FOX-IT
EXPERTS IN IT SECURITY

FOX-IT NIEUWS MEI 2006

KWALITEIT, DIEPGANG EN INTERNATIONALE EXPANSIE

NIET ALLEEN VAKINHOUDELIJK WAS 2005 EEN PRACHTIG JAAR. OOK FINANCIEEL HEBBEN WE EEN UITSTEKEND JAAR ACHTER DE RUG. BIJ ALLE BUSINESS UNITS WAS EEN STERKE GROEI TE ZIEN; IN TOTAAL IS DE OMZET VERDUBBELD! EN OOK 2006 BELOOFT EEN MOOI JAAR TE WORDEN. FOX-IT GAAT INTERNATIONAAL.

We starten een vestiging op de Nederlandse Antillen, we zijn aan de slag in België en in mei nemen we deel aan de Milipol in Qatar. Maar boven alles koesteren wij de goede relatie met onze klanten. Ook in 2006 kunt u op onze service, flexibiliteit en gedegen kennis rekenen. De sterke groei die Fox-IT vorig jaar doormaakte, zet in 2006 nog een beetje door. Om de nieuwe aanwas goed in te lijven, besteden we op dit moment veel aandacht aan kwaliteitsborging, organisatie en training. De volgende lichting CISSP, OSSTMM en particulier onderzoeker wordt nu opgeleid. Verder heeft een aantal werknemers onlangs security gerelateerde WIFI, Oracle en code vulnerability trainingen gevolgd. Ondertussen zijn we samen met klanten continu bezig te bepalen hoe we optimaal service kunnen verlenen. Aan diverse bedrijven en overheidsinstanties hebben wij de afgelopen jaren beveiligingsoplossingen op maat geleverd. Deze applicaties worden vervolgens permanent ondersteund door onze experts in het Security Operations Center. Om in de toekomst dergelijke oplossingen en service te kunnen blijven leveren, zijn mantelcontracten belangrijk. Een nieuwe trend is dat steeds meer opdrachtgevers een apart ICT beveiligingsperceel maken bij het uitbrengen van een Europese aanbesteding. Wij doen er alles aan dit in 2006 goed te regelen.

In deze nieuwsbrief vragen wij uw aandacht voor een aantal boeiende ontwikkelingen en vraagstukken op ons vakgebied. Bestaat een veilige USB-stick? Wat zijn de mogelijkheden van polsbandjes bij de beveiliging van gevangenen? En ook vertellen wij u over een nieuwe training, die eindelijk het opstellen, evalueren en meten van beveiliging mogelijk maakt. Ik wens u veel plezier met het lezen.

MENNO VAN DER MAREL, DIRECTEUR

OP ZOEK NAAR ....DE ONKRAAKBARE USB-STICK

MET REGELMAAT KRIJGEN WIJ VAN KLANTEN DE VRAAG WELKE USB-STICK VEILIG IS. OP DIE VRAAG MOETEN WIJ HEN HET ANTWOORD SCHULDIG BLIJVEN; IETS DAT NIET VAAK VOOR KOMT BIJ FOX-IT. DE DOCUMENTATIE BIJ DE PRODUCTEN BIEDT TE WEINIG INFORMATIE OM EEN GOED OORDEEL TE KUNNEN VELLEN. WEL WETEN WE WAAR JE BIJ DE AANSCHAF VAN EEN VEILIGE USB-STICK OP MOET LETTEN.

Het eerste dat u bij de aankoop van een USB-stick helder voor ogen moet hebben, is het dreigingsbeeld. Het is dan wel mogelijk om staatsgeheimen veilig op een USB stick te zetten (dat was zelfs op het RTL-nieuws), maar een dergelijke oplossing is erg kostbaar.

Veel klanten overwegen dan ook geen beveiliging op het niveau staatsgeheim. Zij denken eerder veel te licht over de veiligheid van USB-sticks. Zij verkeren in de veronderstelling dat enige vorm van beveiliging genoeg is om een journalist of nieuwsgierige vinder tegen te houden. Maar als de stick in een tas is gevonden waar ook politiedocumenten in zaten, zal een journalist er best een beperkt bedrag gecombineerd met media aandacht voor over hebben om de stick te laten kraken. En daarmee kom je een heel eind.

HET EERSTE DAT U BIJ DE AANKOOP VAN EEN USB-STICK HELDER VOOR OGEN MOET HEBBEN, IS HET DREIGINGSBEELD.

