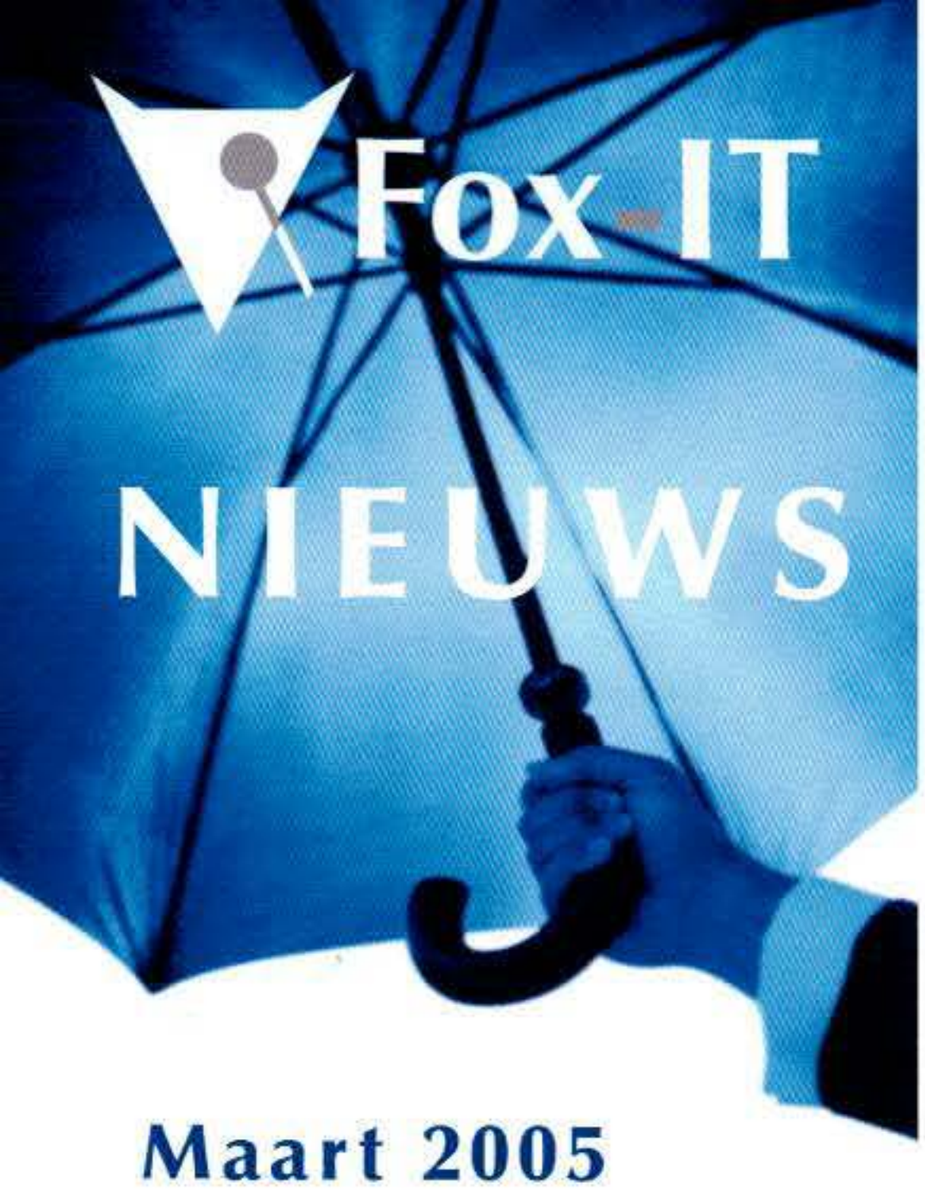


Fox-IT NIEUWS

Maart 2005

CISSP

Samenwerking met Interseco

Voorbeeldcase: Uitwisseling vertrouwelijke informatie

Fox Honeypot Project

Nieuwe Security Expert

Partnership met Secunet zeer succesvol

Trends, resultaten en actualiteiten MSS

Nieuwe Training

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

Algemeen

Fox-IT in een nieuwe jas

Er is veel gebeurd de afgelopen maanden. Helaas kan ik over de meest spannende zaken niets vertellen. Behalve dan misschien dat we dankzij het zwijgen over onze echte werkzaamheden een zodanige indruk hebben gemaakt dat de Carp Coolest Company Award deze keer aan ons is toebedeeld. Een enorme beker staat nu dan ook in onze ontvangstruimte. Ik heb mij er over verbaasd maar zo blijkt dat, door je zaken goed geheim te houden, er toch de juiste indruk kan worden gegeven.

