Fox-IT NIEUWS

Juni 2004

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

Evenementen

Fox-IT op Cebit 2004

Tijdens de Cebit 2004, de grootste ICT-vakbeurs ter wereld, was Fox-IT voor het eerst present. Op het Holland Paviljoen stond Fox-IT met nog een aantal toonaangevende bedrijven in de Security Hal.

Fox-IT heeft op deze beurs voornamelijk de producten Managed Security Monitoring (MSM) en Sec-ID gepromoot. Sec-ID is, zoals eerder in de Fox Nieuwsbrief is toegelicht, de ASP variant van de FoxPKI appliance. Recentelijk heeft Fox-IT het aanbod in MSM uitgebreid, zodat een hoog security niveau geboden kan worden voor het bewaken van alleen de internetverbinding en/of een Demilitarized Zone (DMZ) tot het volledig monitoren van de totale infrastructuur van een multinational, meer hierover leest u op www.fox-it.com/msm.

Door deelname aan het Cebit 2004 heeft Fox-IT haar internationale stap gemaakt en de contacten zijn veelbelovend.

Forensic IT

Rechercheonderzoek in al zijn facetten

Forensic IT is één van de bedrijfsonderdelen waar Fox-IT vijf jaar geleden mee begon is. In eerste jaren hebben we vooral digitale sporenonderzoeken en data recovery zaken uitgevoerd. Fox-IT werd voornamelijk ingeschakeld wanneer de opdrachtgever geen andere uitweg meer zag dan de toedracht van het delict via digitale waarheidsvinding op te lossen.

Tijdens dit soort onderzoeken blijkt vaak dat digitale waarheidsvinding veel informatie oplevert, maar om de zaak volledig op te lossen, dienen koppelingen te worden gemaakt met de fysieke wereld. Uiteindelijk moeten één of meerdere personen aangewezen worden die verantwoordelijk zijn voor de delicten.

Fox-IT heeft zich de afgelopen jaren toegespitst op het maken van deze koppelingen. Hierdoor zijn we ons meer gaan bezighouden met de overige facetten van een rechercheonderzoek, waaronder bijvoorbeeld het afnemen van interviews, het uitvoeren van observaties en het doen van tactische analyses.

In 2003 heeft Fox-IT uitgebreid geïnvesteerd in het opzetten van de recherchetak waarbij alle facetten van rechercheonderzoek aandacht krijgen. Een tiental medewerkers zijn momenteel reeds opgeleid als algemeen particulier onderzoeker en tactisch rechercheurs zijn aangetrokken om op dat gebied de nodige professionaliteit en ervaring aan onze klanten te bieden.

Vervolg op pagina 2

Vervolg van pagina 1
'Rechercheonderzoek in al zijn facetten'

Het forensische bedrijfsonderdeel van Fox-IT is dus uitgegroeid tot een volledige particuliere recherchetak, waarbij de digitale sporen altijd bijzondere aandacht blijven verdienen, maar de traditionele recherchetaken mogen niet over het hoofd worden gezien. Meerdere malen is gebleken dat ook de traditionele taken, zoals observatie en informatievergaring, met nieuwe digitale snufjes wel erg slim en accuraat kunnen worden uitgevoerd.

Recherchemethoden en -technieken

Rechercheren, volgens *Van Dale Hedendaags Nederlands* de **'naspeuring van ongeoorloofde handelingen'**, kan op vele manieren plaatsvinden. De meest bekende recherchetechnieken die worden ingezet, zijn de zogenaamde traditionele rechercheteknieken. Denk hierbij aan statische en dynamische observatie, het houden van interviews en dactyloscopisch (vingerafdruk) onderzoek.