Zijn de sticks zo gemakkelijk te kraken? Helaas wel. Veel 'beveiligde' sticks versleutelen de bestanden met behulp van een wachtwoord. Dat is gelijk de zwakste schakel. Wachtwoorden raden is niet zo moeilijk. Computers kunnen miljoenen wachtwoorden per seconde proberen. Grote kans dat hij die van u zo gevonden heeft.

Iets slimmere sticks zijn vaak ook hardwarematig beveiligd. Soms is de versleuteling zelfs compleet in hardware (meestal wel softwarematig aangestuurd). Maar zelfs deze beveiliging valt binnen het budget van een journalist te kraken. Even de stick openen, een draadje solderen, soms zelfs gelijk de geheugenchip uitlezen, en de gevoelige gegevens liggen op straat. In het ergste geval moet na deze handelingen nog iets gekraakt worden. Afhankelijk van de gebruikte technieken kan dit variëren in moeilijkheid, maar het lukt eigenlijk altijd. Zelfs bij de veelgebruikte biometrische sticks die wij hebben onderzocht!

U zou natuurlijk het liefst van ons horen welke stick het veiligst is. Maar helaas kunnen we daar nog geen uitspraak over doen. Op dit moment zijn we bezig met een uitgebreide analyse van verscheidene sticks en wachten we op informatie van fabrikanten. We hopen de ideale stick zo snel mogelijk gevonden te hebben!

FOX-IT: NETTE MENSEN, EX-JUSTITIE

FOX-IT LEVERT AL JAREN MAATWERK AAN HET MINISTERIE VAN JUSTITIE. OM EEN BEELD TE GEVEN VAN DEZE SAMENWERKING SPRAKEN WE MET DE BEVEILIGINGSAUTORITEIT (BVA) EN EEN VAN FOX-IT'S CONTACTPERSONEN OP HET MINISTERIE.

'De keuze valt steeds op Fox-IT, in plaats van op multinationals die vergelijkbare diensten kunnen leveren'. Ton Fintelman, BVA bij het Ministerie van Justitie is complimenteus. 'Jullie technische kennis gaat veel dieper, jullie zitten meer in de bits & bites zogezegd.' Fintelman is al sinds de oprichting bekend met Fox-IT; hij kreeg de tip van een vroegere collega. Het directe vertrouwen was gebaseerd op de achtergrond van de oprichters, die voorheen bij het NFI werkten. Maar hij ging pas met Fox-IT in zee na een positieve referentie van het NFI.

Het eerste project dat het ministerie in samenwerking met Fox-IT opstartte, was een onderzoek naar de veiligheid van het elektronisch pasjessysteem. Inmiddels zijn er diverse opdrachten gevolgd. Fox-IT geeft ook regelmatig presentaties op het ministerie over 'Security awareness'. Fintelman is blij met deze presentaties, maar: 'Het punt bij awareness is dat er eerst incidenten plaats moeten vinden voordat er echt bewustzijn komt'. Incidenten zoals onlangs bij de voormalige Officier van Justitie Tonino komen Fintelman in zekere zin dan ook goed uit.

Ook Alfons Lammerts van Bueren heeft in zijn functie bij Justitie veel contact met Fox-IT. Hij was als senior beleidsmedewerker bij de Dienst Justitiële Inrichtingen betrokken bij de inventariserende Afhankelijkheids & Kwetsbaarheden analyse waarvoor Fox-IT werd ingezet. 'Jullie bestaansrecht bestaat uit de combinatie van diepe technische kennis, flexibiliteit, forensische kennis, Fox-IT trainingen en de kunde van het uitleggen in gewone taal' aldus Lammerts van Bueren. 'En ondanks jullie gestage groei zijn jullie flexibel gebleven.'

Fintelman is gecharmeerd van de onafhankelijkheid van Fox-IT. 'Daar waar andere bedrijven een derde partij erbij betrekken, heeft Fox-IT zelf alle specialisten voor het daadwerkelijke 'schroeven' in huis. Het ministerie besteedt zelfs recherchewerk aan Fox-IT uit, doordat ze de regie dan in handen kan houden en het werken met eigen mensen ook risico's met zich meebrengt.' Fintelman was blij dat Fox-IT in 2003 de unieke cryptotechnologie van Philips overnam. 'Fox-IT wordt gezien als betrouwbare en kundige partner onder het motto 'nette mensen, ex-justitie'.' Dit laatste uiteraard aan de juiste kant van de deuren.

