat alle medewerkers aan een screening onderworpen worden en dat zij die zich bezig houden met forensisch IT onderzoek over een diploma particulier onderzoeker beschikken. Tevens heeft Fox-IT een Ecabo erkenning als Leerbedrijf ontvangen en een klachtenregeling ingesteld.
Deze laatste is te vinden op de website van Fox-IT: www.fox-it.com/klachtenregeling.

Even voorstellen…

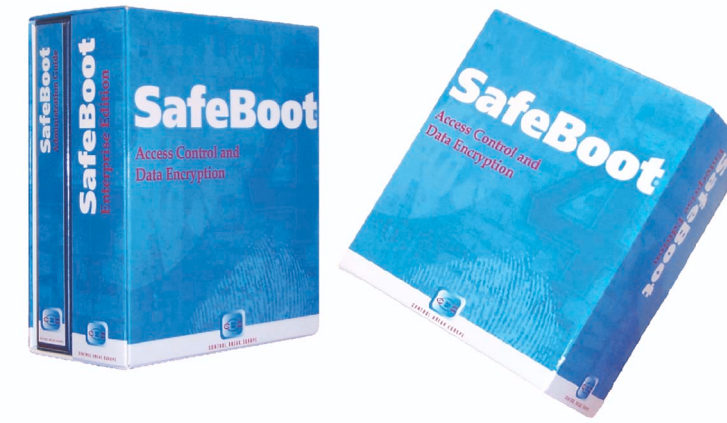
Paul Bakker
IT Security Specialist

Sinds 1 oktober 2002 is hij in dienst bij Fox-IT, na zijn studie Informatica te hebben afgerond aan de Technische Universiteit Delft.
Hij is medeverantwoordelijk voor het uitvoeren van penetratietests en forensische onderzoeken en hij neemt deel aan ontwikkelprojecten.

Daarnaast is het zijn taak het systeem voor Fox-IT Security Monitoring verder uit te denken en te ontwikkelen.

Paul heeft meerdere jaren een eigen bedrijf gehad dat sofware op maat leverde aan middelgrote ondernemingen.
Hij heeft werkervaring opgedaan in het begeleiden en ontwikkelen van projecten op het gebied van IT Security.

SafeBoot



Laptops, werkstations en PDA's bevatten vrijwel altijd waardevolle bedrijfsinformatie, vaak waardevoller dan de hardware zelf. Daarom is het zaak dat informatie goed beveiligd wordt. Fox-IT heeft hiervoor verschillende oplossingen. Een oplossing die zeer effectief en gebruikersvriendelijk is, is SafeBoot.

SafeBoot voorkomt dat data, opgeslagen op een harddisk of geheugenkaart, gelezen of gebruikt wordt door niet geautoriseerde personen. SafeBoot versleutelt alle informatie op de harddisk en voorkomt toegang tot de computer door de gebruiker om identificatie te vragen voordat de computer opstart. Daarnaast kan de toegang, juist van belang in netwerkomgevingen, centraal voor verschillende werkstations centraal worden geregeld.

Het is uitzonderlijk dat Fox-IT met een standaard product werkt. De reden hiervoor is dat Safeboot het enige product is met pre-boot USB-token of Smartcard ondersteuning. Tevens heeft Fox-IT een rol gespeeld bij de ontwikkeling van SafeBoot.

Meer informatie over Safeboot en andere beveiligingsoplossingen van Fox-IT, kunt u aanvragen bij Fox-IT, sales@fox-it.com.

Even voorstellen...

Caroline Frankfort
Office Manager

Sinds 20 januari 2003 is zij in dienst bij Fox-IT.

Caroline is met name verantwoordelijk voor de ondersteuning van de directie en het goed laten verlopen van alle zaken die zich op kantoor afspelen en het ontwikkelen hiervan.

Tevens is zij het eerste aanspreekpunt op kantoor van Fox-IT en beheert ze de administratie.

Caroline heeft al een flink aantal jaren werkervaring opgedaan op secretarieel, administratief en organisatorisch gebied, onder andere als directieassistent bij een groot bowling- en entertainmentcentrum en is daarvoor bijna zeveneneenhalf jaar actief geweest in de horeca.

Joost Bijl
IT Security Specialist

Joost heeft zijn afstudeeropdracht met betrekking tot IDS vervuld bij Fox-IT.
Na afronding van zijn studie Telematica aan de TH Rijswijk is hij op 23 december 2002 in dienst getreden.

Het takenpakket van Joost bestaat uit het ontwikkelen aan Plato, het doen van onderzoek van forensische zaken en deelname aan diverse projecten.

Joost heeft onder andere gewerkt als deeltijd security specialist. Daarnaast heeft hij gedurende 2 jaar een eigen onderneming gehad in MKB-automatisering waarbij uitgebreid gebruik gemaakt werd van Linux.

Rens de Wolf
IT Security Specialist

Rens is sinds januari 2002 na een sabbatical van 6 maanden opnieuw in dienst getreden bij Fox-IT. Als afgestudeerd ingenieur in de informatiebeveiliging aan de TU Delft is hij voornamelijk medeverantwoordelijk voor de coördinatie en uitvoering van grootschalige beveiligingsaudits.

Daarnaast is hij betrokken bij diverse forensische onderzoeken en de ontwikkeling van hoogwaardige beveiligingsoplossingen.
Rens heeft in het verleden uitgebreide kennis opgebouwd van uiteenlopende systemen, netwerken en programmatuur op het gebied van ontwikkeling en beheer. Deze kennis brengt hij in de praktijk bij Fox-IT als IT Security Specialist.

