Oktober 2003

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

PKI nu voor iedereen bereikbaar!

Uit marktverkenning is gebleken dat bedrijven met twintig tot tweeduizend werknemers veel communiceren via Internet en hun e-mail graag willen versleutelen en digitaal ondertekenen; dit is een van de meest gebruikte toepassingen van PKI (Public Key Infrastructure). Daarnaast wordt PKI door ondernemingen veelvuldig gebruikt om een Internet en Intranet structuur te beveiligen. Zoals u in de vorige nieuwsbrief heeft kunnen lezen, introduceerde Fox-IT begin dit jaar al de FoxPKI. Deze appliance is op de markt gepositioneerd met een bereik tot 50.000 certificaten. Het opzetten van een PKI was tot voor kort dan ook alleen voorbehouden aan grote organisaties die behoorlijk moesten investeren. Dankzij de lancering van Secure Identity, kortweg Sec-ID, is het veilig communiceren met certificaten nu voor iedereen binnen handbereik. De Fox-IT Sec-ID is namelijk al vanaf enkele certificaten inzetbaar.

Een half jaar gratis
Met de introductie van Sec-ID (www.sec-id.net) kan iedereen gedurende een half jaar gratis certificaten gebruiken. Daarna kunt u zélf beslissen of u van de certificaten gebruik wilt blijven maken. Nadat een aantal formaliteiten is afgerond, krijgt u een persoonlijk, afgeschermd deel van de Secure Identity website. Als beheerder (Registration Authority) kunt u vervolgens de door de medewerkers en/of relaties aangevraagde certificaten goedkeuren. Na autorisatie kan de aanvrager het certificaat ophalen, waarna bijvoorbeeld e-mail digitaal ondertekend kan worden.

Surft u dus naar www.sec-id.net en overtuig uzelf! Ook op de vakbeurs InfoSecurity 2003 demonstreren wij Sec-ID.

Nieuw!

GSM's serieus beveiligd tegen afluisteren dankzij de bluetooth crypto module

Binnenkort levert Fox-IT ook apparatuur waarmee u kunt voorkomen dat derden uw GSM gesprekken kunnen afluisteren. Wij hopen u op de komende vakbeurs InfoSecurity de eerste toestellen te kunnen presenteren.

Fox-IT heeft een unieke overeenkomst gesloten met het Zweedse bedrijf Sectra. Dit bedrijf is als enige op de wereld in staat gebleken om een GSM te ontwikkelen die door de NATO is goedgekeurd tot op het niveau van NATO Secret. De nieuwste ontwikkeling van Sectra is een losse bluetooth crypto module. Via dit kleine kastje en een normale mobiele telefoon die bluetooth ondersteunt, kunt u gesprekken voeren die door niemand af te luisteren zijn.

Het GSM netwerk is standaard voorzien van diverse maatregelen om te voorkomen dat uw GSM gesprekken op eenvoudige wijze afgeluisterd kunnen worden. De draadloze signalen tussen het toestel en GSM masten zijn versleuteld met de speciaal daarvoor ontwikkelde algoritmes A5/2 en A5/1. Het onderscheppen van het radiosignaal is technisch erg complex.

Vervolg op pagina 2

Intrusion Prevention Systems (IPS)

Voldoende redenen om nog even te wachten

Ze schieten als paddestoelen uit de grond: start-ups die allemaal vinden dat ze het ei van Columbus hebben uitgevonden. Het ei is in dit geval een apparaat dat voorkomt dat aanvallen van hackers kunnen doordringen in een netwerk.
Het detecteren van aanvallen met behulp van Intrusion Detection Systemen (IDS) begint dan ook meer en meer ingeburgerd te raken.
De waarde van detectie naast preventieve middelen als firewalls is inmiddels wel bewezen. Het zou dan ook een logische stap zijn om deze IDS systemen niet alleen een melding te laten geven aan een systeembeheerder, maar ook daadwerkelijk de kwaadaardige netwerkpakketten te laten blokkeren. Daarmee wordt het detectiesysteem weer een preventief systeem. Maar werkt het ook in de praktijk?