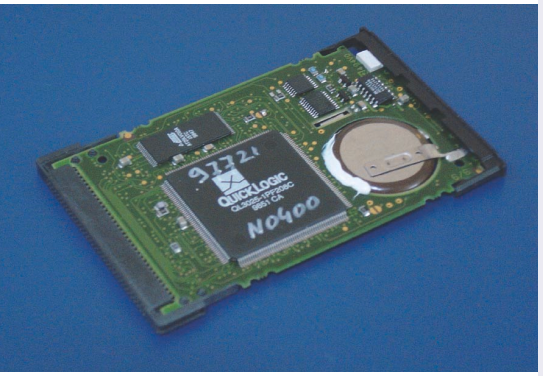
Naast deze onderzoeksmethoden en technieken, die Fox-IT inzet om bewijsvoering te verzamelen, is Fox-IT gespecialiseerd in het toepassen van digitale technieken ter ondersteuning en verbreding van de traditionele recherchemethoden en -technieken. Minder bekend maar daarom niet minder effectief! Zo zien we bij Fox-IT dat we met behulp van deze nieuwe digitale technieken vaak sneller en met meer zekerheid tot waarheidsvinding kunnen komen.

Een paar waargebeurde praktijkvoorbeelden geven een indruk van de toepassing van de combinatie van digitale en traditionele recherchemethoden en -technieken. De namen zijn om privacyredenen gewijzigd.

De directeur van een internationale onderneming ging twee weken op welverdiende vakantie, zijn zaak achterlatend in de handen van Bas, zijn eerste medewerker. Bij terugkomst van vakantie miste de directeur echter een aanzienlijk bedrag van zijn bankrekening en Bas. Forensisch onderzoek wees uit dat Bas een groot aantal luxe goederen bij een leverancier had besteld en met een nagemaakte handtekening van de directeur hiervoor betaald had. Fox-IT onderzocht de PC waarop Bas al die tijd had gewerkt en achterhaalde dat Bas met de leverancier samenwerkte en dat het geld rechtstreeks van de leverancier naar de bankrekening van Bas was doorgesluisd, minus een leuke commissie voor de leverancier. Verder achterhaalde Fox-IT de huidige verblijfplaats van Bas en kon de schade verhaald worden.

Sandra werd al langer lastig gevallen via de telefoon en e-mail. Wie haar geheime aanbidder was, bleef echter onduidelijk. Sandra schakelde een particulier recherchebureau in welke op haar beurt Fox-IT om assistentie vroeg. Fox-IT stuurde een zogenaamd uitlok e-mailbericht naar de stalker. Hiermee kon Fox-IT de verblijfplaats achterhalen. In dit geval bleek de staker zich in een internetcafé in het buitenland te bevinden. Via de openbare webcam van het internetcafé kon een foto van de stalker worden gemaakt, geen onbekende voor Sandra! Met deze foto en de rapportage van Fox-IT kon de stalker een halt toegeroepen worden.

Uit deze voorbeelden blijkt dat Fox-IT vakkundig recherchemethoden- en technieken hanteert en gedegen specialistische ervaring heeft met de inzet van digitale hulpmiddelen voor het vinden van sporen ter ondersteuning en voorbereiding op de rechtsgang.



Fox Crypto

Fox Crypto

Gespecialiseerd in hardwarematige encryptie

Eind vorig jaar heeft Fox-IT encryptietechnologie over genomen van Philips Crypto B.V. Hiermee maakt Fox-IT haar oplossingen op het gebied van digitale beveiliging compleet. Met de start van Fox Crypto, is Fox-IT in staat om haar huidige beveiligingsoplossingen uit te breiden met eigen cryptografische hardware tot op het hoogte niveau: beveiliging van staatsgeheimen.

Technisch betekent dit dat de applicaties, zoals bijvoorbeeld harddiskbeveiliging en VPN's, voor de versleuteling en ontsleuteling van informatie gebruik

maken van speciale hardwaremodules. Deze hardware neemt de versleuteling voor zijn rekening, welke normaal gesproken is opgenomen in software. Verder is de hardware in staat documenten en bestanden te ondertekenen, waardoor wijzigingen aan deze bestanden bij een controle zichtbaar worden.

