Fox-IT
Forensic IT Experts

Nieuwsbrief 2

Februari 2002

Hoogwaardige beveiliging laptops

De afgelopen jaren heeft Fox-IT de reputatie opgebouwd veilige oplossingen exact op maat te maken. Dit is met name belangrijk voor opslag van zeer vertrouwelijke informatie, waarbij de gebruikers 'target' kunnen zijn van eventuele aanvallen.

De organisaties waar deze voorwaarden voor gelden hebben niet genoeg aan een basisbeveiliging, waarbij een serieuze aanvaller de mogelijkheid heeft bij de gegevens te komen door de beveiliging te kraken. Sommige gebruikers hebben zeer vertrouwelijke gegevens op laptops staan omdat zij deze altijd ter beschikking moeten hebben. Dit vormt echter wel een extra groot risico: de laptops komen dagelijks op straat en het risico van ontvreemding is dan vrij groot.

Speciaal voor dit type gebruiker realiseert Fox-IT beveiligingsconfiguraties die volledig voldoen aan de eisen van de gebruikers en aan extreme beveiligingseisen. De beveiliging bestaat uit verschillende lagen in combinatie met een USB-token. De oplossing biedt optimale veiligheid als de laptops zijn afgesloten, maar ook als tijdens gebruik een ontvreemding plaatsvindt. Het is voor een aanvaller niet mogelijk op welke manier dan ook bij de vertrouwelijke gegevens op de laptops te komen. Ook zijn speciale maatregelen genomen voor veilige communicatie tussen de gebruikers onderling.

Naar aanleiding van de ervaringen het afgelopen jaar, hebben dit jaar opnieuw verschillende organisaties de keuze gemaakt hun laptops door Fox-IT te laten beveiligen.

Opleiding

Gevorderde opleiding *Rechercheren op de Digitale Snelweg*

De opleiding *Rechercheren op de Digitale Snelweg* is al door velen met plezier gevolgd. Nu zijn ook de Gevorderde en de Vervolg opleiding *Rechercheren op de Digitale Snelweg* ontwikkeld.

Uit de evaluaties van de deelnemers aan de basisopleiding is gebleken dat voor een aantal mensen het instapniveau te laag is. Voor deze mensen biedt Fox-IT de gevorderde opleiding aan.

De gevorderde opleiding is een variant op de basisopleiding. De opleiding behandelt dezelfde stof als de basisopleiding plus een extra module over beveiliging. De onderwerpen worden in drie dagen in hoog tempo behandeld. Van de deelnemer wordt minimaal 3 jaar ervaring met het Internet verwacht. Ook moeten de deelnemers goed om kunnen gaan met Windows.

De vervolgopleiding *Rechercheren op de Digitale Snelweg* is een vervolg op de basis en gevorderde opleiding en is reeds aan verschillende groepen onderwezen. De evaluaties van de eerste twee vervolgopleidingen wezen echter uit dat hier en daar wat verbeteringen aangebracht kunnen worden. Daar zijn de ontwikkelaars van de opleiding gelijk opgedoken om een optimale opleiding te kunnen presenteren. Het resultaat is dat de deelnemers van de 'aangepaste' vervolgopleiding zeer tevreden zijn.

In dit nummer:

Fox-IT beveiligt internationaal netwerk ZyLAB

***'Na de totale netwerkreorganisatie door Fox-IT verlopen onze bedrijfsprocessen een stuk efficiënter'*, aldus Dr. Jan Scholtes, directeur van ZyLAB Technologies. ZyLAB heeft naast de hoofdvestiging in Amsterdam ook vestigingen in Spanje, Frankrijk, Verenigde Staten en Singapore. ZyLAB ontwikkelt zoek-software, die door de politie veel gebruikt wordt bij hun onderzoeken. ZyLAB beschikt over een team van specialisten, die over de hele wereld verspreid zijn. Toch ontwikkelen en vernieuwen zij gezamenlijk het product.**

ZyLAB®
The Paper Filing Company

'Voorheen maakten we veel gebruik van ISDN-lijnen', aldus Scholtes, 'maar de kosten daarvan rezen de pan uit. Daarom zijn we gaan zoeken naar een goedkopere en betere oplossing om de communicatie tussen de verschillende vestigingen efficiënter en veiliger te laten verlopen.'

