DKUUG-Nyt
Nr. 142 Oktober 2002

Temanummer

Sikkerhed

DKUUG
EurOpen

DKUUG-Nyt er medlemsbladet for DKUUG, foreningen for Åbne Systemer og Internt

Udgiver:
DKUUG
Fruebjergvej 3,
2100 København Ø
Tlf: 39 17 99 44
Fax: 39 20 89 48
email:
dkuugnyt@dkuug.dk
Sekretariatet er åbent:
Mandag - fredag
kl. 10.00 - 15.00

Redaktion:
Hanne Vilmann
(ansvarshavende)
Keld Simonsen
Henrik L. Kramshøj
Kristen Nielsen
Ulf Nielsen

Tryk:
Palino Print

Annoncer:
Kontakt DKUUGs sekretariat

Oplag:
3.000 eksemplarer

Deadline:
Deadline for næste nummer nr. 144 er tirsdag den 11. november 2002

Medlem af Dansk Fagpresse

DKUUG-Nyt
ISSN 1395-1440

Indhold

Leder

Efteråret 2002 har om noget stået i sikkerhedens tegn.
Alle firmaer og foreninger med respekt for sig selv kæmper om at lave de bedste sikkerhedsseminarer, med de bedste sikkerheds-eksperter.
Og det er ikke uden grund; det myldrer frem med eksempler på firmaer og offentlige instanser der har har huller i sikkerhedssystemerne:
Banker der bliver hacket - Rumforskningsprojekter der bliver offentliggjort.
Hvem har ikke hørt om Harald Nyborgs problemer?
DKUUG forsøger med forskellige sikkerhedskonferencer i oktober at komme rundt om problemerne og belyse dem fra flere sider.
Jeg havde inviteret Harald Nyborg til at komme med et indlæg, men de ønsker formodentlig ikke at deltage, da jeg aldrig fik noget svar fra dem.
De kunne ellers nok have lært en del af de tekniske medlemmer og seminar-deltagere som DKUUG har.
Vi har i dette nummer samlet en masse rigtig gode artikler fra nogle af de bedste sikkerhedseksperter.

God fornøjelse

Hanne Vilmann

Østerbro, den 4. oktober 2002
/hsv

DKUUG indkalder herved til generalforsamling.

Generalforsamlingen vil blive afholdt:

Den 27. november 2002 kl. 17.00

Symbion, lokale M1
Fruebjergvej 3, 2100 København Ø

Forslag fra medlemmer eller til medlemmer, der ønskes valgt til bestyrelsen skal ske skriftligt senest den 30. oktober kl. 12.00 til DKUUG´s sekretariat, Fruebjergvej 3, 2100 København Ø eller på E-mail sek@dkuug.dk.

Med venlig hilsen
DKUUG

DKUUG Sekretariat
Fruebjergvej 3, 2100 København Ø
Telefon: 39 17 99 44 • Telefax: 39 20 89 48
Email: sek@dkuug.dk
Http://www.dkuug.dk/
Giro: 137-8600
Bank: Jyske Bank, Lyngby Afdeling

DKUUG afholder generalforsamling onsdag den 27. november 2002 kl. 17.00 i Symbion, Fruebjergvej 3, 2100 København Ø

Deltag aktivt i DKUUG's udvalgsarbejde

Det er i udvalgene tingene sker. Og de er altid på udkig efter aktive og engagerede medlemmer.

Også du kan spille en aktiv rolle i DKUUG's arbejde ved at melde dig ind i et af foreningens udvalg. Henvend dig via mail til det pågældende udvalg, adresserne finder du på side 11 under "Info om DKUUG".

Router Security

By Rik Farrow

Like every other USENIX member, I am always learning. The resources appear endless: new books, classes, online Web pages, mailing lists, magazine articles, and questions that people send me. Just the other day some woman emailed me hoping I could tell her how to change the Admin password on the used notebook running XP she had just acquired.
I checked out my old favorite, a Linux boot floppy that allows you to change any password on a Windows NT system, and discovered that it might not work for Win2K (http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html).
At least the site with the bootdisk is still around.

The buzz for a while now has been attacks on Cisco routers. Now, you probably all remember that Cisco has had its share of security woes (not an unreasonable burdon, but still there). What has changed has more to do with rumours than reality--at least so far.