De opzet van het encyptieproces is gelijk aan die in software. Het grote verschil is echter dat hardware niet gevoelig is voor mutaties door bijvoorbeeld een virus of een hacker. Wanneer een hacker een softwarepakket aanvalt, kan deze bepaalde onderdelen ervan uitschakelen, anders laten werken of zelfs naar buiten brengen. Deze informatie kan bijvoorbeeld sleutelmateriaal zijn.

Hardware gaat hier anders mee om. Het is niet mogelijk hardware bewerkingen te laten uitvoeren waarvoor het niet gemaakt is. Software kan uiteindelijk elke functie vervullen die gewenst is, maar ook die ongewenst is. De hardware is beperkt tot de nodige functionaliteit, maar zal bijvoorbeeld nooit sleutelmateriaal kunnen laten zien, omdat dit niet nodig is voor de normale werking. Door gebruik te maken van haar eigenschappen kan met behulp van cryptografische hardware een informatiebeveiligingssysteem zichzelf controleren op wijzigingen.

De start van Fox Crypto heeft ook een aanzienlijke organisatorische impact voor Fox-IT. De beveiligingsmaatregelen binnen Fox-IT zijn verder aangescherpt. Zowel procedureel als fysiek is een aantal belangrijke aanpassingen doorgevoerd. Daarnaast worden voortaan alle werknemers van Fox-IT uitgebreider gescreend. Een bijkomend voordeel is, dat er tijdens andere projecten die Fox-IT uitvoert, meegeprofiteerd wordt van dit extra niveau van vertrouwen.

Fox Updates

Extra beveiligde co-locatie voor klanten van Fox-IT

Fox-IT beschikt momenteel over twee serverlocaties: de interne serverruimte in het kantoorpand te Rijswijk en een externe ruimte in Amsterdam. De externe ruimte is recent verhuisd naar een extra beveiligde ruimte bij Redbus in Amsterdam. Deze ruimte is gekozen omdat, naast een zeer goede Internet connectivity, stroomvoorziening en redundancy, een hoge mate van fysieke beveiliging kon worden gerealiseerd.

Fox-IT beschikt nu over haar eigen serverkasten in een apart af te sluiten ruimte. Hiermee kunnen we onze klanten met hoogwaardige eisen met betrekking tot hosting, naast onze digitale beveiliging, ook een hoge mate van fysieke beveiliging bieden.

Even voorstellen ...

Boi Sletterink
IT Security Specialist

Sinds 1 december 2003 is Boi in dienst bij Fox-IT. Hij is mede verantwoordelijk voor het uitvoeren van security audits, code reviews en hij neemt deel aan ontwikkelingsprojecten. Zo levert hij een belangrijke bijdrage aan Plato, het expertsysteem voor Managed Security Monitoring. Daarnaast heeft hij zojuist het systeem van BEEP! verbeterd, zoals beschreven staat in het artikel over BEEP! in deze nieuwsbrief. Boi heeft na het afronden van zijn studie Informatica brede praktijkervaring opgedaan op het gebied van programmeren, security- en systeembeheer in diverse projecten aan de TU Delft.

Bas de Wit
Elektrotechnicus

Sinds eind november 2003 is Bas de Wit in dienst bij Fox-IT. Hij houdt zich bezig met de hardware die ontwikkeld en geproduceerd wordt voor en door Fox Crypto. Zijn achtergrond is de opleiding Elektrotechniek aan de HTS te Alkmaar en vervolgens aan de Technische Universiteit te Delft.

Naast de werkzaamheden voor Fox Crypto houdt Bas zich ook bezig met een aantal maatwerk hardware-oplossingen die bij de forensische onderzoeken van Fox-IT gebruikt worden, bijvoorbeeld voor het verbeteren van observatiemogelijkheden.