Eric Cantineau
Sales Manager

Sinds 2 januari is hij in dienst bij Fox-IT als Sales Manager. De doelstelling voor 2003 is om de omzet van Fox-IT te verdubbelen. Zijn gedrevenheid ligt in het creëren van oplossingen die daadwerkelijk toegevoegde waarde hebben.

Eric heeft, na zijn studie HEAO BI,14 jaar ervaring op verschillende terreinen in de ICT, de laatste jaren vooral met CRM, Data Warehouse en Business Intelligence oplossingen en het verkopen ervan.

In zijn vrije tijd houdt Eric zich graag bezig met zeilen, golf en paragliding.

Nieuwe Opleiding Security & Hacking

In de vorige nieuwsbrief heeft Fox-IT aangekondigd bezig te zijn met de ontwikkeling van een nieuwe IT Security opleiding. In maart dit jaar is deze opleiding gestart onder de naam 'Security & Hacking'.

Fox-IT heeft een groot deel van zijn expertise en ervaring verwerkt in deze opleiding. De totale opleiding 'Security & Hacking' bestaat uit 5 modules: TCP/IP Techniek, Security, Hacking & Audits, IDS & Sporen, en Wetgeving. Bij elkaar nemen de modules 11 dagen in beslag. U bepaalt zelf welke modules uw interesse hebben en wanneer u deze modules wilt volgen.

De opleiding 'Security & Hacking' is een zeer praktijkgerichte opleiding geworden en zeer geschikt voor een ieder die werkzaam is in de IT sector, zoals netwerkbeheerders, systeembeheerders, technisch ontwerpers, applicatiebeheerders, helpdesk medewerkers en IT security medewerkers.

Er wordt veel gewerkt met hands-on opdrachten en testopstellingen. De deelnemers worden op deze manier in de gelegenheid gesteld om het volledige traject te doorlopen zoals een 'hacker' dat zou doen. Hierbij kunt u denken aan de verkenning, poortscans en het daadwerkelijk hacken van systemen.

Maar de opleiding gaat verder, tevens behandelen we wat u tegen deze hackers praktijken kunt doen om ze te voorkomen. Aan de orde komen werkstation- , netwerk-, en communicatiebeveiliging. Het 'zoeken' naar mogelijke indringers en de juridische consequenties hiervan vormen het sluitstuk van deze zeer complete opleiding.

Na afronding van de opleiding zal de deelnemer onder andere de kennis hebben om:

- de security architectuur te kunnen beoordelen;
- tools te kunnen gebruiken waar hackers mee werken;
- de aanpak en methodes die hackers gebruiken te begrijpen aanvallen te kunnen detecteren en analyseren.

In de agenda van deze nieuwsbrief treft u de data aan voor de opleidingen van Fox-IT. Meer informatie over deze opleiding kunt u vinden op onze website of u kunt contact opnemen met Fox-IT via training@fox-it.com.

Agenda 2003

- **3 en 4 april**
  Vervolg opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk
- **14 t/m 18 april**
  Basis opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk
- **5 mei t/m 9 mei**
  19 mei t/m 23 mei
  26 mei
  Opleiding 'Security & Hacking', module 1 t/m 5, Fox-IT, Rijswijk
- **21 mei**
  Seminar Managed Security Monitoring
- **2 juni t/m 6 juni**
  Basis opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk

Voor meer informatie over de opleidingen mail naar:
training@fox-it.com

Voor meer informatie over het seminar mail naar:
fox@fox-it.com

Fox-IT lanceert nieuwe PKI oplossingen

Daar waar het tot voor kort erg kostbaar en vooral lastig te implementeren was, heeft Fox-IT een 3-tal veilige, snel implementeerbare en prijstechnisch interessante PKI oplossingen gelanceerd.

Sterke authenticatie door middel van Public Key Infrastructure (PKI) oplossingen is op zich niet nieuw. Toch zijn de PKI projecten tot nu niet erg succesvol geweest. Hiervoor zijn 2 oorzaken aan te wijzen: Complexe, langdurige implementatie trajecten, met veel haken & ogen én PKI bleek prijstechnisch een erg kostbare oplossing. Hieraan maakt Fox-IT een einde door de lancering van 3 PKI oplossingen.

Allereerst MyPKI, een ASP oplossing, geschikt voor 1 tot enkele honderden certificaten. Vervolgens FOX-PKI: dé out-of-the-box oplossing, waarbij de klant alles zelf onder controle heeft, zelf de certificaten kan uitgeven onder eigen naam, binnen 3 maanden operationeel is en geschikt is vanaf enkele honderden tot tienduizenden certificaten. Tenslotte Maatwerk FOX-PKI: een schaalbare maatwerk oplossing, in 3 tot 6 maanden operationeel en geschikt voor specifiek maatwerk en om meer dan enkele miljoenen certificaten uit te geven.

Fox-IT heeft haar ervaring op dit gebied gebundeld in een draaiboek waardoor de klant direct profiteert van eerdere ervaringen en hierdoor snel en veilig PKI kan toepassen. Niet onbelangrijk: de Fox-IT PKI oplossingen kosten hierdoor een fractie van wat nu gebruikelijk is in de markt. Meer informatie: kijk op www.mypki.nl.

Colofon

Uitgave van Fox-IT Forensic IT Experts B.V.
Maart 2003

Redactie
Carlijn Wagemakers, e-mail pr@fox-it.com
Haagweg 137, 2281 AG Rijswijk ZH
Telefoon 070 - 336 99 99