Over de iets minder spannende, overigens wel belangrijke, zaken kan ik meer zeggen. Het jaar 2004 is voor Fox-IT een uitstekend jaar geweest. Door de aanzienlijke groei en uitbreiding van onze activiteiten hebben we onze organisatie verder gestructureerd door een verdeling te maken in vijf **business units**. Deze onderverdeling is ook terug te zien op onze website en in de indeling van deze nieuwsbrief.

De unit **Forensics & Audits** heeft het wederom enorm druk gehad in de maanden rondom de jaarwisseling met diverse rechercheonderzoeken en audits. De nieuwe unit **Crypto** heeft boven verwachting gepresteerd in 2004 en heeft de eerste crypto producten reeds opgeleverd. De unit **Projects** heeft veel gewerkt aan extra beveiligde netwerk omgevingen. Interessant is eveneens het onderzoek dat is gedaan naar internetmisbruik met behulp van honeypots, met nog schokkender resultaten dan verwacht (zie pagina 3). De Managed Security Monitoring service heeft het afgelopen jaar een behoorlijke vlucht genomen binnen de unit **Managed Security Services**. Miljoenen alerts zijn door het expert systeem van MSM verwerkt in 2004. Een overzicht staat onder het kopje MSS in deze nieuwsbrief. De vijfde unit is **Training**. De Security & Hacking praktijktraining is opnieuw aangepast aan de laatste ontwikkelingen, waaronder natuurlijk de wireless problematiek.

Onlangs is een aanzienlijk deel van onze experts, waaronder onze docenten, CISSP'er geworden (zie p. 6). De benodigde kennis is absoluut relevant in ons vakgebied. Daarom worden op dit moment voorbereidingen getroffen om de CISSP training aan onze trainingsportefeuille toe te voegen.

Het verder groeien heeft echter zo zijn voor- en nadelen. Enerzijds worden we steeds vaker als expert gevraagd door actualiteitenprogramma's als NOVA en 1opdeMiddag. Anderzijds groeien we uit ons jasje in ons huidige pand. Dit betekent dat we tot onze spijt de volledig beveiligde locatie in Rijswijk binnenkort gaan verwisselen voor een ruimere jas in Delft. Uiteraard net zo goed beveiligd!

Menno van der Marel
Directeur

Coolest Company

Door de unieke combinatie van digitaal detective werk en beveiliging op het hoogste niveau hebben we onder andere de pers gehaald door het winnen van de 'Carp Coolest Company Award 2004', een prijs die vorig jaar voor de vijfde keer werd uitgereikt door het vacaturemagazine Carp.

Forensics & Audits

Vanaf de start heeft Fox-IT zich intensief bezig gehouden met het uitvoeren van forensische IT onderzoeken. Nu, ruim vijf jaar later, voert de business unit Forensics & Audits nog steeds met dezelfde toewijding en professionaliteit onderzoeken uit. In de afgelopen jaren is de kennis omtrent de technische mogelijkheden en de operationele werkwijze sterk verbeterd. Inmiddels is Fox-IT een officieel erkend Particulier Recherchebureau en ontstaat ook bij (potentiële) cliënten steeds meer erkenning voor dit vakgebied. De praktische manier en de forensische inslag waarop Fox-IT IT security audits uitvoert heeft steeds meer navolging gekregen bij onze 'vakbroeders'. In 2005 staan verdere professionalisering en extra investeringen in R&D op het programma.

Samenwerking met Interseco

Fox-IT heeft in het verleden al meerdere malen zeer succesvol met het particuliere onderzoeksbureau Interseco samengewerkt. Daar waar de expertise van Fox-IT op het technische vlak ligt en met name binnen een ICT-omgeving, heeft Interseco ruimschoots ervaring in het verrichten van (tactisch) fraude- en observatieonderzoek voor bedrijfsleven en overheid in het algemeen en het verrichten van toedrachtsonderzoeken voor verzekeraars in het bijzonder.