EXPERTMEETINGS ZIJN EEN SUCCES

HET CONCEPT 'EXPERTMEETINGS' DAT FOX-IT VORIG JAAR INTRODUCEERDE, IS EEN SUCCES. NA 'DIGITAAL GERELATEERDE INCIDENTEN' WAS OOK 'OUTSOURCING IT SECURITY' JANUARI JL. EEN SCHOT IN DE ROOS. MEDIO APRIL STOND 'SECURITY AWARENESS' OP HET PROGRAMMA.

Het idee van een expertmeeting is dat een selecte groep cliënten en relaties samen op zoek gaat naar een protocol of een 'best practice'. Deze

rondetafelgesprekken zijn tevens een uitstekende mogelijkheid om in een informele sfeer met vakgenoten van gedachten te wisselen.

Een van de redenen voor het succes van de expertmeetings is de focus en compactheid. Hoe vaak krijgt een expert nu de kans om los van de dagelijkse beslommeringen zich een middag en avond lang in security issues te verdiepen? Achteraf ontvangen alle deelnemers het verslag van de bijeenkomst.

Foto: Marcel Israel Fotografie / Geodan

NIEUW DETENTIECONCEPT: POLSBANDJES VOOR GEVANGENEN

ONDER HET TOEZIEND OOG VAN HET MINISTERIE VAN JUSTITIE IS IN LELYSTAD EEN 'NIEUW DETENTIECONCEPT' ONTWIKKELD: 'S WERELDS EERSTE VOLLEDIG GEDIGITALISEERDE GEVANGENIS. NU DE EERSTE GEVANGENEN HUN INTREK NEMEN, TEST FOX-IT HET VOLLEDIG DRAADLOZE NETWERK. PROJECTLEIDER, WERKZAAM BIJ DE DIENST JUSTITIËLE INRICHTINGEN, VOORMALIG GEVANGENISDIRECTEUR EN MEDE-INITIATIEFNEMER JAN PIEK VERTELT:

'De gevangenis in Lelystad is de eerste in de wereld waar alles is gedigitaliseerd. De behoefte voor een nieuw concept kwam enerzijds voort uit de bezuinigingen die de overheid ons oplegde. Anderzijds kwam vanuit de maatschappij de behoefte aan meer cellen om meer gedetineerden te kunnen opsluiten. Minister Donner zelf legde de eerste steen, wat aangeeft dat het idee tot op het hoogste niveau werd omarmd.

Om het nieuwe concept te realiseren hebben we op drie punten veranderingen doorgevoerd. Op het gebied van architectuur, de inzet van personeel en het gehandhaafde regime. Architectonische ingrepen hebben veel voordelen opgeleverd. Het gebouw is bijzonder overzichtelijk en sterk gecompartimenteerd geworden. Bepaalde activiteiten kunnen nu zonder personeel worden uitgevoerd. Daarnaast voeren gedetineerden nu een aantal activiteiten zelf uit, die we eerder uitbesteedden. Hierdoor zijn de personeelskosten met 40% afgenomen. Tot slot hebben we polsbandjes ingevoerd. In deze polsbandjes zit een RFID chip waarmee gevangenen kunnen telefoneren, tv kijken, bestellen etc. Ook kan de bewaarder door dit systeem met zijn palmtop altijd zien waar de gevangenen zich bevinden. Camera's die ook via de palmtop zijn op te roepen, helpen hem hierbij.

Veiligheid is bij dit project uiteraard van het grootste belang. Aangezien alles draadloos werkt, bestaat het gevaar dat hackers de systemen van buitenaf penetreren en manipuleren. Daarom hebben we Fox-IT gevraagd een audit op het systeem uit te voeren. Nadat we de cruciale zaken hebben opgelost, kunnen we aan de slag met de lijst met verbeterpunten die Fox-IT aanlevert.'

FORENSICS & AUDITS: VAKER, MEER EN BREDER

FOX-IT'S BUSINESS UNIT FORENSICS & AUDITS MERKT DUIDELIJK DAT INFORMATIEBEVEILIGING VOLOP IN DE BELANGSTELLING STAAT. ZE HEBBEN HET DRUKKER DAN OOIT. BUSINESS UNIT MANAGER MATTHIJS VAN DER WEL SIGNALEERT DE LAATSTE ONTWIKKELINGEN OP FORENSISCH IT GEBIED.

'Je ziet dat steeds meer organisaties en bedrijven zich voorbereiden op een incident met mogelijke digitale sporen. Stel dat je een rechercheur op bezoek krijgt, met het nieuws dat iemand via jouw internetaansluiting een bommelding heeft verstuurd. Beschik je dan over de juiste digitale sporen om na te gaan wie dat heeft gedaan? Hebben de logbestanden vastgelegd wat je wilt weten? Weten de verschillende afdelingen wat hen te doen staat?

