Juni 2003

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

Fox-IT introduceert de Expert Vulnerability Scanner

Veel problemen die ontstaan door Trojans, wormvirussen en hack-aanvallen, zijn het gevolg van kwetsbaarheden in bepaalde systemen. Of het nu gaat om Microsoft Windows, Linux, Internet Information Server, Exchange, SQL-Server of Oracle. Om u te wapenen tegen nieuwe kwetsbaarheden, introduceert Fox-IT de Expert Vulnerability Scanner (EVS).

Zodra de zwakke plekken in een systeem bekend zijn, is er altijd wel een selecte groep kwaadwillenden die hiervan misbruik maakt. Daarentegen zijn er vaak wel al patches beschikbaar om de zwakke plekken te ondervangen. Deze patches zorgen ervoor dat een virus geen vrij spel krijgt. Helaas komt het nog regelmatig voor dat de patches niet tijdig geïnstalleerd worden. Met alle gevolgen van dien. Denk bijvoorbeeld aan de SQL-Slammerworm. De kwetsbaarheid en patch voor Microsoft SQL Server waren al een half jaar van te voren beschikbaar voordat de SQL-Slammerworm toesloeg. Toch werden er binnen een kwartier 75.000 servers besmet…

EVS
Met de EVS behoort dat probleem nu tot het verleden. De EVS is een appliance met daaraan een gekoppelde dienst. De EVS scant regelmatig het netwerk op kwetsbaarheden, nieuwe (nog onbekende) apparatuur en rapporteert welke security patches geïnstalleerd moeten worden. De EVS wordt geheel door Fox-IT onderhouden, zodat de vulnerability database altijd op orde is. Daarnaast maakt Fox-IT een rapportage om false positives te vermijden.

De combinatie van de Expert Vulnerability Scanner én een onderhoud & supportcontract is een goed middel om u te wapenen tegen nieuwe kwetsbaarheden!

Wet Elektronische Handtekening

Fox-IT levert Turnkey PKI Solution

Op 6 mei is de wet aangenomen die een juridische status geeft aan de elektronische handtekening. Dit betekent dat de elektronische handtekening onder een elektronisch document dezelfde status heeft als een handgeschreven handtekening voor een papieren document. De wet bepaalt aan welke eisen een elektronische handtekening moet voldoen om voldoende betrouwbaar te zijn. Fox-IT levert in een turnkey oplossing een Public Key Infrastructure (PKI) die nodig is om de elektronische handtekening te gebruiken.

Met de PKI Solution van Fox-IT kunnen organisaties zelf certificaten uitgeven waarmee een elektronische handtekening geplaatst kan worden. Daarmee is de aanpak van Fox-IT anders dan van andere PKI-aanbieders. Conform de eisen van PKI-overheid, kan de PKI Solution certificaten uitgeven onder het Root Certificaat van de Staat der Nederlanden. Hiermee worden documenten voorzien van een rechtsgeldige digitale handtekening.

Gebruikersvriendelijk
De PKI Solution is gebaseerd op open standaarden. Zij is compatibel met de gangbare standaarden en schaalbaar tot gebruik in omgevingen waarbij miljoenen digitale certificaten uitgegeven en beheerd moeten worden. Dit alles is conform de nieuwe Wet Elektronische Handtekening.
Met de PKI Solution wordt een oplossing geboden die snel in te zetten is. Vanzelfsprekend is er een stappenplan beschikbaar om PKI Solution te implementeren. De PKI Solution is zeer gebruikersvriendelijk en speciale eindgebruikers-software is dan ook niet nodig.
Al met al is de PKI Solution een kosteneffectieve oplossing die grote flexibiliteit biedt.

Traditionele audit blijkt onvoldoende

Bijna ieder theoretisch security model bestaat in grote lijnen uit onderstaande stappen. Zo worden eerst de bedrijfsdoelen bepaald, waar het (IT) securitybeleid op afgestemd wordt. Dit beleid wordt vervolgens vertaald naar concrete voorschriften (policies), waarna de IT-beheerders aan de slag gaan om de procedures en systemen aan te passen. Om te controleren of het securitybeleid nog wel aansluit bij de bedrijfsdoelen en of het beleid op juist wijze wordt uitgevoerd, vindt periodiek een audit plaats. Grote accountantskantoren en 'IT-Auditors' zijn inmiddels de gevierde uitvoerders van deze audits.