One rumour is that the source code for IOS, Cisco's Internetworking Operating System, have been stolen. That rumour dovetails nicely with a second rumour, that a rootkit for Cisco routers is in the wild. Rootkits for UNIX systems have been around since at least 1994. The "original" rootkit ran on SunOS, included trojanned commands that hid the existence of a sniffer and its log file, and made it easy for the installer to return and upload the logfile.
Some people really appreciated rootkits, as they were busy installing them on every open system they could find--particularly at ISPs.

ISPs made dandy places to install rootkits, especially in the mid-90's.
Small ISPs would install a UNIX mail/web server, and the attacker would load the rootkit on it. The UNIX server also would sit on a broadcast network, so any transit traffic would be sniffed as well. Of course, the accepted practice today is to put servers on their own subnets, and to use switches instead of hubs. Not that switches are a proven way to prevent sniffing.
Check out angst (http://angst.sourceforge.net/) if you don't believe me.

The notion of a Cisco rootkit disturbed me at first. I guess I just didn't like to think of a router as something running a vulnerable OS with vulnerable services. But, of course, routers run operating systems.
Cisco has written their own. Juniper Networks uses a modified version of BSD.

O'Reilley keeps publishing books, and occasionally sends me a copy, which I much appreciate. "Hardening Cisco Routers", by Thomas Akin, seems very appropriate for these days. And, Akin's tome secretly pleased me as well, because it covers much of the same turf that I once did in a router security class--but in more detail. For example, I didn't realize that the difference between logging into a Cisco router and what you can do after entering the enable password is based on privilege levels. You can actually set up user accounts (if you are using TACACS or RADIUS) with different privilege levels, then configure the router to provide access to sets of commands at any of the 16 different privilege levels. I had heard that IOS runs at a single hardware privilege level, and the notion of software configurable access to commands agrees with this. IOS is its own "secure" OS, although without the usual aid of hardware support. Like running a shell within the kernel.

Akin takes you through the hardening process succinctly, starting with a description of the issues, going into access control, passwords, remote authentication servers, logging, disabling dangerous protocols/services, controlling routing protocols, and even physical security. I had hoped there would be more on BPG4 filtering, but the focus was more on not accepting or distributing routes via IGPs, and setting up connection authentication with BGP4. I have always wanted to have all of the security documentation for Cisco routers in one place.
While "Hardening" does not include the firewall features of Cisco routers (other than rate limiting for DDoS attacks and which ICMP packets you can consider dropping), it admirably covers its topic area. And at 172 pages, its a quick read too.

The other oft-rumoured "big attack" on routers involves BGP4.
BGP, Border Gateway Protocol, is the glue that holds the Internet together. Unlike interior gateway protocols (IGPs), BGP uses Autono-

mous Systems (AS) Numbers to describe routes. An autonomous system is a collection of networks under the technical control of a single agency. The way I think about how BGP works is this. Each AS has routes to many networks that belong within that AS, their netblocks (see arin.net, ripe.net, apnic.net for the various AS and netblock registries). An AS advertises routes to their many networks via their AS number, rather than as specific routes through a list of routers. That makes routing within an AS transparent to sites outside of the AS. You just get the packets to the border of the AS, and the AS handles routing the packets to their destinations.

Of course, this setup implies that each AS must be using an IGP internally, so that its own routers know the actual routes to each supported network. What BGP4 does is take the information from the IGP routing advertisements, convert it to BGP4 advertisements, and share this with the BGP speaking neighbors. Only updates are distributed, as every update must be exchanged with every BGP4 speaker. Unstable networks result in frequent changes, or route flapping, wasting not so much network bandwidth as router CPU cycles.

Okay, so BGP4 is the glue and seems to be working just fine. What's the problem? A nice answer to that is AS7001, in April, 1997. AS7001 was the AS number for a small ISP in Florida, a Sprint customer. This ISP made a mistake in configuring BGP advertisements, so that all the routes that were being advertised internally were forwarded to Sprint using BGP4. As I understand it, this little ISP began advertising itself as the best route for many Class C networks, and as soon as this route spread, the link between Sprint and this little ISP became flooded. Imagine, if you will, the US airline system of spokes and hubs, and now Santa Rosa, California, has announced it has taken the place of San Francisco International, Altlanta Hart, Washington Dulles, Chicago O'Hare, etc., and all the traffic heads there. It was not a pretty picture. Cooler heads prevailed. By examining the BGP routing updates, someone noticed that AS7001 was declaring itself the best route for networks having nothing to do with it, and filtered all updates coming from AS7001.