De voordelen van een Intrusion Prevention System (IPS) zijn duidelijk. Op één centraal apparaat wordt immers al het gevaarlijke verkeer geblokkeerd. De servers die beschermd worden, hoeven niet tijdelijk uit de lucht gehaald worden om ad hoc security patches te installeren. Daarnaast zijn de betere IPS oplossingen ook zelfstandig in staat de nieuwste updates te downloaden van de website van de fabrikant (vergelijkbaar met antivirus pakketten).

Vals ei

Helaas heeft dit ei van Columbus een aantal grote nadelen dat vaak onderbelicht blijft. Een bekende eigenschap van IDS oplossingen is dat ze nog wel eens "vals alarm" geven. De expertise van een Intrusion Detection Analyst is dan nodig om vast te stellen of er actie genomen moet worden of dat het vals alarm betreft.
Het zou vervelend zijn als de IPS oplossing de toegang tot een e-commerce omgeving verbiedt omdat het ten onrechte denkt dat een hacker een aanval uitvoert. Sommige IPS oplossingen gaan dan ook zo ver om gelijk het IP nummer van de (zogenaamde) aanvaller permanent te blokkeren. Wanneer hackers merken dat een IPS is geïnstalleerd, kunnen zij hier creatief gebruik van maken. Hierbij valt te denken aan het uitvoeren van aanvallen vanaf een "vals" IP adres , waardoor ze voor een groot aantal mensen de toegang tot de e-commerce omgeving blokkeren. Daarnaast is een IPS alleen in staat om verkeer te blokkeren wanneer dit systeem in de lijn tussen de hacker en het slachtoffer systeem is geplaatst. Dat heeft diverse nadelige gevolgen. Al het verkeer moet bijvoorbeeld door deze flessenhals gerouteerd worden, waardoor alle investeringen in een snel netwerk te niet worden gedaan. Daarmee is het ook een extra single point of failure geworden. Als het IPS uitvalt zijn de achterliggende systemen immers niet meer bereikbaar.

Voorzichtigheid geboden

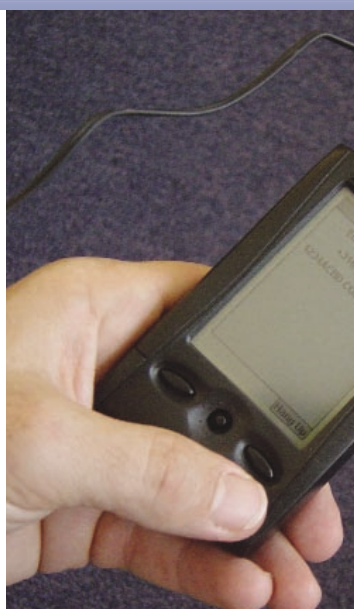
Is IPS dan iets dat totaal geen waarde heeft? Afgezien van de hierboven genoemde continuïteitsrisico's is het systeem natuurlijk wel goed in staat om bekende aanvallen zoals de recente Blaster worm tegen te houden. In de praktijk zijn voor dit soort aanvallen echter ook altijd patches beschikbaar die voorkomen dat het systeem nog kwetsbaar is. Het grootste gevaar van IPS schuilt in feit dat het als vervanging van IDS wordt beschouwd. Als een apparaat niet alleen de detectie maar ook de actie uitvoert, waarom zou ik dan nog willen weten wat er op het netwerk voor ongewenste zaken afspelen? Dit is misschien wel de belangrijkste reden om voorzichtig te zijn met IPS. Een IDS genereert dan weliswaar vaak teveel informatie, maar daartussen zit over het algemeen wel de informatie waaruit af te leiden is dat een hacker actief is. Het is de kunst van de Intrusion Detection Analyst om deze informatie goed te kunnen interpreteren. En zolang de expertise van deze analist nodig blijft voor het juist inschatten van de alerts, kan een IPS als zelfstandig opererend systeem nooit tegen Managed IDS op.

Vervolg van pagina 1

Sommige netwerken maken zelfs gebruik van zogeheten frequency hopping waardoor 217 keer per seconde van frequentie gewisseld wordt.