Naast de onderzoekswerkzaamheden is Interseco gespecialiseerd in de uitvoering van persoonsbeveiligingsactiviteiten, het verzorgen van verhoogde rijvaardigheidsopleidingen en het geven van praktische workshops bijvoorbeeld met beveiligingsthema's als toegangsbeheersing en omgang met agressie.
De deskundigheid en hoge professionaliteit van Interseco sluiten aan bij de expertise van Fox-IT en dragen bij aan een hoog kwalitatieve uitvoering en afhandeling van de gezamenlijke opdrachten. Voor meer informatie over Interseco kunt u terecht op de website: www.interseco.nl.

Interseco

Crypto

Deze business unit, waarbinnen de apparatuur ontwikkeld wordt voor de bescherming van staatsgeheimen, bestaat nu één jaar. Fox Crypto heeft in dit eerste jaar bewezen dat het in zeer korte tijd in staat was om de activiteiten van Philips Crypto goed over te nemen. Dat heeft zich geuit in de ontwikkeling van een nieuwe versie van de C-kaart, genaamd Fort Fox File Encryptor (FFFE). Met de FFFE kunnen gerubriceerde bestanden tot en met het niveau Staatsgeheim Geheim versleuteld worden. Na versleuteling mogen de bestanden via elk medium, dus ook via het internet, verstuurd worden.
In 2004 is er tevens een start gemaakt met de ontwikkeling van de hardware datadiode. Door middel van deze datadiode kunnen twee netwerken gekoppeld worden die elk een ander rubriceringsniveau hebben. Op deze manier kan zelfs een eenrichtingskoppeling tot stand worden gebracht tussen het internet en een Staatsgeheim Geheim netwerk. De verwachting is dat dit product in 2005 door het NBV (Nationaal Bureau Verbindingsbeveiliging) geëvalueerd zal worden.

Fox-IT

Fox Crypto
Cryptographic Products

Partnership met Secunet zeer succesvol

In augustus 2004 heeft Fox-IT een partnerovereenkomst gesloten met het Duitse Secunet. Secunet is de fabrikant van de SINA VPN-oplossing. Bij een aantal cliënten zijn netwerken op basis van SINA inmiddels succesvol opgeleverd. De verwachting is dat SINA-VPN dit jaar goedgekeurd wordt voor het gebruik op staatsgeheimniveau.

secunet

Projects

De business unit Projects bestaat uit ervaren security-architecten, ontwikkelaars en programmeurs. Zij houden zich bezig met het creatief oplossen van complexe beveiligingsproblemen.
De oplossingen zijn pragmatisch en helder met een hoog veiligheidsniveau. De afdeling Projects gebruikt de meest geschikte bestaande producten in combinatie met zelf ontwikkelde high-end security producten en specifiek maatwerk voor de cliënt.

Door deze combinatie past het resultaat precies bij de bestaande bedrijfsprocessen en zijn aanpassingen veelal eenvoudig door te voeren. Aan het gewenste veiligheidsniveau wordt uiteraard geen enkele concessie gedaan.

Naast externe projecten houden de medewerkers zich permanent bezig met het verder ontwikkelen van het expertsysteem Plato van onze Managed Security Monitoring service.

Voorbeeldcase:
Uitwisseling vertrouwelijke informatie

Onlangs heeft Projects een sterk beveiligde infrastructuur opgeleverd voor een opdrachtgever waarbij vertrouwelijke informatie wordt gecommuniceerd tussen laptops, digitale zakagenda's (PDA's), thuiswerkplekken en het kantoor. De communicatie vindt plaats via internet en GPRS.
De beveiliging bestaat uit een combinatie van een VPN oplossing, sterke authenticatie met certificaten en Managed Security Monitoring. De oplossing stelt de medewerkers in staat wereldwijd real time vertrouwelijke informatie uit te wisselen.
Op deze manier kan efficiënt gewerkt worden in een vertrouwelijke omgeving en door direct beschikbare informatie kunnen beslissingen tijdig worden genomen.

Fox Honeypot Project

Een honeypot is een informatie- en/of computersysteem, dat speciaal is opgezet om gehackt te worden door derden. Honeypots kunnen worden gebruikt om aanvallen te voorkomen en te detecteren; Fox-IT heeft in 2004 eigen onderzoek gedaan naar digitale dreigingen op internet, waarbij gebruik is gemaakt van deze honeypot-technologie.