The problem stopped once people started filtering (blocking) updates from AS7001, and gave Sprint a chance to help the little ISP fix their problem.

The AS7001 incident helped make NSPs aware of how crucial BGP filtering is.
Configuring BGP4 routing and filtering is an artform, and not practiced by many (compared to the number of network admins there are).
We haven't had a similar problem in years. Also, it is standard practice today to either use dedicated links between BGP4 neighbors, or include an MD5 digital signature with each packet, to prevent spoofing, resetting or hijacking of the connection between BGP4 neighbors which stays up as long as the link and routers are up.

This brings me back to where I started, to potential, wide-scale attacks on routers. If many routers can be penetrated, rootkits installed, then these routers become similar to the agents used in DDoS attacks. On command, if these routers begin sending incorrect BGP4 updates (from authenticated routers, mind you), then considerable disruption of the Internet will occur. With no one suspecting that their router has been corrupted, and general Internet connectivity being disturbed, well, things could get messy for a day or so. Just remember the original Internet Worm.
If you want to read more on this, check out the Internet Routing Instabilit Article by Craif Labovitz, et al (Arbor Networks): http://www.comsoc.org/confs/ieee-infocom/1999/papers/.
BBN and others have suggested using digital signatures on every update, but some people, including Labovitz, don't believe that router CPUs have the horsepower to handle digital signatures on top of everything else they are doing. For more on Secure BGP (S-BGP), check out http://www.ir.bbn.com/projects/s-bgp.

Note that this is not just a problem for router vendors. You can run BGP4 on Linux and BSD systems as well (MRTD, www.mrtd.net, and Zebra, www.zebra.org). And we know that these systems are always totally secure.

During DefCon 10, an annual hacker con in Las Vegas (in the summer time, with daily temperatures above 40C), I met with FX of Phenoelit

(www.phonoelit.de). FX explained to me how he and other members of Phenoelit had worked out a way to buffer overflow Cisco routers, and invalidate their flash memory. IOS also crashes as a result of this, and when it reboots and checks for a configuration file, the checksum is invalid. The router begins broadcasting for any server that can provide a configuration file, giving an attacker a giant chance to be very polite and provide one.

FX, being a visitor to the US, made very certain that I (and any US Federal Agencies, as well as Cisco) knew that he did not reverse engineer any Cisco code to create this attack. What he used was access to low-end Cisco routers, removing the cover (which reveals a Motorola 68K CPU), error messages from this router, and online documentation from Cisco. From this information, FX deduced the structure of heap entries (used for any allocated memory), and how to subvert these structures. FX did not want to become the Dmitri Skylarov of 2002 (Slylarov was arrested in 2001 for revealing the Adobe eBook uses XOR with a fix string for encryption, a violation of the Digital Millenium Copyright Act, or DMCA; using XOR and a fixed string for encryption is incredibly lame). Later, a lawyer, Jennifer Granick of Stanford University, also attending DefCon 10, told me that reverse engineering per se is not a violation of the DMCA unless it involves bypassing copyright protection. And, in fact, FX and the other Phonoelit members did get to leave the US unmolested.

Rootkits for Cisco routers are fantasy and rumours right now. Having talked to FX, I now know that Cisco IOS is indeed an embedded system running as a kernel level process, designed about 1985. As a rumour-monger, I am strongly suggesting to you that you see to the security of any routers under your control. The little whispers I have been hearing remind me a lot of what was being said before the DDoS attacks of February 2000 occurred, and I really thought I should mention this.

Næste temanummer er om LinuxForum 2003

Og udkommer i februar 2003

VISHED FOR SIKKERHED

Af Claus Fonnesbech,
Kommunikationschef i PROTEGO

Ved du alt om dine IT systemer?

På trods af stadig mere avancerede sikkerheds-teknologier og konsulent-tilbud, afsløres der stadigt flere og flere sikkerhedsbrister hos danske virksomheder. Der er set flere hackerangreb indenfor de sidste 6 måneder end nogensinde før. Og disse tilfælde får masser af pressedækning. Hvem har f.eks. ikke hørt om huller i sikkerheden hos Harald Nyborg eller hos Økonomiministeriet?