Normenkader

Bij de controle of het securitybeleid wel op een juiste wijze nageleefd wordt, vindt een toetsing van de systeeminstellingen en procedures plaats. Hierbij wordt het security beleid als normenkader gebruikt. Bij afwezigheid van een securitybeleid dient de 'Code voor Informatiebeveiliging' veelal als normenkader waaraan getoetst wordt. Een probleem met een dergelijk normenkader is echter de vraag of het normenkader zélf volledig is en of de genomen maatregelen en procedures voldoende bescherming bieden.

Hacker audit

Een goede hacker denkt namelijk 'out-of-the-box' en maakt vaak gebruik van een combinatie van diverse manieren om zijn of haar doel te bereiken. Het is daarom een welkome aanvulling om ook een ander soort audit te laten uitvoeren; namelijk een audit 'door de ogen van de hacker'. Waar een accountantskantoor of IT-auditor slechts genomen maatregelen en procedures vergelijkt met een gesteld normenkader, wordt bij een hacker audit gekeken naar de wijze waarop systemen en procedures al dan niet in combinatie te misbruiken zijn.
In de praktijk komt het erop neer dat bij een hacker audit - zonder een blik op het security beleid te werpen - (een deel van) het bestaande netwerk en de daarop aanwezige systemen en bijbehorende procedures, geanalyseerd worden. Hierbij wordt een correlatie tussen aangetroffen zwakheden gemaakt. Net zoals een hacker ook de combinatie van zwakheden weet uit te buiten en zich niet alleen beperkt tot de op zich zelfstaande aangetroffen zwakheden. Ook een codereview van de aanwezige scripts en een fysieke controle van de netwerkarchitectuur behoren tot de onderdelen van een hacker audit.
Verder kan op verzoek gekeken worden welke schade een kwaadwillende medewerker kan aanrichten. De

In de schoenen van de hacker:

Kick-off van de Opleiding 'Security & Hacking' groot succes!!!

Na een drukke periode van ontwikkelen en testen was het dan zover. In maart was de kick-off van de opleiding 'Security & Hacking' van Fox-IT. De training duurde twee weken en bestond uit zowel theorie als praktijkgerichte hands-on opdrachten. Onderwerpen als netwerkbeveiliging, hacken en IDS (security monitoring) zijn hierbij uitgebreid aan bod gekomen. De opleiding is een groot succes gebleken en vraagt dan ook om een vervolg.

De kandidaten hebben de geleerde theorie via diverse opdrachten in praktijk gebracht. Vooral het in de schoenen kruipen van een hacker is door de kandidaten als een van de hoogtepunten van de opleiding gezien. "Door de mogelijkheden van de vijand te leren kennen, leer je de vijand beter buiten de deur houden," aldus een van de deelnemers.
Dankzij de variëteit en de logische opbouw van de diverse modules, bleven de deelnemers enthousiast en hebben zij de totale opleiding als zeer nuttig ervaren.

Na een periode van evaluatie en 'fine-tuning' staat de volgende opleiding gepland voor september 2003.
Op onze website www.fox-it.com vindt u uitgebreide informatie over de inhoud van de diverse modules, de agenda en het inschrijfformulier.
Door de unieke opzet van deze opleiding kunnen de kandidaten zelf aangeven wanneer zij welke modules willen volgen.

'Security & Hacking' een Must voor security Nederland.

In de schijnwerpers

De kennis en ervaring die ik heb opgegaan aan de TU Delft en later bij het Nederlands Forensisch Instituut, waren een goed uitgangspunt voor mijn werk binnen Fox-IT. Als een van de eerste medewerkers ben ik begin 2000 mijn loopbaan bij Fox-IT begonnen als software-engineer. Mijn werkzaamheden bestonden onder meer uit cryptografische beveiliging van CD-ROMs voor gebruik in justitiële onderzoeken en forensisch onderzoek in uiteenlopende zaken.

Gaandeweg is mijn rol uitgegroeid en tegenwoordig ontwerp ik als security architect security oplossingen. De combinatie van een zeer hoog veiligheidsniveau met de wensen van de klant staan hierbij centraal. De ontwikkeling van Fox-PKI is hier een goed voorbeeld van. Deze efficiënte en praktische Public Key infrastructure is voor vier miljoen certificaten ingezet in het NOC*NSF Nederland Sportland Digitaal project. Maar ook het Plato

volgende stap in de hacker audit is de uitvoer van een penetratietest. Hierbij wordt daadwerkelijk getracht om systemen binnen te dringen en misbruik te maken van procedures.