De onderzoeksopstelling werd vaak aangevallen om financiële redenen, zoals het versturen van valse en ongewenste e-mail. Deze is veelal bedoeld om persoonlijke informatie van mensen te achterhalen, zoals financiële gegevens, creditcard nummers en wachtwoorden. Dit wordt ook wel 'phishing' genoemd. Verder werd van de systemen gebruik gemaakt om gebruikersaccounts en creditcardgegevens uit te wisselen en om aanvallen uit te voeren op andere computersystemen en netwerken.
Een andere onderzoeksopstelling is gebruikt om het surfgedrag van internetgebruikers die anoniem willen surfen op internet te onderzoeken. De onderzoeksopstelling is bekend gemaakt op internet als een zogenaamde 'anonieme proxy'. Gebruikers kunnen dan via deze server anoniem verder surfen.
De servers werden voornamelijk gebruikt om naar porno te surfen, te chatten, websites te hacken en om kraakprogramma's en serienummers te downloaden. Het is schrikbarend hoeveel illegale activiteiten in korte tijd ontdekt zijn gedurende het onderzoek, dat zes maanden heeft gelopen. Het ziet er naar uit dat dergelijke dreigingen in de toekomst alleen maar zullen toenemen.
Uit dit onderzoek blijkt dat Windows en Linux computersystemen die aan internet gekoppeld zijn, worden blootgesteld aan een continue stroom van aanvallen. Hoewel de meeste aanvallen niet succesvol zijn is de gemiddelde overlevingstijd van een slecht geconfigureerd Windows-systeem slechts enkele minuten. De computer wordt in die tijd besmet door een van de vele virussen. De gemiddelde Linux distributie kent daarentegen een overlevingstijd van enkele maanden. De reden hiervan is dat een standaardinstallatie van een Linux distributie vaak veiliger is dan die van een Windows variant. Daarnaast worden de meeste virussen voor het Windows platform ontwikkeld.

Nieuwe Security Expert

Per 1 januari dit jaar is Christian Prickaerts aangenomen om de business unit Projects te versterken. Hij houdt zich bezig met de diverse projecten die bij cliënten worden uitgevoerd. Christian heeft onder andere specifieke kennis over beveiliging in combinatie met grote Windows omgevingen en Citrix. Deze ervaring heeft hij opgedaan binnen de Universiteit van Maastricht, waar hij tevens lid was van het lokale CERT team waarbinnen hij als incident handler fungeerde. Daarnaast is hij al een aantal jaren GSEC (GIAC Security Essentials Certification) gecertificeerd.

Managed Security Services (MSS)

Voor de handhaving van een minimaal vereist beveiligingsniveau is een kwalitatief hoogwaardig dagelijks beheer van de beveiligingscomponenten essentieel. Naast preventie is bovendien tijdige detectie van beveiligingsincidenten absoluut noodzakelijk. Fox-IT biedt haar cliënten daarom de mogelijkheid om continu van de expertise van Fox-IT gebruik te maken in de vorm van de business unit Managed Security Services. Fox-IT biedt haar geleverde beveiligingsoplossingen zoals firewalls, VPN's en PKI systemen daarom ook in een beheerde variant aan.
Tevens biedt Fox-IT een hoogwaardige Managed Security Monitoring dienst aan, waarbij de netwerken van cliënten 24x7 gecontroleerd worden op verdachte gebeurtenissen. Voor de continue dienstverlening beschikt Fox-IT over een eigen Security Operations Centre (SOC).

Trends in MSM detectietechnieken

**Steeds meer organisaties komen tot de conclusie dat het essentieel is om op de hoogte te zijn van wat er zich afspeelt op het bedrijfsnetwerk om de bedrijfsrisico's te verlagen.
Verkeerd geconfigureerde computersystemen, virussen en wormen, kwaadwillende medewerkers en hackers op het netwerk kunnen leiden tot ernstige incidenten. Een continue bewaking is dan de enige manier om goed inzicht te verschaffen. Menig bedrijf wordt geconfronteerd met een tekort aan kennis, expertise en mankracht; uitbesteding is vaak de beste keuze.**

Voor een effectieve bewaking is een nieuwe generatie intelligente detectiemethodieken noodzakelijk. Geavanceerde correlatie tussen meldingen afkomstig van netwerksensoren, actieve beveiligingscomponenten en kwetsbaarhedeninformatie van de betreffende systemen ontbreekt nog bij alle bestaande producten. Bovendien is er een slimme manier voor het detecteren van afwijkingen (anomalies) en trendanalyse vereist voor een hoogwaardige technologische detectieoplossing. Fox-IT werkt dan ook aan de verdere ontwikkeling van aanvullingen op haar MSM dienst, zoals:

- een integratie met managed vulnerability scanning (MVS)
- koppelingen met firewalls
- antivirus-systemen via syslog
- een host-based Intrusion Detection System-component (HIDS).