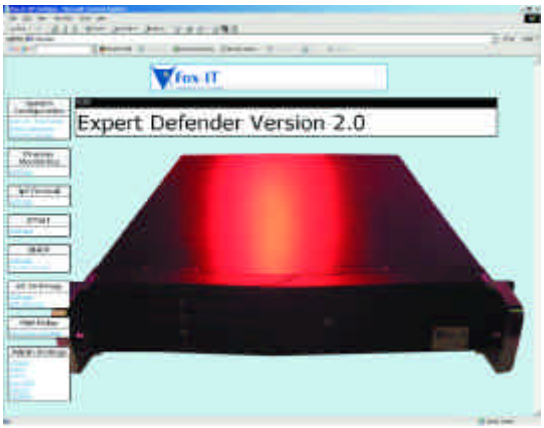
Door slim gebruik te maken van VPN-technologie worden de verschillende vestigingen nu onderling gekoppeld door middel van versleutelde tunnels via het Internet. *'Met deze operatie hebben we twee vliegen in één klap geslagen. We kunnen nu veel efficiënter samenwerken, en daarnaast zijn alle vestigingen nu voorzien van hoogwaardige firewalls. De kosten van deze operatie verdienen we binnen een half jaar makkelijk terug. Een aantal medewerkers heeft nu ook de mogelijkheid gekregen om thuis te werken. Zij gebruiken hiervoor USB-tokens met daarin alle sleutels die nodig zijn om toegang tot ons netwerk te krijgen.'*

De hoofdvestiging is voorzien van twee Expert Defender Firewalls op twee verschillende Internetaansluitingen. Omdat het bedrijf afhankelijk is van de VPN-verbindingen is gekozen voor een volledige redundante oplossing. De internationale vestigingen maken gebruik van de zeer prijsvriendelijke Netscreen firewalls. Thuiswerkers hebben PGP op hun laptop geïnstalleerd om veilig met collega's te kunnen samenwerken.

Firewall

Expert Defender Versie 2.0 gepland 1 maart 2002

Fox-IT heeft de release van de nieuwste versie van Expert Defender gepland staan op 1 maart 2002. Expert Defender is de door Fox-IT ontwikkelde firewall gebaseerd op het meest veilige operating system OpenBSD (www.openbsd.org).



In deze release is vooral aandacht besteed aan de koppeling van de firewall met ons Network Operations Centre. Door de nieuwe functies kan nog effectiever ingesprongen worden op de nieuwste dreigingen. Zo kan bijvoorbeeld, bij het bekend worden van een nieuw security probleem met de IIS - webserver van Microsoft, met één druk op de knop, een nieuw filter worden aangebracht op alle Expert Defender firewalls die zijn verbonden met het Network Operations Centre. Op deze manier kunnen we in de toekomst aanvallen zoals veroorzaakt door Code Red en Nimda blokkeren, zonder dat de klant op de patch van Microsoft moet wachten.

Over het algemeen zijn firewalls slechts in staat, om op basis van de header van ip-pakketten beveiligingen aan te brengen. Expert Defender kan daarnaast ook in de inhoud van de packets kijken om vast te stellen of deze gevaarlijke opdrachten bevatten. Op deze manier wordt het mogelijk om aanvallen gericht op servers zoals Microsoft IIS en Microsoft Exchange ook tegen te houden.

Voor de duidelijkheid nog even de belangrijkste features kort op een rij:

- Statefull packet filter
- Network Address Translation
- DHCP server
- HTTP/FTP Proxy
- Mail Relay
- Intrusion Detection System (Alleen in combinatie met aansluiting op het NOC)
- Content filtering (Alleen in combinatie met aansluiting op het NOC)

De meeste belangrijke settings kunnen worden uitgevoerd via een web interface. De geavanceerde opties kunnen op afstand door Fox-IT ingesteld worden.