Waarom zou u investeren in deze toch wel kostbare bluetooth crypto module? Daar kunnen we meerdere redenen voor noemen. Zoals hierboven aangegeven zijn de draadloze signalen versleuteld. In het netwerk van de mobiele operator zijn deze gesprekken daarentegen in onbeschermde vorm beschikbaar. Voor onze Nederlandse GSM operators en overheid hoeven we niet zo bang te zijn, in het buitenland kan dat echter anders liggen. Daarnaast worden steeds meer aanvallen bekend op crypto algoritmen A5/1 en A5/2. Deze zomer presenteerden drie Israëlische cryptografen een methode om A5/2 te kraken in minder dan één seconde op een pc. Deze ontdekking wordt op dit moment gepatenteerd. Dat betekent dat er binnenkort apparatuur op de markt kan verschijnen waarmee GSM signalen uit de lucht te plukken zijn.
De bluetooth crypto module van Fox-IT maakt afluisteren daarentegen onmogelijk.

Voor meer informatie zie ook www.fox-it.com/Tigerxs.pdf.

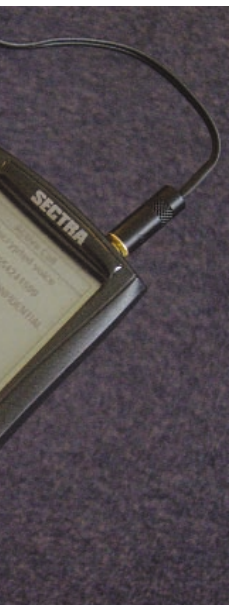


Houd virussen buiten de deur

De afgelopen maanden zorgden de computervirussen (of meer specifiek: wormen) Sobig.F en Blaster voor veel overlast bij zowel particulieren als be-drijven. Met name Sobig.F blonk uit in een ongekend hoog verspreidingstempo. Deze recente uitbraken tonen aan dat veel computersystemen nog steeds vatbaar zijn voor virusinfecties en dat de gevolgen steeds verstrekkender zijn. Hoe houd je infecties buiten de deur?

Een computervirus of -worm is een programma dat in eerste instantie zichzelf probeert te verspreiden naar andere computers, bijvoorbeeld via e-mail of netwerkverkeer. Daarnaast kan het een tweede, wellicht kwaadaardig, doel hebben zoals het wissen en/of stelen van computergegevens van de geïnfecteerde computer om te worden gebruikt in cyber attacks als Denial-of Service aanvallen. Het voortplantingsmechanisme van een dergelijk programma bepaalt of het als een virus of een worm wordt gekenmerkt. Een virus verspreidt zich door zich ongemerkt te hechten aan bestanden (heeft een drager nodig) terwijl worms zorgen voor hun eigen voortplanting.

Hoe ontstaat infectie?
Virussen en wormen maken gebruik van fouten in programmacodes van derden om zichzelf te kunnen nestelen in andere computers.
In het geval van Sobig.F en Blaster worden fouten in het besturingssysteem Microsoft Windows uitgebuit, maar ook andere platformen zijn in principe vatbaar.



Verspreiding van virussen en wormen gebeurt meestal via e-mail of via direct netwerk- en Internetverkeer. De eerste vorm van verspreiding is veelal te herkennen aan e-mail met vreemde onderwerpregels en uitvoerbare bijlagen.
De tweede vorm is zonder extra middelen minder snel te herkennen. Het gaat hierbij om een virus dat op allerlei manieren contact probeert te leggen met een andere computer om vervolgens een veiligheidslek uit te buiten. De computergebruiker merkt hier doorgaans niets van!

