FOX-IT
EXPERTS IN IT SECURITY

FOX-IT NIEUWS DECEMBER 2005

VOLOP ONTWIKKELING BIJ FOX-IT!

WE ZIJN NAAR DELFT VERHUISD! DAT WAS HARD NODIG, WANT WE GROEIDEN SNEL UIT ONS JASJE. IN EEN JAAR TIJD GROEIDE ONS PERSONEELSBESTAND VAN 30 NAAR 52 MEDEWERKERS. DAT IS NATUURLIJK PRACHTIG, MAAR WE WILLEN NU OOK WAT RUST CREËREN.

We hebben elkaar daarom plechtig beloofd de komende vijf jaar niet te verhuizen. Zo kunnen onze nieuwe medewerkers in alle rust ons bijzondere vakgebied leren kennen. En dat is noodzakelijk om onze kwaliteit te waarborgen. Een van de manieren om die kwaliteit te garanderen is onze eigen kennis op peil houden. Daarom volgen wij zelf ook regelmatig trainingen. Nadat een groot aantal medewerkers hun CISSP examen had gehaald, kregen we afgelopen jaar de smaak goed te pakken. Een gedeelte van onze medewerkers heeft nu ook CISA (Certified Information Systems Auditor) op zijn visitekaartje staan. Onlangs volgde het hele bedrijf een PrinceII training, zodat we relevante opdrachten volgens dezelfde methodiek kunnen aanpakken als veel van onze klanten doen. Dat we unieke kennis in huis hebben, is de afgelopen tijd wel gebleken. Buitenlandse banken doen steeds vaker een beroep op ons bij hack- en fraude-incidenten. Zo komt er gelukkig ook wat kleur op de, soms bleke, gezichten van onze medewerkers.

Ons Incident Response Team heeft tegenwoordig permanent een uitrukkoffer klaar staan. Ze kunnen onmiddellijk het vliegtuig pakken om waar dan ook ter wereld assistentie te verlenen. Maar ook in Nederland handhaven we ons in de absolute top. Zo hebben we een contract gesloten met de Nederlandse overheid om een nieuwe crypto chip te ontwikkelen: de RedFox. De overheid zal deze crypto chip gebruiken om het (Top Secret) berichtenverkeer tegen afluisteren door derden te beschermen.

Naast al dit goede nieuws, is er helaas ook een heel treurig bericht. In oktober hebben we afscheid moeten nemen van onze gewaardeerde collega Rob Paar die zeer onverwacht op 36-jarige leeftijd is overleden. Als programmeur heeft hij een enorme bijdrage geleverd aan ons intrusion detection systeem Plato.

RONALD PRINS, DIRECTEUR

SECURITY PARTNER VOOR FOX-IT IN BELGIË EN LUXEMBURG

FOX-IT IS EEN PARTNERSCHAP AANGEGAAN MET KREOS CONSULT, DAT SINDS KORT EEN AANTAL FOX-IT DIENSTEN OP DE BELGISCHE EN LUXEMBURGSE MARKT AANBIEDT.

Het Leuvense bedrijf is een nieuwe speler op de IT beveiligingsmarkt. Op het gebied van beleid, management en technologie kan het Belgische bedrijf echter bogen op ruime kennis en ervaring. Wat KreoS uniek maakt is dat ze die beleid- en managementinzichten combineert met kennis van beveiliging. Zij slaat een brug tussen het managementteam en de andere relevante spelers in de organisatie, waardoor ze precies kan bepalen welke IT beveiligingsoplossingen perfect binnen het bedrijf passen.

KIJK VOOR MEER INFORMATIE OVER KREOS CONSULT OP WWW.KREOS-CONSULT.BE OF NEEM CONTACT OP MET DIRK PEETERS OF WILLIAM VERSTRAETEN OP TELEFOONNUMMER +32 (0)16 38 60 30 OF VIA INFO@KREOS-CONSULT.BE.