NOC (Network Operations Centre)

Fox-IT levert een managed security oplossing in de vorm van een network operations centre (NOC). Dit NOC controleert de netwerken van haar klanten op mogelijke problemen op het gebied van veiligheid. Hackers, virussen en andere zaken kunnen voor veel problemen zorgen en veel kosten met zich meebrengen. Om het risico voor dit soort problemen te minimaliseren is het nodig om te zorgen dat de gebruikte systemen en software volledig up to date zijn en geen beveiligingsgaten bevatten.

Adequaat security management is noodzakelijk voor de veiligheid van de technische infrastructuur. Iedere week komen er wel nieuwe veiligheidsgaten aan het licht die gepatched moeten worden. Dit kost systeembeheerders veel tijd, die ze niet kunnen besteden aan het verhelpen van andere problemen. Daarom voert het NOC de beveiligingstaak 24 uur per dag 7 dagen per week uit. Deze beveiligingstaak houdt niet alleen monitoring in. Ook het direct patchen van de veiligheidsgaten valt onder de beveiligingstaak.

Het NOC maakt voor zijn klanten gebruikt van state of the art oplossingen om het netwerk veilig te houden. Het gebruikt toepassingen om de beschikbaarheid van het netwerk en de services te controleren. Het eventueel uitvallen van bepaalde netwerkservices die door een klant gebruikt worden, zoals bijvoorbeeld webservers of email servers zal dan ook gelijk gedetecteerd worden. Hierdoor kan de downtime van cruciale services geminimaliseerd worden alsmede de daarmee gekoppelde schade.

Een andere toepassing die door het NOC wordt gebruikt is intrusion detection. Binnen het netwerk van een klant wordt een Expert Defender 2.0 machine geplaatst samen met een intrusion detection sensor. Beide kunnen op afstand worden geconfigureerd. Door middel van de Expert Defender 2.0 kan op aanvraag van de klant een gedeelte van het netwerkverkeer worden geblokkeerd.

Het overige netwerkverkeer wordt door het intrusion detection systeem gecontroleerd op mogelijke aanvallen. Hackers kunnen worden gedetecteerd terwijl ze aan het hacken zijn en voordat ze grotere schade kunnen aanrichten. De Expert Defender 2.0 is er ook nog eens op gericht om de noodzaak voor patches te minimaliseren. Hierdoor hebben uw systeembeheerders meer tijd over voor de ondersteuning van uw echte bedrijfsactiviteiten.

Voor meer informatie kunt u contact opnemen met Ronald Prins, prins@fox-it.com.

Even voorstellen

Sinds 15 december 2001 ben ik in dienst getreden bij Fox-IT als Project Manager. Mijn taak bestaat vooral uit het, op professionele manier, projecten succesvol laten slagen. Hiervoor kan ik gebruik maken van mijn ervaringen onder andere als Projectleider bij een van de dochterondernemingen van Imtech, binnen het ICT cluster. Tevens heb ik ervaring opgedaan met het gebruik van de PRINCEII projectmanagement methode.

Ik heb Fox-IT leren kennen op 'The Internet Working Event 2001' die in de RAI gehouden werd. Wat me aansprak in de werkwijze van Fox-IT, is dat zij niet alleen ervaring heeft in het forensisch onderzoek, maar deze ervaring tevens benut voor het inzetten van diverse beveiligingsoplossingen voor haar klanten. De nieuwe dienst van Network Operations Centre is daar een logische aanvulling op.

Dat Fox-IT tenslotte daar waar mogelijk gebruik maakt van Open Source oplossingen juich ik van harte toe.

Matthijs van der Wel

Nieuwe telefoon-nummers Fox-IT

Fox-IT is een jong bedrijf dat nog steeds groeit. Niet alleen in aantallen medewerkers, ook het aantal relaties neemt toe. Een logisch gevolg hiervan is dat het telefoonverkeer toeneemt.