De infectie tegengaan
Het tegengaan van virussen gaat helaas niet vanzelf. Een blik op de site van Symantec, een van de grootste leveranciers van antivirus software, laat zien dat er dagelijks maar liefst drie à vier virussen of varianten op virussen worden ontdekt. Het is dus van belang om het gevaar van virussen niet te onderschatten en een actief antivirus beleid te voeren.
De volgende zaken kunnen onderdeel uitmaken van een dergelijk beleid:

- Installeer updates van programma's van softwarefabrikanten om ontdekte veiligheidslekken te dichten. Houd nauwkeurig in de gaten of de updates van alle gebruikte software binnen een onderneming ook daadwerkelijk geïnstalleerd worden. (Zoals het in oktober 2002 ontdekte Klez virus, dat zich nog steeds kon verspreiden door een programmafout in Internet Explorer uit te buiten, terwijl hier al in maart 2001 een update voor beschikbaar was!)
- Investeer in een goed geconfigureerde firewall. Naast een centrale firewall die een intern netwerk beschermd tegen aanvallen vanaf het Internet, zijn er ook software firewalls per werkstation beschikbaar.
- Investeer in goede antivirus software. Naast een centraal antivirus pakket dat alle in- en uitgaande e-mail controleert, kan voor ieder werkstation een antivirus programma geïnstalleerd worden om ook virussen die zich op andere manier verspreiden tegen te gaan.
- Zet zogenaamde 'services' uit, dit zijn elektronische diensten die computers kunnen aanbieden zoals webservers, dns-servers en bestandsdeling, als deze niet gebruikt worden. Op deze manier zullen eventuele veiligheidslekken in de services niet uit te buiten zijn.
- Beperk de toestroom van onbekende en/of onbetrouwbare bestanden. Laat werknemers geen software installeren die zij van huis meebrengen of van het Internet downloaden.
- Met een IDS (Intrusion Detection System) oplossing kunnen wormen vrij snel gedetecteerd worden en zijn snel passende maatregelen te nemen, zonder dat het hele netwerk plat gaat.

IT Security in het nieuws

De ontwikkelingen op het gebied van IT Security gaan in een razendsnel tempo. Achterblijven op dit gebied kan leiden tot kwetsbaarheden van het bedrijfsnetwerk en dient daarom voorkomen te worden. Het is dan ook van belang goed op de hoogte te blijven van de allerlaatste ontwikkelingen.

Op Internet zijn veel websites te vinden met nieuws over IT Security. We hebben voor u een selectie gemaakt van veel gebruikte nieuwssites:

- **http://www.securityfocus.com**
  Site met veel artikelen en columns op het gebied van IT Security en thuisbasis van een groot aantal beveiliging gerelateerde mailinglijsten.
- **http://www.securitydatabase.net**
  IT Security gerelateerde nieuwssite met een veelgebruikt forum.
- **http://www.dsinet.org**
  Nederlandse IT Security gerelateerde nieuwssite
- **http://www.security.nl**
  Nederlandse IT Security gerelateerde nieuwssite
- **http://www.hackinthebox.org**
  IT Security gerelateerde nieuwssite
- **http://www.cotse.com/**
  Site met columns en artikelen over IT Security

Mailinglijsten
Naast de verschillende websites waarop informatie verzameld kan worden, zijn er nog andere bronnen die gebruikt kunnen worden. Veel gebruikte bronnen van informatie zijn de verschillende mailinglijsten op het gebied van IT Security. BugTraq, te vinden op (http://www.securityfocus.com/archive) is hier een goed voorbeeld van. Via deze mailinglijst wordt informatie uitgewisseld over nieuw ontdekte beveiligingsproblemen, wormen en uitgebrachte patches.

Veilige vakbeurs: InfoSecurity 2003

Op 11 en 12 november a.s. vindt alweer de vijfde editie plaats van InfoSecurity, de vakbeurs op het gebied van informatiebeveiliging. In de Jaarbeurs Utrecht ontmoeten ruim 2.700 IT specialisten en beslissers uit de sectoren ICT, zakelijke dienstverlening, banken en verzekeringen, overheid en telecommunicatie elkaar. Meer dan 80 aanbieders en leveranciers van hardware, software en consultancydiensten op het gebied van IT Security, presenteren hier hun nieuwste producten.

