Fox-IT
Forensic IT • IT Security • Practical Training

Nieuwsbrief 3

Augustus 2002

Digitaal Forensisch Onderzoek

Digitaal Forensisch onderzoek is één van de basisgebieden waaruit Fox-IT is opgebouwd. In 1999 was Fox-IT het eerste en enige bedrijf gespecialiseerd in digitaal forensisch onderzoek. Vandaag de dag blijken digitale fraude en misdrijven met behulp van de computer aan de orde van de dag te zijn. Dit heeft grote gevolgen voor het digitale forensische onderzoek.

In 1999 waren zowel de misdaad als de rechtsgang niet op de hoogte van de mogelijkheden op het gebied van digitaal forensisch onderzoek. Indien digitaal bewijsmateriaal werd gevonden, was dit meestal meteen doorslaggevend. Tegenwoordig is de kennis op dit vakgebied breder ingebed. Zowel in de rechtsgang als in het criminele circuit zijn computers geen magische zwarte dozen meer. Daardoor worden steeds hogere eisen gesteld aan het uitvoeren van en rapporteren over forensisch onderzoek.

Het onderzoek moet compleet en correct verlopen. Bewijzen dienen op de juiste manier verzameld te worden, zodat er geen twijfel kan bestaan over de juistheid en de echtheid ervan. Hierdoor kunnen de experts van 'de tegenpartij' de bewijzen niet onderuit halen. De methode van forensisch onderzoek verdient daarom tot in details alle aandacht.

Fox-IT hanteert een door haar zelf ontwikkelde methode voor forensisch onderzoek. Deze bestaat uit het combineren van de ervaringen op strafrechtelijk gebied, binnen Justitie, met de civielrechtelijke ervaringen uit het bedrijfsleven. De methode wordt telkens aan de laatste (wettelijke) eisen en de ontwikkelingen aangepast en vervolgens toegepast. Hierdoor blijft de kans op het verliezen van relevante sporen minimaal en is het bij een contraonderzoek eenvoudig om controle uit te voeren op de werkwijze en op het verkregen bewijsmateriaal.
Fox-IT heeft een team met forensische onderzoeksspecialisten, dat continu bezig is om de onderzoeksmethode te verbeteren en de verkregen kennis toe te passen in de praktijk. Hierdoor kunnen de meest recente en meest innovatieve forensische delicten uitstekend door Fox-IT opgelost worden.

Fox-IT is verhuisd!

Op 5 juli 2002 is Fox-IT verhuisd naar een volledig gerenoveerde herenvilla aan de Haagweg 137 in Rijswijk. Een gebouw met bijna vijf keer zoveel vloeroppervlak. Op de bovenste verdieping is een complete trainingsruimte ingericht en er is extra parkeergelegenheid. Maar het allerbelangrijkste is dat Fox-IT u vanaf de nieuwe locatie nog beter van dienst kan zijn.
Tot ziens in Rijswijk!

Fox-IT Forensic IT Experts B.V.
Haagweg 137
2281 AG RIJSWIJK ZH

Telefoonnummer: 070 - 336 99 99
Faxnummer: 070 - 336 99 90

In dit nummer:

Fox-IT
Forensic IT • IT Security • Practical Training
Augustus 2002

Public Key Infrastructure: maak het eenvoudig en betaalbaar!

Public Key Infrastructure, oftewel PKI. Een paar jaar geleden was dit het toverwoord dat in ieder gerespecteerd computerblad stond. De PKI-oplossing zou een hoop problemen met e-mail en internet-gebruik oplossen. Door deze oplossing zou e-commerce een enorme vlucht nemen, dankzij PKI zou …. En toen werd het stil rond PKI.

Wat is er gebeurd?
Vanuit de aanbieders van de PKI-systemen, heerste de overtuiging dat, wilde de systemen goed werken, er veel en dure certificaten moesten worden aangeschaft door bedrijven en vaak ook nog op een omslachtige methode. De potentiele klanten van de PKI-systemen zagen dit echter niet zo zitten en het leek een zachte dood te sterven. En dat is jammer, omdat het idee achter PKI zeer goed is.