De behoefte aan mobiliteit dwingt bedrijven om WiFi in te voeren. De beveiliging hiervan baart menig persoon echter zorgen. Met een juiste combinatie van versleuteling en PKI certificaten is een veilige communicatie goed mogelijk. Toch kunnen dan nog steeds achterdeuren wagenwijd openstaan doordat illegale toegangspunten worden aangesloten (rogue access points). De meest voor de hand liggende achterdeur wordt echter altijd vergeten; het mobiele systeem zelf. Dit is meestal de laptop of PDA maar ook draadloze apparaten zoals de Airport van Apple kunnen de beveiliging omzeilen. Niet altijd kunnen deze systemen worden voorzien van persoonlijke firewalls en andere maatregelen. Juist dan kan Fox MSM uitkomst bieden. Detectie van illegale access points is nu reeds mogelijk. Geavanceerde detectie van rechtstreekse aanvallen op mobiele systemen via de WiFi verbinding zullen naar verwachting binnenkort aan de service worden toegevoegd.

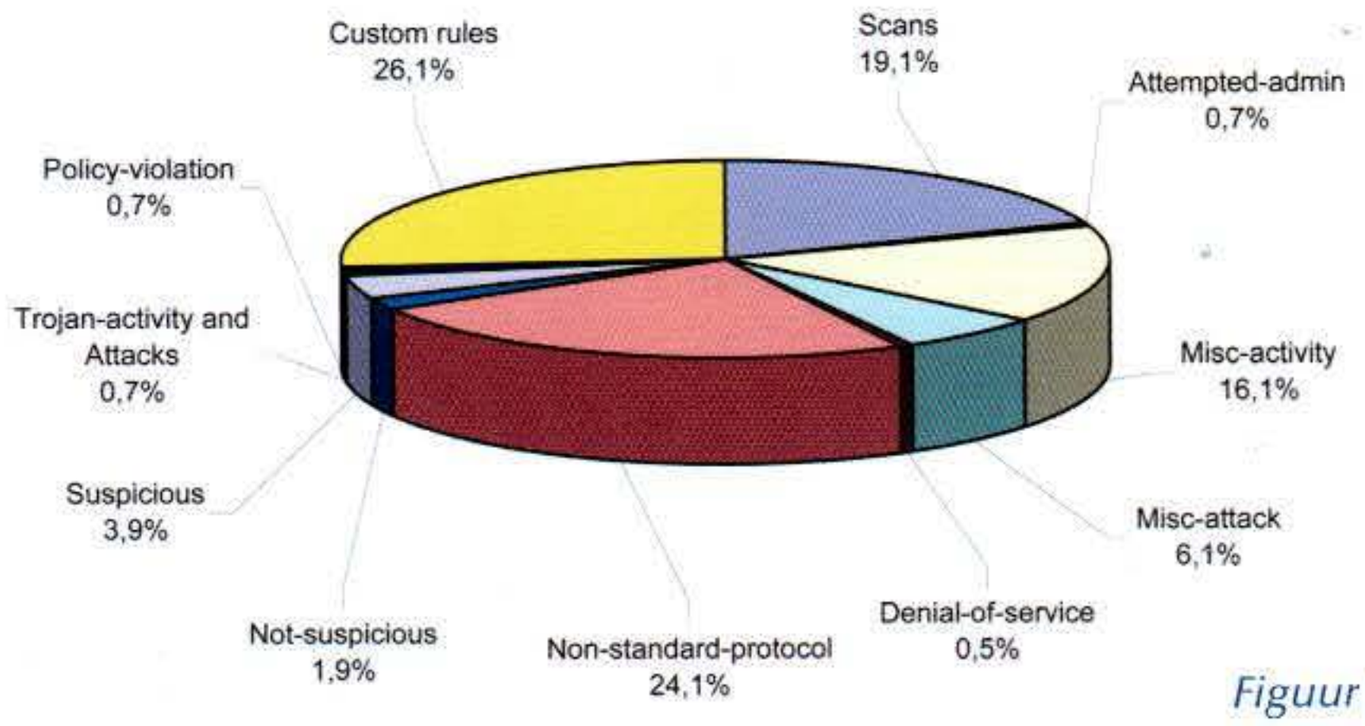
24x7x365 bewaking

De resultaten over 2004

In 2004 heeft het SOC ruim 5,6 miljoen alerts verwerkt afkomstig van de sensoren opgesteld in cliëntnetwerken (zie fig. 1). Ruim 180.000 zijn verwerkt als meta-alerts en vervolgens geanalyseerd. Afwijkend gebruik van protocollen in combinatie met portscans komen voornamelijk veel voor. Een groot deel van de meldingen is afkomstig van maatwerkinstellingen.

Vervolg op p. 5

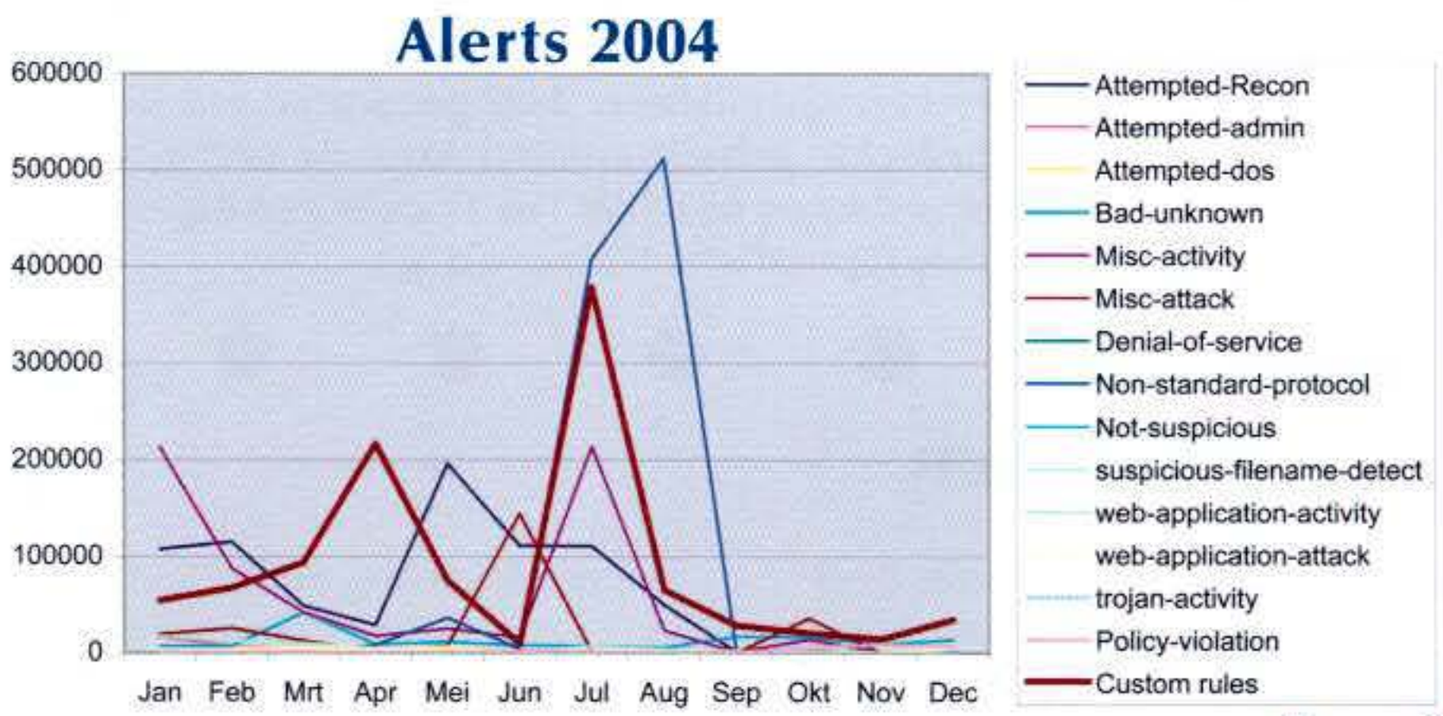
Verdeling van de meldingen (Alerts)