Hilde Willems
Management Assistent

Sinds 22 maart 2004 is Hilde werkzaam bij Fox-IT. Na haar opleiding Arbeidszaken/personeelsbeleid heeft ze bij een drietal bedrijven gewerkt als receptioniste, financieel medewerkster en management assistent.

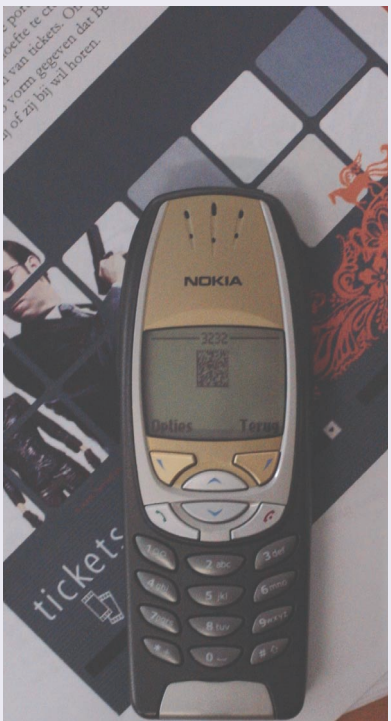
Hilde is bij Fox-IT mede verantwoordelijk voor de afdeling Office Management en zal tevens een deel van de boekhouding voor haar rekening nemen.

IT Security

BEEP! veiliger en flexibeler dankzij smartcardtechnologie

Nooit meer een uur van te voren je reservering ophalen. Bij enkele bioscopen en evenementen in Nederland is het al mogelijk: kaartjes bestellen via Internet en deze via SMS naar je mobiele telefoon laten versturen.

BEEP! is een veelbelovend innovatief systeem voor elektronische kaartverkoop. Door een slim ontwerp kunnen kaartjes vanaf een mobiele telefoon of papier eenvoudig met een scanner gelezen en op echtheid gecontroleerd worden. Een cruciaal onderdeel van dit systeem is de beveiliging rondom deze digitale kaartjes. Mogelijk misbruik van een dergelijk nieuw systeem moet tot een minimum beperkt worden.



Bostec heeft Fox-IT ingeschakeld om het beveiligingssysteem van BEEP! te vervolmaken door gebruik te maken van digitale handtekeningen op basis van smartcards.

Het grote voordeel van BEEP! boven concurrerende elektronische kaartjessystemen is dat de controle geheel decentraal plaatsvindt. Er is geen verbinding met een centrale database nodig om te kijken of een kaartje geldig is, een scanner onthoudt uitsluitend welke kaartjes al gebruikt zijn. Kopiëren heeft dus geen zin, maar de lokale controle dient wel waterdicht te zijn. Bij de bioscopen waar het systeem in productie is, staat een scanner die het kaartje in de vorm van een matrixcode direct van je display kan lezen. Voor evenementen wordt een mobiele toepassing in de vorm van een koffer toegepast.

BEEP! had in eerste instantie een beveiliging met een cryptografische oplossing in de software. Door de aanpassingen van Fox-IT gaan de nieuwe systemen op locatie nu gebruik maken van een smartcard voor het controleren van de digitale handtekeningen, waarbij de sleutels nooit van de smartcard komen. Hierdoor is het vrijwel uitgesloten om met het systeem te frauderen.

De combinatie van de decentrale controle en het gebruik van smartcards met digitale handtekeningen maken BEEP! bij uitstek geschikt om grootschalig toe te passen met een hoge mate van beveiliging.

Explosieve stijging Security Audits

In het afgelopen jaar is Fox-IT onverwacht geconfronteerd met een stijging van informatiebeveiliging auditopdrachten. Ten opzichte van 2002 is deze groei bijna 300%. Vooral voor de industrie en de overheid zijn grote audits, penetratietesten en code reviews uitgevoerd. Waar komt deze toename vandaan?