Steeds meer bedrijven realiseren zich dat ze veel winst kunnen behalen door zich goed voor te bereiden op een incident. Fox-IT helpt hen hierbij. We hebben onder andere een speciale tweedaagse workshop ontwikkeld voor IT-ers samen met de beveiligingsmedewerkers. Zij leren daarin zich goed voor te bereiden op incidenten met mogelijk digitale sporen. Spreken ze elkaars taal? Wat besteed je uit? Ga je zelf de mail van een collega doorspitten, of laat je dat doen? Gaat de helpdesk adequaat om met verzoeken om logbestanden? Een andere groeimarkt voor forensisch IT-onderzoek is die van van de incidenten waarbij niet een IT-systeem zelf het doelwit is (zoals bij hackers), maar waarbij een digitale toepassing als middel is gebruikt. Denk aan een valse factuur die in Excel is gemaakt. Ook die laat digitale sporen na. Steeds vaker schakelen bedrijven ons in voor dit soort onderzoeken. Dat gaat om de meest uiteenlopende zaken, denk aan fraude, afpersing, of het lekken van gevoelige informatie, etc.

Tot slot voeren we steeds vaker contra-expertises uit. Advocatenkantoren schakelen ons in om te kijken of onderzoeken die anderen hebben uitgevoerd op een goede en juiste manier zijn gedaan.'

SOCIAL ENGINEERING PAKT DE ZWAKSTE SCHAKEL IN DE BEVEILIGINGSKETEN AAN: DE MENS

FOX-IT TEST BEVEILIGINGEN, MAAR BEVEILIGEN IS MEER DAN ALLEEN DE TECHNIEK. MET BEHULP VAN SOCIAL ENGINEERING KIJKEN WE DAAROM OF PERSONEN ZICH WEL HOUDEN AAN DE PROCEDURES EN RICHTLIJNEN BINNEN HET BEDRIJF. VAAK BLIJKT HET BEVEILIGINGSBEWUSTZIJN OF DE 'SECURITY AWARENESS' VAN MEDEWERKERS NAMELIJK DE ZWAKSTE SCHAKEL IN DE BEVEILIGING.

Social engineering wordt meestal gedefinieerd als: 'de kunst en wetenschap om anderen zover te krijgen iets te doen zonder dat het doelwit in de gaten heeft dat hij/zij misbruikt wordt'. In de praktijk blijkt telkens hoe succesvol zo'n strategie kan zijn. De techniek is niet nieuw: oplichters gebruiken 'm al jaren. Als organisatie is het zaak hierop voorbereid te zijn, onder andere door op voorhand de reacties van personeel te testen.

Met technieken die ook hackers en andere criminelen gebruiken, proberen we toegang te krijgen tot uw bedrijfsgeheimen. Uiteraard volgt hierna een uitgebreide rapportage, inclusief aanbevelingen. Een speciale methode die Fox-IT op verzoek hanteert, is het inzetten van 'mistery guests' of 'tiger teams'. Zij gaan als 'tijdelijke kracht' of 'externe consultant' aan de slag. Maar met een heel specifieke opdracht: vanuit een 'insider' perspectief kwetsbaarheden identificeren in de informatiebeveiliging!

Fouten maken is menselijk, maar wat de amateurs van professionals onderscheidt, is hoe zij met hun fouten omgaan. Met een social engineering test kan een bedrijf in ieder geval van gemaakte fouten leren.

SOCIAL ENGINEERING IN DE PRAKTIJK

Stelt u zich eens voor. U krijgt een telefoontje van iemand van de IT-afdeling. Er iets mis is gegaan bij het installeren van nieuwe software en al uw gegevens zijn tijdelijk verloren gegaan. Gelukkig zijn ze al bezig de bestanden te repareren. Om uw e-mail terug te kunnen zetten, hebben ze uw wachtwoord veranderd. Opgelucht wilt u ophangen, als de systeembeheerder u vraagt: 'wilt u uw oude wachtwoord behouden'?

Wat zou u antwoorden? 'Ja, graag'? Dan is de volgende vraag waarschijnlijk 'wat was uw oude wachtwoord?' Als u dat dan geeft, is de kans groot dat iemand met social engineering uw wachtwoord heeft ontfutseld. De systeembeheerder was geen systeembeheerder, en er was geen sprake van verlorengegane bestanden. Misschien dat u uw wachtwoord niet via de telefoon aan een (on)bekende doorgeeft. Maar hoe zit dat met een 'collega' die voor uw bureau staat? Hoever kan een kwaadwillende 'collega' komen, om uw informatiebeveiliging te doorbreken?