In eerste instantie biedt KreoS de volgende diensten van Fox-IT op de Belgische markt aan:

- Security Monitoring
- Digitaal forensisch onderzoek
- Security Audits

Daarnaast is Kreos Consult actief op het gebied van:

- Enterprise Security Management:
  KreoS helpt bedrijven bij de juiste toepassing van IT beveiliging. Enterprise Security Management maakt inzichtelijk welke invloed IT beveiliging heeft op de bedrijfsprocessen en de operationele capaciteiten.
- Identity Management:
  Dit betreft het geheel aan mensen, middelen en processen dat een organisatie inzet om het beheer van identiteiten en de toegang tot de informatievoorziening effectief, efficiënt en gecontroleerd uit te voeren.

SLECHT BEVEILIGDE MEDEWERKERS

DE GEMIDDELDE WERKNEMER DENKT WEINIG VAN DOEN TE HEBBEN MET DE BEVEILIGING VAN INFORMATIE. DAAR HEBBEN WE TOCH DE ICT-AFDELING VOOR? MAAR DAT IS NATUURLIJK NIET WAAR. FOX-IT HEEFT DAAROM EEN SPECIAAL PROGRAMMA ONTWIKKELD. OP BASIS VAN CASE BASED INTERVIEWS EN KORTE, INTENSIEVE WORKSHOPS BRENGT DIT PROGRAMMA HET BEVEILIGINGSBEWUSTZIJN TERUG OP DE WERKVLOER.

Fox-IT voert Security Audits uit bij een groot aantal organisaties. Naast een kritische analyse van de technische infrastructuur en de informatiesystemen, wordt ook de organisatie zelf op zwakheden getest. Het blijkt telkens weer dat een van de zwakste plekken in de beveiliging van informatie, de medewerkers zelf zijn. Zij zijn vaak 'slechter beveiligd' dan de fysieke systemen. Een gemiddelde medewerker weet nauwelijks hoe belangrijk zijn of haar rol binnen informatiebeveiliging is. En juist zijn of haar gedachten over vertrouwelijkheid, beschikbaarheid en integriteit van informatie, bepalen het beveiligingsniveau in een organisatie.

De oorzaak van 'slecht beveiligde medewerkers' ligt vaak in de organisatie zelf. Het bewustzijn van informatieveiligheid onder medewerkers krijgt binnen de organisatie te weinig prioriteit. Vaak heerst de gedachte dat het vergroten van dit bewustzijn tijdrovend en kostbaar is. Maar dit is een misvatting.

De doelgerichte aanpak van case based interviews en korte workshops, zoals Fox-IT die heeft ontwikkeld, blijkt heel effectief. Via deze interviews en korte, intensieve workshops doen medewerkers en managers direct toepasbare kennis op. Ze leren niet alleen te kijken door de bril van een informatiebeveiliger, maar ook door de bril van een kwaadwillende. Door te speuren naar mogelijkheden om misbruik te maken van mens en voorziening binnen de eigen organisatie, groeit hun beveiligingsbewustzijn. En daarmee verandert ook hun gedrag.

RUSSISCHE HACKERS OP OORLOGSPAD

HET INTERNET ALS HET MODERNE WILDE WESTEN, WAAR HACKERS IN PLAATS VAN GEWAPENDE BANDIETEN DE BOEL ONVEILIG MAKEN EN BANKEN BEROVEN. DIT DOEMSCENARIO WORDT AL JAREN VOORSPELD, MAAR IN DE PRAKTIJK VIEL HET TOT DUSVER WEL MEE. DIT IS ECHTER IN RAP TEMPO AAN HET VERANDEREN. VOORAL RUSSISCHE HACKERS GEBRUIKEN ZWAKKE PLEKKEN IN INTERNETAPPLICATIES OM GROTE HOEVEELHEDEN GELD WEG TE SLUIZEN.

Steeds meer financiële instellingen bieden hun producten ook online aan. Bankieren, beleggen en verzekeringen afsluiten: het kan allemaal op het internet. De applicaties voor deze services zijn meestal op maat ontwikkeld, maar zijn vaak niet op het juiste niveau beveiligd. Hackers maken hier dankbaar gebruik van.