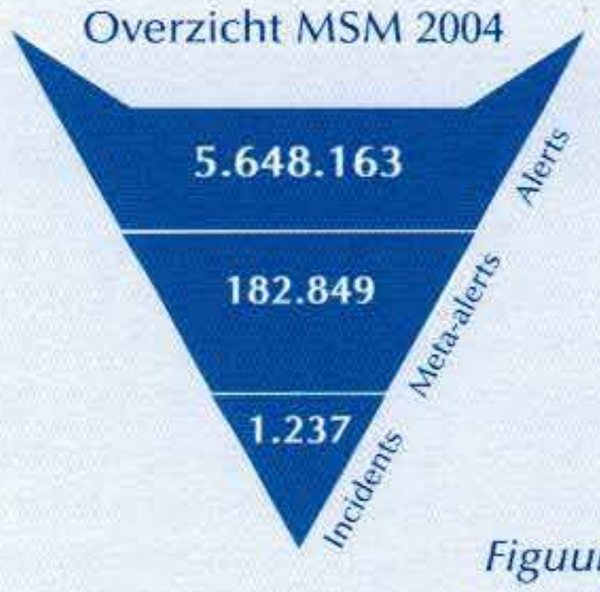
Figuur 1

Vervolg pagina 4

Zo zijn bijvoorbeeld sensoren voor een bepaalde periode ingezet voor forensische doeleinden. Denial of Service (DoS) en Trojan activiteiten werden in totaal respectievelijk 442 en 704 keer gemeld (zie fig. 2).
Opvallend is een piek in niet-standaard protocol gebruik in de periode juli/augustus (zie fig. 3).



Figuur 3



Figuur 2

Deze piek werd veroorzaakt door één onjuist geconfigueerde webserver en een nieuwe specifieke maatwerk sensor. In totaal deden er zich ruim 1200 beveiligingsincidenten voor waarvan in ruim 50 gevallen de cliënt binnen 15 minuten werd gewaarschuwd voor een sterk bedreigende situatie.

Hand-in-hand:

WBP, NEN 7510, Sarbanes Oxley en monitoring

Menig bedrijf ondervindt een groeiende behoefte aan informatiebeveiliging voortkomend uit recente wetgevingen. In het bijzonder de Sarbanes Oxley (SOX) wetgeving, voor alle bedrijven die zaken doen in de USA, vereist een gedegen aanpak.

Organisaties moeten bullet proof procedures implementeren die manipulatie van financiële data uitsluiten. Interne procedures, evenals alle ondersteunende IT-middelen, moeten pogingen tot ongeautoriseerde wijzigingen kunnen tegenhouden en detecteren. SOX eist verder een scheiding van functies, externe controles, audits en inzage in (interne) financiële zaken. CEO's en CFO's moeten zich er eens per kwartaal van vergewissen dat de financiële- en IT-controles zijn geïmplementeerd en effectief zijn.

Dichter bij huis wordt de roep om betrouwbaarheid en integriteit van informatie ook steeds luider. Trends hierbij zijn de voortgaande digitalisering van bijvoorbeeld patiëntendossiers in de gezondheidszorg en allerhande telewerk mogelijkheden die verder gaan dan het lezen van e-mail alleen. Met name de wet bescherming persoonsgegevens (WBP2000) dwingt vaak tot een evenwichtig informatiebeleid. In de zorgsector zijn deze eisen en adviezen vertaald in de richtlijn NEN 7510 van het Nederlands Normalisatie-instituut, een rechtstreekse afleiding van ISO 17799.

Het (be)houden van inzicht, maandelijkse heldere management rapportages, en het implementeren van incident response zijn essentieel bij de ondersteuning en invulling van dergelijke wetgeving. Een continue (netwerk)bewaking om computermisbruik te voorkomen, tegen te gaan en op te sporen is daarbij een geoorloofd en effectief middel. Hierbij kan wel een spanning ontstaan met de persoonlijke levenssfeer van de gebruiker. Het College Bescherming Persoonsgegevens (CBP) geeft aan dat op grond van artikel 8f WBP, een werkgever een gerechtvaardigd belang heeft om een controle uit te oefenen en dit eventueel mag uitbesteden aan een derde. Hierbij dient de controle de privacy belangen van de betrokkenen in acht te nemen.
Managed Security Monitoring (MSM) is een passief middel van detectie in het kader van interne controle en beveiliging, welke bovendien niet gericht wordt ingezet tegen een specifiek individu.