Wat is een PKI-toepassing en wat is een certificaat?
Kort gezegd zorgt een PKI-toepassing ervoor dat er op een veilige wijze elektronisch gecommuniceerd kan worden. Hiervoor heeft de gebruiker de beschikking over een certificaat. Dit certificaat, een klein tekstbestand, bestaat op haar beurt weer uit een soort sleutel, een publieke sleutel. Met behulp van de publieke sleutel kan een bericht versleuteld worden. Dat versleutelde bericht kan alleen met de bijbehorende privé sleutel van de ontvanger weer ontcijferd worden.

Trusted Third Party
De PKI leveranciers dachten dat het noodzakelijk was om, behalve het uitdelen van de certificaten, als extra dienst de identiteit van de eigenaar te controleren. Deze controle door een Trusted Third Party (TTP) zorgt ervoor dat de identiteit van iemand met een publieke sleutel met zekerheid wordt vastgesteld. Zo kan iemand met de publieke sleutel van bijvoorbeeld Jan de Groot met zekerheid zeggen dat het om Jan de Groot gaat. Deze identiteitscontrole is echter een dure zaak, waardoor de prijs van een certificaat behoorlijk hoog wordt.

Een andere werkwijze!
Het is niet altijd noodzakelijk om door een externe partij de identiteit van een gebruiker van een certificaat te laten controleren. Stel in een bedrijf of bij een vereniging wil men met eigen medewerkers communiceren. Dan zijn er voldoende andere, eigen, controlemiddelen ter beschikking. Door bijvoorbeeld gebruik te maken van de adresgegevens in de salarisadministratie, kan men ervoor zorgen dat het certificaat bij de juiste, gecontroleerde, gebruiker terechtkomt. Zo ook bij NOC* NSF. Daar is deze betaalbare en gebruiksvriendelijke PKI-werkwijze toegepast. (Zie pagina 4)

Even voorstellen

Even voorstellen…..

Fox-IT groeit en heeft drie nieuwe enthousiaste en vakkundige mensen aangenomen, welke we hierbij graag aan u voorstellen.

Eric Eekhof
IT-Security Specialist

Sinds 1 april 2002 in dienst bij Fox-IT. Zijn takenpakket is erg gevarieerd. Deelname aan diverse projecten, waaronder penetratietesten, forensische onderzoeken en ontwikkelprojecten. Daarnaast levert hij een bijdrage aan de Fox-IT Security Monitoring in de vorm van probleemanalyse en systeembeheer.
De werkervaring van Eric bestaat uit diverse jaren als systeemprogrammeur bij een gerenommeerd internet bedrijf.

Casper Aleva
IT-Security Specialist

Is op 1 mei 2002 begonnen bij Fox-IT en is medeverantwoordelijk voor het uitdenken en bouwen van security oplossingen op het gebied van de Public Key Infrastructure. Daarnaast is het zijn taak om een kritische factor te zijn bij het reviewen van security-concepten en -systemen.
Casper is gedetacheerd geweest bij verschillende bedrijven.
Van banken tot internet service providers, waar hij onder andere heeft gewerkt als UNIX-beheerder en security engineer. Door in korte tijd kennis te maken met veel bedrijven en systemen heeft Casper veel ervaring van de verschillende kanten van Informatie Technologie.

Rob van Boxtel
Docent Practical Training

Is op 1 mei 2002 begonnen als docent. Rob is verantwoordelijk voor het up to date houden, het organiseren en het geven van de huidige trainingen. Tevens is een belangrijk onderdeel van zijn functie het bewaken van nieuwe mogelijkheden op het gebied van security, hacken & audits en sporenonderzoek, om deze ontwikkelingen vervolgens om te zetten naar opleidingen.
De werkervaring van Rob is zeer breed. Hij heeft een didactische opleiding genoten aan de sportacademie in Den Haag en heeft daarna enkele jaren in de IT branche gewerkt als onder andere netwerkbeheerder en IT-Security specialist.