EENMAAL INGELOGD IS HET EEN KOUD KUNSTJE OM GELD OVER TE MAKEN NAAR STROMANNEN.

Criminelen verleggen hun werkterrein steeds vaker naar het internet. Het technisch vernuft van deze cyberonverlaten is de afgelopen jaren sterk gegroeid. Een groep professionele Russische hackers struint momenteel bijvoorbeeld het internet af op zoek naar financiële applicaties met beveiligingsfouten. Wanneer ze die vinden, breken ze in en nemen ze zoveel mogelijk gegevens mee over de online banking applicatie. Enige tijd later gebruiken ze de ontdekte zwakheden in de bankapplicatie om in te loggen onder de naam van een echte klant. Eenmaal ingelogd is het een koud kunstje om geld over te maken naar stromannen. Deze stromannen nemen het geld op, waarna de cash naar Rusland wordt gebracht.

Fox-IT is de afgelopen maanden bij diverse hackincidenten ingeschakeld die volgens dit scenario zijn ontstaan. Het valt op dat de criminelen zich extreem goed voorbereiden en uitstekend op de hoogte zijn van eventuele lekken in de systemen en applicaties. De Russische groep heeft zich echt gespecialiseerd in internet bankapplicaties.

Veel van de bankapplicaties zetten een versleutelde verbinding met de klanten op, waardoor de bankmedewerkers de inhoud van dat verkeer niet zomaar kunnen monitoren. Het gevolg is dat de hackers hun gang kunnen gaan zonder dat de bank dit opmerkt. Zodra de inbrekers binnen zijn, zorgen ze dat ze een account krijgen dat alle rechten heeft, waardoor hun sporen niet meer opvallen. Op deze manier kunnen ze in alle rust uitzoeken via welke eindgebruikers het geld het beste kan worden weggesluisd.

Maar, kan er dan niets gedaan worden tegen deze internetmaffia? Jawel, Fox-IT kan deze problemen grotendeels voorkomen. Het is zaak de beveiliging van de verschillende applicaties serieus onder de loep te nemen. Een veilig systeem moet aan een aantal minimale eisen voldoen. Om te beginnen is dat een correct geïmplementeerde 2-factor authentication methode (bijvoorbeeld door gebruik van een token/bankpas). Daarnaast is een goed werkende patch- en updateprocedure noodzakelijk. Ook de controle van de broncode van de applicatie en de permanente monitoring van het verkeer rondom de applicatie zijn onontbeerlijk.

Vooral kleinere banken blijken last te hebben van deze vorm van internetcriminaliteit. Zij zijn zelf vaak niet in staat de belangrijkste voorzorgsmaatregelen op de juiste wijze te implementeren; Fox-IT kan hier vanzelfsprekend bij van dienst zijn.

NETWERKEN SCHEIDEN EN VERBINDEN MET FORT FOX DATA DIODE

EEN FIREWALL VAN VLEES EN BLOED WAS TOT OP HEDEN DE ENIGE WATERDICHTE NETWERKBEVEILIGING. DIT ZOGENAAMDE 'ADIDASNETWERK' HIELD IN DAT MENSEN DAGELIJKS MET TAPES VAN HET ENE NAAR HET ANDERE NETWERK WANDELDEN. MAAR ZEER BINNENKORT IS DAT NIET MEER NODIG. FOX-IT HEEFT NAMELIJK EEN DATA-DIODE ONTWIKKELD MET DEZELFDE VEILIGHEIDSGARANTIES ALS EEN PAAR ADIDAS SPORTSCHOENEN. ALLEEN WEL EEN STUK EFFICIËNTER.