Al jaren laten bedrijven informatiebeveiligingaudits uitvoeren. Zo op het eerste gezicht zijn er niet veel redenen die een dergelijke stijging kunnen verklaren. Maar wellicht moet verklaring gezocht worden in een combinatie van verschillende ontwikkelingen in de markt. De volgende signalen zijn hierbij van belang:

- Het aantal virussen en wormen is opnieuw toegenomen en heeft harder toegeslagen het afgelopen jaar.
- Organisaties die niet direct vertrouwelijke informatie verwerken, zien in dat informatiebeveiliging ook voor hen essentieel is.
- De media hebben het onderwerp informatiebeveiliging serieus opgepakt.
- Het aantal processen dat wordt gedigitaliseerd, stijgt.
- Ondanks de traditionele audits blijven de problemen toenemen. De informatiesystemen worden technisch complexer waardoor meer technische diepgang noodzakelijk is.
- Naast de bekende problemen als hackers, virussen en wormen zijn steeds meer traditionele delicten die digitaal plaatsvinden. Denk aan bedrijfsspionage, vervalsing en fraude.

Ook in 2004 is deze trend van het toenemende aantal serieuze informatiebeveiligingaudits doorgezet. In het eerste half jaar van 2004 zullen auditers en penetratietesters van Fox-IT geen moment stil zitten.

Nieuw samenwerkingsverband met Security Counsellor Group

Experts hebben elkaar gevonden: Security Counsellor Group (SCG) en Fox-IT werken samen bij het oplossen van de beveiligingsproblemen van hun van de klanten.

Aangezien Fox-IT steeds complexere en grotere informatiebeveiligingstrajecten uitvoert, groeit daarmede tevens de behoefte aan ondersteuning bij het adviseren van onze klanten op het gebied van bijvoorbeeld crisismanagement, dreigingprofilering, diefstalpreventie en terrein- en gebouwbeveiliging. Security Counsellor Group (SCG) is een onafhankelijk adviesbureau voor TSM® (Total Security Management) met een bewezen reputatie in het efficiënt en (kosten)effectief oplossen van beveiligingsproblemen.

Door het in samenwerkingsverband aanbieden van beide specialismen zijn SCG en Fox-IT in staat hun klanten strategisch, tactisch en operationeel ondersteunen van hun klanten, bij zowel het ontwikkelen als het uitvoeren van hun beveiligingsbeleid.

Website SCG:
www.securitycounsellor.com

SECURITY COUNSELLOR GROUP
full security service

Frans Serré, Directeur SCG

ANWB

ook veilig op de digitale snelweg

Iedereen kent de ANWB van de hulp langs de weg. Om dit goed te kunnen doen, wordt steeds meer gebruik gemaakt van een complexe ICT-infrastructuur. Vooral in de zomermaanden wordt van de hulpverleningsorganisatie verwacht dat hun alarmcentrale met dezelfde zekerheid reageert als een politiemeldkamer. Daarnaast beschikt de ANWB over de grootste ledenbestand van alle verenigingen in Nederland.

Om er voor te zorgen dat de belangrijke diensten ongestoord door kunnen draaien, huurt de ANWB regelmatig de security experts van Fox-IT in. Bij de nieuwe IT-projecten voert Fox-IT audits uit en op dit moment wordt hard gewerkt aan de structurering van het informatiebeveiligingsbeleid.

"Fox-IT helpt ons bij het veiligheid houden van onze digitale snelweg. Hun security consultants zijn goed in staat om ons van adviezen te voorzien die enerzijds recht doen aan het open karakter van de ANWB als vereniging en anderszijds zorgen dat de netwerken afgeschermd blijven voor buitenstaanders", aldus Rein van der Oever directeur van het ANWB Facilitair Bedrijf.

Toename van het aantal virussen en wormen

De afgelopen vier maanden zijn meer dan honderd virussen verschenen. De originaliteit van deze virussen is echter ver te zoeken. Bijna alle virussen zijn varianten van één van de volgende vier moedervirussen: Netsky, Bagle, Sasser en MyDoom.