24 x 7 bewaking van de bedrijfsnetwerken door een externe beveiligingspartner is dus een toegestane en effectieve maatregel die bijdraagt aan de implementatie van de diverse regelgevingen. Fox-IT zal het komende jaar dan ook veel aandacht besteden aan de Fox MSM diensten en aan het optimaliseren van de rapportages.

Contactpersonen

Forensics & Audits
Matthijs van der Wel

Projects
Menno van der Marel

Crypto
Ronald Prins

Training
Dave Engbers

MSS
Erwin van der Zwan

Nieuwe Business Unit Manager

Vanaf 1 oktober 2004 is Erwin van der Zwan in dienst bij Fox-IT als Business Unit Manager voor Managed Security Services.
Hij is verantwoordelijk voor de kwaliteit en continuïteit van de geleverde operationele diensten aan onze cliënten. Na zijn studie aan de TU Delft heeft Erwin ruim 10 jaar ervaring opgebouwd met Windows-, migratie- en security-projecten. De laatste jaren heeft hij gewerkt als Information Security Consultant bij Siemens. Gedurende 2005 zal zijn focus liggen op het uitbreiden van de Managed Security Services en de 24x7 bewakingsdiensten.

Training

Sinds een aantal jaren biedt Fox-IT twee zeer praktijkgerichte trainingen aan; *Security & Hacking* en *Rechercheren op de Digitale Snelweg*. Hierbij wordt, naast een deel theorie, de specifieke praktijkkennis die wordt opgedaan binnen onze andere business units overgedragen aan de cursisten. De 10-daagse training *Security & Hacking* beantwoordt essentiële vragen op het gebied van security, hacking, intrusion detection (IDS) en sporenonderzoek.
De training *Rechercheren op de Digitale Snelweg* leert een onderzoeker efficiënt en creatief gebruik te maken van de diensten van het internet en de onderliggende technieken voor het vinden van digitale sporen.
Naast deze trainingen geeft Fox-IT maatwerktrainingen op de vakgebieden van de verschillende business units.

Nieuwe Training

Ook onze docenten hebben in januari het CISSP-examen met succes afgerond, zodat Fox-IT Training zich nu kan richten op het ontwikkelen van een cursus die voorbereidt op dit examen. De titel 'CISSP' is een internationaal geaccrediteerde afkorting die staat voor een hoogstaand generalistisch inzicht in de beveiliging van informatie- en communicatiesystemen en hun wisselwerking in de kernprocessen van een bedrijf of de overheid.

CISSP

De titel CISSP* wordt verstrekt door (ISC)², de Amerikaanse organisatie die zich ten doel stelt het vakgebied Informatiebeveiliging te professionaliseren en bij te dragen aan standaardisering.

De toegevoegde waarde van het certificaat is vooral te vinden in het feit dat het een internationaal geaccepteerde term is, waardoor het aanwezige kennisniveau beter in te schatten is.
Regelmatig wordt de titel al gevraagd bij vacatures en binnen de bancaire wereld wordt de titel ook steeds populairder. Vorige maand hebben 14 medewerkers van Fox-IT deelgenomen aan het CISSP examen met als resultaat een slagingspercentage van 100%! Landelijk zijn er tot nu toe ruim 200 personen die de titel CISSP aan hun naam mogen toevoegen. De CISSP-certificering is de snelst groeiende standaard op het gebied van Security Management; ook in Nederland wint de titel snel terrein.

* Certified Information Security Systems Professional

Trainingen 2005

- ***Training Security & Hacking***

Module	Datum
Techniek: TCP/IP en Unix	4 april 19 sept. 14 nov.
Security	5 t/m 7 april 20 t/m 22 sept. 15 t/m 17 nov.
Hacking & Audits	8, 18 en 19 april 23 sept. en 10 en 11 okt. 18, 28 en 29 nov.
IDS & Sporen	20 t/m 22 april 12 t/m 14 okt. 30 nov. t/m 2 dec.
Wetgeving	25 april 5 dec.

- ***Training Rechercheren op de digitale snelweg***

Type	Datum
Basis	30 mei t/m 3 juni 31 okt. t/m 4 nov. 12 t/m 16 dec.
Vervolg	8 en 9 juni 21 en 22 dec.

Colofon

Uitgave van Fox-IT Forensic IT Experts B.V.
Maart 2005

Redactie
Dominique de Gast, e-mail de.gast@fox-it.com
Haagweg 137, 2281 AG Rijswijk ZH
Telefoon 070 - 336 99 99