Daarnaast nemen steeds meer klanten diensten af van het Network Operations Centre (NOC). Om de bereikbaarheid van het NOC te verbeteren, is deze afdeling vanaf nu recht-streeks te bereiken voor klanten met een support contract

Deze maatregelen hebben tot gevolg dat Fox-IT voortaan onder andere nummers te bereiken is:

Algemeen	**015 - 219 1111**
Fax	**015 - 219 1100**
NOC (support)	**015 - 219 1199**

Vanzelfsprekend zijn wij nog steeds te bereiken op onze oude nummers. Dit zal echter vanaf 1 juli 2002 niet meer mogelijk zijn.

Agenda

- **7, 14, 21, 28 maart**
  Basis opleiding *Rechercheren op de Digitale Snelweg,* Den Haag
- **26, 27 maart**
  Vervolgopleiding *Rechercheren op de Digitale Snelweg,* Den Haag
- **8, 9, 15, 16, 22, 23 april**
  Basis politie opleiding *Rechercheren op de Digitale Snelweg,* Den Haag
- **7, 14, 21 mei**
  Gevorderde opleiding *Rechercheren op de Digitale Snelweg,* Den Haag
- **6, 13, 20, 27 juni**
  Basis opleiding *Rechercheren op de Digitale Snelweg,* Den Haag
- **19, 26 september, 3, 10 oktober**
  Basis opleiding *Rechercheren op de Digitale Snelweg,* Den Haag
- **10, 11 oktober**
  Infosecurity, Jaarbeurs, Utrecht

Enig idee, wat deze medewerker op het netwerk van onze klanten uitspookt?

Wij wel.

Fox-IT zoekt 2 IT-Security Specialisten (HBO/WO niveau)

Fox-IT is een jong en dynamisch bedrijf. Gevestigd in een karakteristiek pand in het centrum van Delft, werken we aan de IT-security van onze klanten. Dat doen we met zo'n 18 mannen en vrouwen in een gezellig team.

We bouwen aan eigen firewall en intrusion detection software op basis van OpenBSD. We monitoren 24 uur per dag de Internet-aansluitingen van onze klanten. We ontwikkelen permanent onze PKI software. We voeren penetratietesten uit en houden audits. We leren onze klanten hoe ze digitaal op het Internet moeten rechercheren. En mocht er ooit iets misgaan bij onze klanten, dan behoort forensisch onderzoek ook tot onze dienstenportefeuille.

Tot onze klanten rekenen we dan ook de overheid, diverse banken, verzekeringsmaatschappijen, accountantskantoren en multi-nationals.

Op de korte termijn is Fox-IT op zoek naar twee IT-Security Specialisten. In deze functie word je verantwoordelijk voor het implementeren en ontwikkelen van security oplossingen voor onze klanten. Tevens zal je worden ingezet voor het uitvoeren van forensische onderzoeken, audits en penetratietesten.

We verwachten van je dat je goede netwerkkennis hebt. Daarnaast heb je ruime ervaring met opensource unix omgevingen en heb je interesse om je verder te ontwikkelen op het gebied van beveiliging.

De medewerkers van Fox-IT zijn communicatief vaardig, Internet- en security-minded en dat verwachten we ook van jou.

Als de kernwoorden OpenBSD, PKI, VPN, Secure Email, en Managed Network Security je aanspreken, en je voldoet aan bovenstaand profiel, zien we graag je sollicitatie tegemoet. Kijk voor meer informatie over Fox-IT op http://www.fox-it.com en stuur je reactie naar prins@fox-it.com, t.a.v. Ronald Prins.

Colofon

Uitgave van Fox-IT Forensic IT Experts B.V.
Februari 2002

Redactie
Carlijn Wagemakers, e-mail pr@fox-it.com
Oude Delft 47, 2611 BC Delft
Telefoon 015 - 219 11 11

Opmaak en productiebegeleiding
NANS Communicatiemiddelen, Den Haag

Druk
Impressed Drukkerij, Pijnacker