Fox-IT
Forensic IT • IT Security • Practical Training
Augustus 2002

In iedereen schuilt een hacker!

Nieuwe IT-Security opleiding
Op basis van signalen uit de markt is Fox-IT een nieuwe IT-Security opleiding aan het ontwikkelen. Deze nieuwe opleiding, speciaal voor 'security minded' Nederland, is dé opleiding die vragen beantwoordt op het gebied van hacken, intrusion detection (security monitoring) en forensisch onderzoek.

De opleiding is uit een aantal modules opgebouwd en duurt, afhankelijk van welke modules u kiest, tussen de vier en tien dagen. Tijdens de opleiding wordt gewerkt met veel praktijkgerichte hands-on opdrachten waarbij de deelnemer onder meer zelfstandig leert systemen te hacken.

De focus van de opleidingsmodules ligt aan de ene kant op de manier waarop (kwaadwillende) hackers doelbewust IT-systemen compromitteren. Aan de andere

kant ligt de focus op het onderzoeken op welke wijze dit heeft kunnen plaatsvinden, wie de daders zijn en het achterhalen welke schade is aangericht.

De totale opleiding is onder te verdelen in drie hoofdmodules:
1. Security technieken, waaronder firewalls, cryptografie en smartcards.
2. Hacken & audits.
3. Intrusion detection system & forensisch sporenonderzoek.

Deze opleiding staat gepland voor eind 2002 en begin 2003.

Wilt u op de hoogte blijven van de ontwikkeling van deze nieuwe opleiding, surf dan naar www.fox-it.com/opleiding.

Rechercheren op de Digitale Snelweg
Ook de succesvolle Fox-IT opleiding 'Rechercheren op de Digitale Snelweg' wordt in het vierde kwartaal weer enkele malen gegeven. In de agenda van deze nieuwsbrief treft u de data aan voor deze opleiding.
Meer informatie over deze opleiding kunt u vinden op de website www.fox-it.com of neem contact op met onze docent Rob van Boxtel, boxtel@fox-it.com.

Plug & play

Fox-IT ontwikkelt de plug & play appliance voor PKI

Een van de producten waar Fox-IT momenteel hard aan werkt is een zogenaamde PKI-AAA appliance, gebaseerd op OpenSource software.

De appliance
Met deze plug & play appliance kunnen klanten een Public Key Infrastructure in hun netwerk introduceren waarbij de nadruk ligt op de AAA-services: Authenticatie, Autorisatie en Accounting. Er worden digitale certificaten gebruikt in plaats van username en password. Door te werken met een appliance, waarin PKI technologie is ingebouwd en geoptimaliseerd, worden veel van de huidige problemen weggenomen.

Snel
Als klant hoeft u zich niet meer te verdiepen in de installatie en de configuratie van complexe PKI technologie. Met de PKI-AAA appliance heeft u binnen één dag een werkend systeem inclusief uw eigen Certificate Authority waarmee u direct aan het werk kunt. Uiteraard is dit gebaseerd op de laatste PKI standaarden en is het compatibel met de gangbare E-mail applicaties en webbrowsers.

Fox-IT streeft ernaar om deze appliance eind van dit jaar klaar te hebben. Wilt u meer weten over deze appliance en de mogelijkheden ervan? Neem dan contact op met Ronald Weber of e-mail naar weber@fox-it.com.

Fox-IT
Forensic IT • IT Security • Practical Training
Augustus 2002

Nederland Sportland Digitaal

Binnenkort gaat de eerste proef in het ambitieuze project 'Nederland Sportland Digitaal' van start. Dit is een communicatieplatform van het NOC*NSF waarmee sportbonden en sportverenigingen met elkaar elektronisch kunnen communiceren. Het doel is dat uiteindelijk 4,3 miljoen sporters van dit elektronische platform gebruik kunnen maken. En voor elektronische communicatie is een PKI uitermate geschikt.