Resultaat
Het resultaat van een hacker audit is een rapportage waarin de aangetroffen zwakheden in de netwerkarchitectuur, de onderdelen en de procedures staan vermeld. Tevens wordt advies gegeven hoe deze zwakheden ondervangen kunnen worden. Het is vervolgens aan de opdrachtgever van een hacker audit om dit rapport te vergelijken met het opgestelde security beleid en te bezien of de bedrijfsdoelstellingen niet in gevaar kunnen komen. In de praktijk blijkt dat bij een hacker audit vaak meer (ernstige) zwakheden aangetroffen worden dan bij een traditionele audit. De reden hiervoor schuilt in de andere manier van denken door de auditor. Waar in het laatste geval de auditor slechts een vergelijking tussen het gestelde normenkader en de uitvoering maakt, wordt bij een hacker audit getracht te denken als een aanvaller. Daarom alleen al is een hacker audit een welkome aanvulling op de reeds bestaande audits!

Ir. Jeremy Butcher

IDS systeem, dat binnen Fox-IT voorziet in de technische ondersteuning van het Managed Security Monitoring proces, geeft een aardig beeld van de security oplossingen die Fox-IT te bieden heeft.

Niet alleen vanwege het vooruitstrevende karakter van het werk bij Fox-IT blijf ik enthousiast. Ook de nauwe samenwerking met onderzoeksgroepen aan de TU Delft én de goede banden met de Open Source community (bijvoorbeeld te zien in onze aanpassingen aan het OpenBSD besturingssysteem) dragen ertoe bij dat ik nog lange tijd veel plezier denk te beleven bij Fox!

Jeremy Butcher

Seminar gaat 'De Firewall Voorbij'

Ir. Ronald Prins

Onlangs heeft Fox-IT het seminar 'De Firewall Voorbij' georganiseerd, dat plaatsvond in het Keringhuis in Hoek van Holland. Tijdens dit seminar kwamen Managed Security Monitoring (MSM) en Plato uitgebreid aan bod. Ronald Prins en Jeremy Butcher namen de presentatie van dit geavanceerde Intrusion Detection System (IDS) met het expertsysteem Plato voor hun rekening. Maar wat houden MSM en Plato nu eigenlijk in?

De meeste organisaties leggen de focus op preventieve maatregelen tegen virussen en hackers.
Voor elke dreiging bestaat wel een technische oplossing. Een systeem wordt echter onwerkbaar als je álle technische oplossingen inzet. Hier heeft Fox-IT een voordelige en effectieve oplossing voor: MSM.
MSM biedt detectie en respons op problemen in netwerkomgevingen.

MSM blijft alert
Bij MSM wordt door het Security Operations Center (SOC) gereageerd op verdacht verkeer (alerts). Het SOC bewaakt netwerken 24 uur per dag, zeven dagen per week en 365 dagen per jaar. Om te onderscheiden welke alerts daadwerkelijk een bedreiging vormen, is het expertsysteem Plato ontwikkeld. Plato is een grote verbetering ten opzichte van een 'gewone' IDS. Dit is vooral te danken aan de krachtige analyse, de kennis over netwerkomgevingen en de uitgebreide contextinformatie bij de verwerking van alerts.
Bekijk de presentaties op www.fox-it.com/seminar/ids.

Delicten aan het licht

Forensisch onderzoek in kaart gebracht

Al meer dan vier jaar voert Fox-IT gespecialiseerde digitale sporenonderzoeken uit. In deze periode zijn bijna honderd op zich zelf staande zaken behandeld. Tijdens deze onderzoeken is veel nieuwe kennis en ervaring opgedaan over de manieren waarop delicten worden gepleegd en over de (soms onverwachte) locaties waar digitale sporen worden gevonden. Deze specifieke kennis is veelvuldig toegepast in de digitale beveiligingsoplossingen die door Fox-IT worden gerealiseerd. Onlangs zijn de onderzoeken geïnventariseerd en daaruit is een aantal relevante conclusies getrokken.

Opvallend is dat een constante hoeveelheid aangeleverde zaken betrekking heeft op delicten als fraude en (kinder)porno.
Daarnaast vindt een stijging plaats op het gebied van bedrijfsspionage en hacking. Opvallend hierbij is dat bedrijfsspionage - net als fraude - vrijwel altijd met hulp van binnenuit gebeurt. Alleen bij de hackzaken komen de criminelen volledig van buiten de organisatie. De succesvolle hacks die plaatsvinden, slagen overigens meestal niet vanwege de hoge kwaliteit van de hacker, maar met name vanwege bekende aanwezige lekken binnen het veiligheidssysteem. Maar… De belangrijkste conclusie is wellicht dat de forensische experts van Fox-IT ruim negentig procent van de aangeleverde zaken oplossen!