Ook Fox-IT presenteert dit jaar weer een aantal noviteiten. Wij kunnen nog niet alles onthullen, maar zoals u verderop in de nieuwsbrief kunt lezen, demonstreren wij Secure Identity (Sec-ID). Deze unieke Fox-IT service is nu voor iedereen bereikbaar. Ook demonstreren wij Managed Security Monitoring. Voor beide diensten heeft Fox-IT een speciale beursaanbieding in petto! En alsof dat nog niet genoeg is, doet Fox ook nog een verrassende lancering. Reden genoeg dus om via www.fox-it.com gratis kaarten aan te vragen om een bezoek te brengen aan onze stand. Uiteraard kunt u voor de beurs een afspraak maken met een van onze medewerkers.

PKI Seminar: Droom, mythe of waarheid?

De weg naar een succesvolle PKI implementatie

Het is duur en lastig, kent veel organisatorische problemen en zitten juridische haken en ogen aan. Dat zijn de kenmerken die in de markt, en vooral bij het management, worden verbonden aan een PKI (Public Key Infrastructuur). Niets is echter minder waar. Een PKI implementatie is wel degelijk wenselijk voor organisaties. Vrijwel elke organisatie heeft immers behoefte aan veilige e-mailcommunicatie, veilig thuiswerken en beveiligde Internet transacties.

Een succesvolle PKI implementatie is dan ook absoluut geen droom of mythe. De waarheid is dat PKI organisatorisch afgedekt en technisch superieur te realiseren is, op een goed vertrouwelijkheidniveau én binnen het beschikbare budget van een organisatie. Fox-IT zal dit bewijzen tijdens het kosteloze PKI seminar dat zij op 28 oktober a.s. in Bilthoven organiseert.

Praktische stappen
Tijdens het seminar wordt, aan de hand van een organisatiemodel, samen met de deelnemers bepaald hoe de PKI het beste ingericht kan worden. Vervolgens wordt daadwerkelijk een PKI opgebouwd die aan het eind van de middag operationeel is.

Eigen PKI
Na afloop van het seminar ontvangen alle deelnemers het standaard stappenplan dat Fox-IT bij PKI projecten hanteert. Dit algemene stappenplan kan als leidraad dienen bij eigen PKI projecten. Ook krijgen alle deelnemers de beschikking over een volledig werkende eigen PKI gedurende 6 maanden.

Deelnemers seminar
Het seminar is met name geschikt voor (project)managers die met een PKI aan de slag willen en een pilot willen opstarten. Maar ook een ieder die interesse heeft in het onderwerp PKI is van harte welkom.

Meer informatie over het PKI-seminar en een inschrijfformulier is te vinden op http://www.fox-it.com/seminar/pki

Agenda

2003

- **28 oktober**
  Seminar Public Key Infrastructure 'Succesvolle PKI: Droom, mythe of waarheid?' Implementatie in één middag
- **27 t/m 31 oktober**
  Opleiding 'Security & Hacking, module 1 , 2 en start met module 3, Fox-IT, Rijswijk
- **10 t/m 14 november**
  Opleiding 'Security & Hacking', vervolg module 3 en 4, Fox-IT, Rijswijk
- **11 t/m 12 november**
  Fox-IT op Infosecurity.nl, Jaarbeurs Utrecht, Innovatieve producten en verrassende lancering!
- **24 t/m 28 november**
  Basisopleiding 'Rechercheren op de Digitale Snelweg', Fox-IT, Rijswijk

2004

- **9 t/m 13 februari**
  Basisopleiding 'Digitaal Rechercheren', Fox-IT, Rijswijk
- **8 t/m 12, 22 t/m 26 maart**
  Opleiding 'Security & Hacking', module 1, 2 en start 3 (8 t/m 12), vervolg 3 en 4 (22 t/m 26), Fox-IT, Rijswijk
- **29 t/m 31 maart**
  Basisopleiding 'Digitaal Rechercheren', Fox-IT, Rijswijk

Voor meer informatie over de opleidingen kunt u een e-mail sturen naar training@fox-it.com Meer informatie over de evenementen is op te vragen via fox@fox-it.com

Colofon

Uitgave van Fox-IT Forensic IT Experts B.V.
Oktober 2003

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