De Fort Fox Data Diode (FFDD) koppelt twee netwerken met de garantie dat datastromen tussen de netwerken slechts één kant op kunnen. Dit is noodzakelijk wanneer één van de netwerken een hoger beveiligingsniveau heeft. De diode zorgt ervoor dat de informatie niet naar een netwerk met een lager beveiligingsniveau kan weglekken. Waar speelt dit? Bijvoorbeeld bij overheidsorganisaties die gegevens van burgers via het internet willen ontvangen. Deze gegevens komen binnen via het internet en moeten naar het fysiek gescheiden rekencentrum. Deze scheiding voorkomt dat gegevens uit het rekencentrum naar het internet kunnen lekken. Dit betekent wel dat iemand 's avonds de gegevens met een grote tape van de internetservers naar het rekencentrum moet verplaatsen. De FFDD kan deze netwerken automatisch scheiden, zonder iets van de huidige veiligheid in te leveren.

Netwerkverkeer kan normaal gesproken niet zonder communicatie van beide kanten. De nieuwe data diode beschikt daarom over extra intelligentie en functioneert als een store-and-forward systeem. Eerst vangt de FFDD het verkeer op. Vervolgens gaat het via de hardwarematige data diode naar de andere kant van de FFDD en wordt het doorgestuurd naar de eindbestemming. Via een eenrichtingsverbinding kunnen bestanden op deze manier in het afgeschermde netwerk toch worden gemaild, geprint of op een server worden gezet.

De FFDD zit in de laatste ontwikkelingsfase. De evaluatie van de FFDD voor het gebruik bij koppelingen tot en met het niveau Staatsgeheim Zeer Geheim is al gestart.

EEN FLEXIBELE DIENST IN EEN DYNAMISCHE OMGEVING: FOX MSM BIJ ORANGE

TELECOM BEDRIJVEN PROBEREN COMMUNICATIE IN HET DAGELIJKSE LEVEN PRETTIG EN GEMAKKELIJK TE MAKEN. ZIJ WILLEN ZICH ERVAN VERZEKEREN DAT HUN CLIËNTEN OP EEN PROBLEEMLOOS NETWERK VOOR DE MOBIELE TELEFOONDIENSTEN KUNNEN REKENEN, NU EN IN DE TOEKOMST.

Als leverancier van deze diensten is het belangrijk om alle veiligheidskwesties te bekijken. Niet alleen waar het over fysieke veiligheid gaat, zoals alarmsystemen, maar ook digitaal. Door hun lijnen goed te beveiligen, houden zij deze open. Voor Orange is een veilig computernetwerk essentieel. Het wordt gevuld met vertrouwelijke informatie. Om die reden besteden zij de beveiliging niet gemakkelijk uit. Zij willen het aan specialisten overlaten die tegelijkertijd ervaren en absoluut betrouwbaar zijn, en die dat tevens kunnen bewijzen. Met deze eisen in gedachten, vond Orange, één van de vijf grootste telecommunicatieleveranciers in Nederland, al snel Fox-IT. Met Fox MSM (Managed Security Monitoring), was Orange er zeker van dat zijn netwerk 24 uur per dag zorgvuldig werd gecontroleerd. Alle vertrouwelijke informatie zou in veilige handen zijn met de zorgvuldig gescreende IT security experts.

De flexibiliteit van MSM was een andere reden om voor Fox-IT te kiezen. Na het opzetten van de nieuwe afdelingen, het aanpassen van bedrijfsprocessen en netwerkuitbreidingen, wordt de MSM dienst onmiddellijk aangepast en verbeterd. Orange ontwikkelt zich voor de toekomst. En Fox-IT houdt de ontwikkeling bij.

REDFOX: NIEUWE GENERATIE CRYPTO CHIPS

FOX CRYPTO HEEFT IN NOVEMBER VAN DE NEDERLANDSE OVERHEID OPDRACHT GEKREGEN EEN NIEUWE GENERATIE CRYPTO CHIPS TE ONTWIKKELEN: DE REDFOX. CRYPTO CHIPS ZIJN DE ULTIEME OPLOSSING ALS HET GAAT OM HET BEVEILIGEN VAN INFORMATIE. DE REDFOX ZAL GESCHIKT ZIJN VOOR BEVEILIGING VAN STAATSGEHEIMEN TOT EN MET DE RUBRICERING STAATSGEHEIM ZEER GEHEIM.