Trend
Kijkend naar het onderzoek zelf, is daar eveneens een trend in waar te nemen. Fox-IT hanteert haar eigen methode die uit een aantal fasen bestaat en steeds technische en tactische handelingen onderscheidt. ▶

Vervolg pagina 3

Door de enorme toename van digitaal materiaal en de complexiteit van de onderzoeken is de tactische component in het onderzoek aanzienlijk toegenomen. In iedere fase zien we dat onze tactische vaardigheden de doorlooptijd van het onderzoek verkorten en de efficiëntie verbeteren.

Gemeengoed

Fox-IT verwacht dat het laten uitvoeren van digitaal sporenonderzoek in de toekomst meer gemeengoed zal worden bij de ontdekking van een mogelijk delict. In combinatie met de - overigens cruciale - tactische component gaat het oplossen van een delict regelmatig veel sneller dan de traditionele manier.

Uw PDA beveiligd tegen insluipers dankzij Safeboot

De ontwikkeling van de Personal Digital Assistant (PDA) gaat in rasse schreden voort. Zo wordt het interne geheugen steeds uitgebreider en worden de mogelijkheden van dit handzame apparaat met de dag groter. PDA's nemen dan ook steeds meer functies van de laptop over. Naast relatiebestanden, bevatten de PDA's van tegenwoordig ook spreadsheets en Worddocumenten gevuld met interne bedrijfsinformatie. Door het kleine formaat is de PDA echter wel extra gevoelig voor verlies of diefstal. Met Safeboot voorkomt u dat gevoelige informatie in verkeerde handen valt.

Safeboot maakt gebruik van het sterke encryptie algoritme AES met 256-bits versleuteling.
Een extra veiligheid is de optie om het geheugen van de PDA te overschrijven na een ingesteld aantal foute inlogpogingen.
Door de gegevens meerdere malen met willekeurige tekens te overschrijven, wordt het geheugen daadwerkelijk onleesbaar gemaakt.
De gegevens zijn dan niet meer te achterhalen. Eerder heeft Fox-IT al bij een groot aantal klanten in de publieke en private sector PDA's op deze manier beveiligd. Met Safeboot is uw PDA in 'veilige handen.'

Fox-IT draagt bij aan het boek 'Facetten van Fraude & Fraudebestrijding'

Recent publiceerde een aantal hoogleraren en specialisten het boek 'Facetten van fraude & fraudebestrijding'. Menno van der Marel, directeur van Fox-IT, heeft de digitale aspecten rondom fraude en beveiliging in dit boek uiteen gezet.

In het onderdeel 'Gebruiksgemak is de vijand van beveiliging: een waarschuwing van de digitale detective', gaat Menno onder meer in op de beveiligingsanalyse, het forensisch onderzoek en de informatiemaatschappij.
Maar ook repressie en preventie, digitale identiteit en de factor mens worden in dit onderdeel uitgebreid beschreven.
"Je kunt zoveel beveiligen als je wilt, maar de menselijke factor mag je nooit veronachtzamen," aldus Menno.

Daarnaast bevat het boek opstellen uit de juridische praktijk en politiek over de bestrijding van fraude. Gepleit wordt om fraudebestrijding uit de strafrechtelijke sfeer te halen en onder te brengen bij diensten die daar wel goed (of in elk geval beter) voor zijn toegerust.

Titel: "Facetten van Fraude & Fraudebestrijding"
(Forensische Studies Deel 11)
Auteur: mr. Gerard J.C.M.Bakker e.a.

Agenda 2003

- **1 t/m 5 september, 15 t/m 19 september en 22 september**
  Opleiding 'Security & Hacking', module 1 t/m 5, Fox-IT, Rijswijk
- **25 en 26 september**
  Vervolg opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk
- **29 en 30 september, 1 t/m 3 oktober**
  Basis opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk
- **7 oktober**
  Seminar Public Key Infrastructure
- **27 t/m 31 oktober, 10 t/m 14 november**
  Opleiding 'Security & Hacking', module 1 t/m 4, Fox-IT, Rijswijk
- **11 en 12 november**
  Infosecurity.nl, Jaarbeurs, Utrecht
- **24 t/m 28 november**
  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

Colofon

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

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