Grootste PKI-toepassing

Fox-IT levert voor dit platform de grootste PKI-toepassing van Nederland. Hierbij pakt Fox-IT de zaken anders aan dan gebruikelijk is in de markt. Het is zowel betaalbaar als gebruiksvriendelijk!

Registration en Certification Authority

Voordat een sporter of een bestuurder van een sportvereniging van het elektronische platform gebruik kan maken, heeft men een geldig certificaat nodig. Om dit certificaat te verkrijgen, surft de potentiële gebruiker naar de website van 'Nederland Sportland Digitaal'. Hier voert de sporter zijn gegevens in en wordt automatisch een certificaat gegenereerd. Er worden twee sleutels aangemaakt, een privé en een publieke sleutel. De privé sleutel, het geheime gedeelte van het certificaat, verlaat nooit de PC van de gebruiker en de publieke sleutel, wordt automatisch opgestuurd naar het NOC*NSF. Bij het NOC*NSF controleert de zogenaamde Registration Authority de aanvraag voor het certificaat en als deze juist wordt bevonden, ondertekent de Certification Authority digitaal de publieke sleutel. Vervolgens stuurt de Certification Authority een brief naar de aanvrager met hierin de instructies hoe deze zijn ondertekende certificaat met zijn browser kan ophalen.

Eureka

Doordat het NOC*NSF zelf de identiteit van haar sporters kan controleren, deze staan immers in de diverse ledenbestanden vermeld, worden de dure kosten van een Trusted Third Party voorkomen. Op deze manier kan het NOC*NSF op een eenvoudige en snelle wijze beschikken over een uitgebreide PKI. Door deze toepassing van Fox-IT kunnen op korte termijn alle sportbonden –verenigingen en alle leden betrouwbaar, snel en betaalbaar met elkaar communiceren.

Agenda 2002

- **10, 11 oktober**
  'Infosecurity.nl', Jaarbeurs, Utrecht
- **28, 29 oktober**
  ''Digitaal Rechercheren; Criminaliteit… Toekomst vandaag, blik op morgen!', Nederlands Congres Centrum, Den Haag.
- **4, 5 november**
  Vervolgopleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk
- **7, 14, 21 november**
  Gevorderde opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk
- **11, 12, 18, 19, 25, 26 november**
  Basis politie opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk
- **2, 3, 9, 10 december**
  Basis opleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk

Infosecurity

Infosecurity.nl

Op 10 en 11 oktober 2002 vindt in de Jaarbeurs te Utrecht de Infosecurity.nl plaats.

De Infosecurity.nl is de gelegenheid bij uitstek om inhoudelijk op de hoogte te blijven van trends en productontwikkelingen. Tevens worden adviezen gegeven over informatiebeveiliging binnen een bedrijf.

Ook dit jaar is Fox-IT aanwezig op de Infosecurity.nl. Hier informeren en demonstreren wij onze bezoekers onze nieuwste producten waaronder Security Monitoring en de nieuwe PKI-appliance.

U bent van harte welkom om een bezoek te brengen aan de stand van Fox-IT. Wij hebben een aantal toegangskaarten beschikbaar. Heeft u interesse, surf dan naar www.fox-it.com/beurs.

Let wel, op = op!

Graag zien we u op de de Infosecurity.nl 2002.

Colofon

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

Redactie
Carlijn Wagemakers, e-mail pr@fox-it.com
Haagweg 137, 2281 AG Rijswijk ZH
Telefoon 070 - 336 99 99
Carin van Alst, 5xP Marketing & Communicatie

Opmaak en productiebegeleiding
NANS Communicatiemiddelen, Den Haag

Druk
Drukkerij ImPressed, Pijnacker