Eerder leverde Fox Crypto exclusief de vorige generatie crypto chips: de GcdPhi voor de overheid en de GP2000 voor andere organisaties. De nieuwe opdracht komt voort uit de groeiende behoefte aan veilige communicatie. De overheid gebruikt de crypto chips onder andere om haar staatsgeheimen te beveiligen. Net als bij de vorige generatie ontwikkelt Fox-IT naast een variant specifiek voor de Nederlandse overheid ook een commerciële variant.

De nieuwe chipfamilie biedt grote voordelen. Naast een fors hogere snelheid, zijn dat onder andere de ondersteuning van de meest gebruikte moderne versleutelingsalgoritmes en de aanwezigheid van volledige VPN/IPSEC ondersteuning in de chip. De chip is geschikt voor diverse nieuwe toepassingen zoals VPN en harddisk vercijfering. Ook past Fox Crypto verschillende van haar huidige producten aan, zoals de off-line file vercijferaar FFFE. Zo kunnen deze producten meeprofiteren van voordelen van de nieuwe chip.

De nieuwe generatie crypto chips zal rond het tweede kwartaal van 2007 op de markt komen.

KNIPPEN EN PLAKKEN IN POLITIE TAPGESPREKKEN ONMOGELIJK GEMAAKT

Knipt en plakt de politie in tapgesprekken? Verdachten in verschillende rechtszaken claimden van wel. Zo heeft Baybasin zelfs getuige deskundigen opgetrommeld om dit te onderschrijven.

Justitie gaf PriceWaterhouseCoopers daarom opdracht onderzoek te doen naar de veiligheid en integriteit van de Nederlandse tapkamers. In het verlengde hiervan kreeg Fox-IT opdracht een integriteitsysteem te ontwikkelen. Dit systeem zet over elk tapgesprek een digitale handtekening en een tijdstempel. Mocht in de rechtszaal ooit twijfel ontstaan over een getapt gesprek dan kan voortaan eenvoudig worden vastgesteld of er mee is gerommeld of niet.

CRIMINELE POLITIEREGISTERS VEILIG GEKOPPELD

In september heeft Fox-IT een project voor de Nederlandse politie opgeleverd, waarmee criminele politie informatie landelijk wordt ontsloten. Deze opdracht van het CIP (Concern Informatiemanagement Politie) kwam voort uit de wens van het kabinet de kennis en informatie van de verschillende politiediensten beter te bundelen.

Fox-IT heeft de betreffende politieregisters van alle politieregio's, de nationale recherche en de bijzondere opsporingsdiensten hiervoor met elkaar verbonden. Aan deze koppeling werden zeer hoge veiligheidseisen gesteld aangezien het hierbij om zeer vertrouwelijke informatie gaat, die onder meer is aangeleverd door politie-informanten.

INFOSECURITY 2005

De Utrechtse Jaarbeurs stond 9 en 10 november jl. in het teken van Infosecurity.nl. Dit is dé beurs voor trends en ontwikkelingen in beveiliging van informatie, netwerken en communicatie. Op deze belangrijke beveiligingsvakbeurs was Fox-IT natuurlijk prominent aanwezig.

Fox-IT heeft tijdens deze dagen onder andere de apparatuur gedemonstreerd, waarmee het forensische onderzoeken en security audits uitvoert. Ook nam Ronald Prins deel aan 'Cybercrime in de polder', een discussiesessie die deel uitmaakte van de Computable Live sessies.

TRAINING

De maanden januari en februari zijn bijna vol geboekt, voor de overige maanden kunt u zich inschrijven via www.fox-it.com.

Hier treft u tevens de volledige agenda aan:

Digitaal Rechercheren basisopleiding
- februari
- april
- mei

Digitaal Rechercheren vervolg
- maart
- mei
- september
- december

CISSP (Certified Information Systems Security Professional)
- maart
- juni

Security & Hacking
- april
- augustus
- oktober

COLOFON: UITGAVE VAN FOX-IT DECEMBER 2005.

REDACTIE: DOMINIQUE DE GAST - E-MAIL DE.GAST@FOX-IT.COM - OLOF PALMESTRAAT 6 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