Van deze virussen zijn tientallen varianten gemaakt. Dit kan duiden op een zeer actieve virusschrijver, maar het is logischer om te veronderstellen dat er samenwerking plaatsvindt. Onlangs is de auteur van de Sasser-worm opgepakt. Terwijl hij achter slot en grendel zat, verscheen echter een nieuwe Sasser-variant op het Internet. Zo vermoedt het antivirusbedrijf F-secure, dat achter het Netsky-virus zelfs een hele groep Russsische hackers zit.

Het creëren van nieuwe virussen is tegenwoordig ook niet meer zo ingewikkeld. Op diverse websites, zoals bijvoorbeeld www.metasploit.org, wordt een raamwerk aangeboden waarin programmeurs stukken software kunnen plaatsen die bepaalde kwetsbaarheden uitbuiten. Een andere site is die van de groep K-otic: www.k-otik.com/exploits. Zij biedt op haar website een aantal volledig werkende proof-of-concept exploits aan. Het is dan slechts een knip- en plak-oefening om een nieuw virus te maken dat gebruik maakt van een nieuwe kwetsbaarheid.

De enige creativiteit die een virusschrijver moet hebben, is om te bepalen wat er met een geïnfecteerde PC moet gebeuren. Die creativiteit is overigens op dit moment meestal ver te zoeken. De PC's worden vaak ingezet om netwerken of servers plat te leggen (DDoS) of om spam mee te versturen.

Door de verhoogde samenwerking van virusschrijvers in combinatie met de verbeterde beschikbaarheid van informatie over bekende beveiligingslekken, ontstaat er meer kans op beveiligingsproblemen. Naar aanleiding van deze ontwikkelingen valt te verwachten dat er in de nabije toekomst meer aanvallen zullen komen die toegespitst zijn met een specifiek doel. Denk hierbij aan aanvallen tegen een specifieke organisatie, het verkrijgen van vertrouwelijke informatie in het kader van bedrijfsspionage of zelfs terroristische aanvallen. Een voorbeeld is de recente aanval op het UNIX-bedrijf SCO. De motivatie van de daders was onvrede over de rechtzaak tegen een paar grote gebruikers van het besturingssysteem Linux.

Informatiebeveiliging met beleid

In de praktijk ervaren steeds meer organisaties dat informatiebeveiliging een belangrijk onderdeel is of zou moeten zijn van de andere bedrijfsprocessen. Mede ingegeven door meldingen in de media van bijvoorbeeld aanzienlijke (imago)schade door voornamelijk computervirussen en -wormen en de bijkomende kosten ter voorkoming en herstel, komen organisaties tot de conclusie dat informatiebeveiliging meer zou moeten zijn dan operationele maatregelen alleen. Een goede organisatie en sturing op hoger niveau is noodzakelijk voor informatiebeveiliging. De roep om een informatiebeveiligingsbeleid en duidelijke uiteenzetting van de taken, bevoegdheden en verantwoordelijkheden op elk niveau in de organisatie wordt daarom steeds luider.

In de literatuur bestaan verschillende modellen die de volwassenheid van het proces van de informatiebeveiliging in een organisatie beschrijven. De volwassenheid van het informatiebeveiligingsproces hangt af van de mate waarin het proces geïntegreerd is in de andere bedrijfsprocessen en de effectiviteit van de werkwijze binnen het proces. De onderstaande tabellen tonen beide vijf fasen voor deze factoren van volwassenheid. Naarmate het proces van informatiebeveiliging in een organisatie meer volwassen is, verschuift ook het niveau van alleen het operationele vlak naar het tactische en strategische niveau van de organisatie.