NIEUWE TRAINING: OSSTMM

IN MEI START DE NIEUWE TRAINING OSSTMM (OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL). HIERVOOR IS FOX-IT EEN PARTNERSCHAP AANGEGAAN MET ISECOM (INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES).

OSSTMM is uniek. Het is de eerste en meest wijdverspreide open standaard voor het opstellen, evalueren en meten van beveiliging. Door haar transparante werkwijze, het gebruik van een consistent raamwerk en direct meetbare resultaten biedt OSSTMM de mogelijkheid structuur aan te brengen in het meten van de informatiebeveiliging. De concrete getallen die dit oplevert, maken het eenvoudig om positieve of negatieve veranderingen in kaart te brengen. OSSTMM voegt in vergelijking tot methodieken als ISO17799 en de Code voor Informatiebeveiliging duidelijk iets toe. In tegenstelling tot andere methodieken benadert OSSTMM informatiebeveiliging echter bottom-up in plaats van top-down. Voordat OSSTMM bestond, was er geen standaard voor het evalueren en meten van informatiebeveiliging. Security audits werden naar eigen inzicht uitgevoerd.

Met OSSTMM is het mogelijk beveiliging op een consistente manier te meten. Hoe dat precies werkt, leren cursisten tijdens deze training bij Fox-IT. Roland Vergeer, Business Unit Manager Training sinds begin 2005 geeft de training.

Roland is gecertificeerd trainer (OPST/OPSA) en werkt deels als Security Expert bij Fox-IT. Cursisten worden in één week opgeleid tot Security Analyst én Security Tester. De training is geschikt voor zowel systeembeheerders als managers die zich beroepsmatig met IT beveiliging bezighouden. **Meer informatie over de OSSTMM methodiek op www.osstmm.org.**

TRAINING

OOK DE BUSINESS UNIT TRAINING HEEFT EEN GOED JAAR GEHAD. GROTERE ORGANISATIES ZIJN ZICH MEER EN MEER BEWUST VAN HET BELANG VAN INFORMATIEBEVEILIGING. ZIJ KIEZEN ER DAAROM STEEDS VAKER VOOR HUN PERSONEEL PRAKTIJKGERICHTE TRAININGEN VAN FOX-IT TE LATEN VOLGEN. EEN AANTAL REACTIES VAN CURSISTEN:

'De cursus was uitermate nuttig, we gebruiken dingen in de praktijk. Het was ook erg leuk om zo'n echte wizzkid eens aan het werk te zien...' **THEA SIBMA, INTERPOLIS**

'Ik vond de inhoud zeer geschikt voor het digitaal rechercheren van groepen onbekende personen. Zo kan men adresgegevens en telefoonnummers van verdachten achterhalen via allerlei zoekmogelijkheden. Bij verzekeraars beschikken we bijna altijd over de adres en telefoongegevens van de betrokkenen. Hier zou achtergrondinformatie of achterhalen of men chat over de zaak een welkome aanvulling op het onderzoek zijn. Als rechercheur vind ik het nuttig om te weten dat er een mogelijkheid is om zo diepgravend te zoeken op internet.' **JOHN KEMP, INTERPOLIS**

AGENDA TRAININGEN

Onderstaand treft u de agenda aan voor het komende jaar. U kunt zich inschrijven via www.fox-it.com; hier treft u tevens de volledige agenda aan.

Digitaal Rechercheren (Basis)
- 15 mei, 2 oktober en 20 november

Digitaal Rechercheren (Opfriscursus)
- 23 en 24 mei, 13 en 14 september, 6 en 7 december

OSSTMM
- 17 juli

CISSP (Certified Information Systems Security Professional)
- 19 juni, 26 juni (examen op 1 juli), 27 november en 11 december

Security & Hacking
- 14 augustus, 28 augustus, 30 oktober en 13 november

COLOFON: UITGAVE VAN FOX-IT MEI 2006.
REDACTIE: DOMINIQUE DE GAST - E-MAIL DE.GAST@FOX-IT.COM - OLOF PALMESTRAAT 6 - 2616 LM DELFT - POSTBUS 638 - 2600 AP DELFT
TELEFOON: 015 284 79 99 - FAX: 015 284 79 90 - E-MAIL: FOX@FOX-IT.COM - WEB: WWW.FOX-IT.COM