In de praktijk blijkt dat veel organisaties niet veel verder zijn dan de eerste 2 à 3 fasen qua integratie en effectiviteit van de werkwijze. Een duidelijke aanwijzing voor deze constatering is de afwezigheid van een informatiebeveiligingsbeleid. Uiteraard geeft de aanwezigheid van een informatiebeveiligingsbeleid geen garantie voor een volwassen informatiebeveiligingsproces. Het is wel een eerste onmisbare stap, waarmee het voor iedereen in de organisatie duidelijk is welke waarde de organisatie aan informatie en de beveiliging ervan hecht en op welke wijze deze gewaarborgd moet worden.

Lees meer over de informatiebeveiligingsprojecten die Fox-IT uitvoert in het artikel over het project voor de ANWB.

Fase	**Integratie**
Onbezorgd	Informatiebeveiliging wordt niet in overweging genomen en de organisatie heeft geen budget voor beveiligingsmaatregelen.
Onbekend	De organisatie acht informatiebeveiliging nuttig maar informatiebeveiliging heeft geen duidelijke positie in de organisatie; de oplossingen worden ad hoc gekozen.
Ontluikend	Informatiebeveiliging heeft een duidelijke positie in de organisatie; het is een stafaangelegenheid.
Beheerst	De organisatie stelt dat informatiebeveiliging een integraal onderdeel is van ieder proces; het is een lijnmanagementaangelegenheid.
Professioneel	De organisatie stelt dat informatiebeveiliging een integraal onderdeel is van de bedrijfsvoering; het is een directieaangelegenheid en een continu aandachtspunt.

Fase	**Effectiviteit van de werkwijze**
Ad hoc	In de organisatie zijn geen eenduidige processen voor informatiebeveiliging te onderkennen.
Herhaald	De organisatie werkt procesmatig ten behoeve van informatiebeveiliging, maar het proces is niet formeel beschreven.
Gedefinieerd	Het informatiebeveiligingsproces is beschreven in formele procedures.
Gecontroleerd	In het informatiebeveiligingsproces wordt gemeten en bijgestuurd op basis van prestatie-indicatoren.
Geoptimaliseerd	Het informatiebeveiligingsproces wordt geoptimaliseerd ten behoeve van de ondersteunde primaire processen.

Bronnen: Dr. M.E.M. Spruit - ITIL security management: een kritische beschouwing, Compact 2000/4
P.L. Overbeek, E. Roos Lindgreen en M.E.M. Spruit - Informatiebeveiliging onder controle, Financial Times, Prentice Hall, Amsterdam 2000.

Agenda

- **Opleiding 'Security & Hacking'**
  14 t/m 17 juni: Module 1: Techniek & Module 2: Security
  18 & 28 juni t/m 2 juli: Module 3: Hacking & Module 4: Intrusion Detection
  6 t/m 9 september: Module 1 & 2
  10 & 20 t/m 24 september: Module 3 & 4
  1 t/m 4 november: Module 1 & 2
  5 & 15 t/m 19 november: Module 3 & 4
  22 november: Module 5: Wetgeving

- **Opleiding 'Rechercheren op de Digitale Snelweg'**
  4 t/m 8 oktober: Basisopleiding
  13 & 14 oktober: Vervolgopleiding
  24 & 25 november: Vervolgopleiding
  29 & 30 november & 1 t/m 3 december: Basisopleiding
  9 & 10 december: Vervolgopleiding

- **Opleiding 'Verdieping Computercriminaliteit'**
  23 & 24 juni:
  Organisatie: Studiecentrum Rechtspleging (SSR)
  Doelgroep: Rechterlijke macht

- **2 juni Seminar 'Misbruik van computernetwerken en fraude'**
  Organisatie: Computer Associates, Ernst & Young, EDS & Fox-IT
  Doelgroep: grootbedrijf ondernemingen
  Informatie: www.ca.com/nieuwegein

- **16 juni Seminar 'Cybercrime'**
  Organisatie: Verbond van verzekeraars, doelgroep: particuliere verzekeraars

- **13 & 14 oktober Beurs Infosecurity.nl**
  jaarbeurs, Utrecht

Colofon

Uitgave van Fox-IT Forensic IT Experts B.V.
Juni 2004

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