At de mange sikkerheds-brister får lov at leve, er dog langt fra på grund af specifik software, tjeneste eller andet udstyr. I de fleste til-fælde hviler de lave sikkerhedsniveauer på den over-pressede IT-chef eller systemadministrator. Med dette menes, at IT-folk som oftest bliver bedt om at tage sig af flere sager hver dag, end der er timer til i dagen. Endvidere fyldes tiden typisk op med drifts-problemer ("...min e-mail virker ikke, kan du..?"). Den værdifulde tid kan dermed ikke benyttes til detaljerede analyser (hvor skal man dog starte?) og den nødvendige opdatering og sikring. Og dette er på trods af, at en neglige-ring af nye sikkerheds-brister, potentielt set kan betyde mistet forretning og måske en betydelig forringelse af det image, som man har brugt mange markeds-føringskroner på at opbygge.

Markedet for IT-sikkerhed udikler sig drastisk og ligeledes gør udbudet af sikkerhedsløsninger. Man kunne på baggrund heraf formode, at flere IT-professionelle ville se konsekvenserne på manglende sikkerhed i øjnene og yderligere sikre deres netværk. Ikke desto mindre er virkeligheden en helt anden, hvilket også pressehistorierne tyder på. Bestyrelser rundt omkring er blændet af mulighederne ved e-commerce, mens sikkerheden til stadighed ned-prioriteres i lighed med "andre udgifter". Og så er der den, om den uuddannede IT-ansvarlige, der mener at hans nyind-købte anti-virus og firewall installation er fyldestgørende, hvilket den meget sjældent er.

Som en samlet konsekvens af ovenstående (det er forskelligt fra virksomhed til virksomhed hvad der er den direkte grund til manglende sikkerhed) - synes mange at udvise en 'herlig uvidenhed' om de interne og eksterne risici, der eksisterer i stadig mere komplekse netværk.

Sikkerhedsbrister er grunden til, at enhver kan bryde ind og stikke af med kritisk data – oftest uden at virksomheden finder ud af det. I øjeblikket opdages og rapporteres ca. 30 nye system-sårbarheder om ugen, hvoraf omkring halvdelen kan klassi-ficeres som 'høj-risiko', med fulde administrator rettigheder til følge af en udnyttelse. Det er et faktum i moderne netværks-liv. Og selvom Microsoft's systemer naturligvis er mest ramt – er det langt fra ene-stående, at de rammes. Af alle rapporterede angreb i dette års første 6 måneder hos det amerikanske selskab Riptech, udgjorde angreb og udnyttelse af sårbarheder på UNIX og LINUX systemer hhv. 12% og 10%.

Kort sagt bør alle professionelle, der arbejder med IT, i højere grad bekymre sig om sikkerhed. Og et naturligt første skridt i denne sammenhæng kunne være at samle noget mere viden op. Viden er magt. Og med konsekvent viden om sit IT-sikkerhedsniveau, har man magten til at beskytte sine systemer.

Præsentation af alle talere ved sikkerhedskonferencerne

Ulf Munkedal

Den anerkendte sikkerhedsekspert Ulf Munkedal - direktør i Fortress Group og kendt fra den meget succesfulde virksomhed VIGILANTe - tidligere kendt under navnet Neupart & Munkedal.

Ulf Munkedal fortæller om de seneste sikkerhedstrusler
Indlægget sætter fokus på de seneste sårbarheder der er blevet kendte. Hvad er deres natur? Hvilke systemer truer de? Hvem finder disse nye sårbarheder - blackhats, whitehats eller greyhats? Har vi brug for blackhats? Er full disclosure godt eller skidt?

Foredraget finder sted mandag den 7. oktober kl. 09.00

Carsten Stenstrøm

Carsten Stenstrøm der er IT-Sikkerhedschef i Danske Bank

Han fortæller om hvordan Danske Bank har sikret sig mod hackere.

Foredraget finder sted mandag den 7. oktober kl. 10.00

Ib Alfred Larsen

Ib Alfred Larsen er IT-chef i Datatilsynet

Ib Alfred Larsen vil føre deltagerne gennem junglen af love og krav til systemerne.

Foredraget finder sted mandag den 7. oktober kl. 11.00

Ken Willen

Teknisk chef og medstifter af Fort Consult.

Fortæller om effektive hacker- og virusberedskaber og hvorfor virus- og hackerberedskaber er nødvendige. Han beskriver, hvad de bør indeholde og hvilke overvejelser der bør ligge bag at etablere dem. Deltagerne får desuden gode råd om hvordan man kan begrænse skaden som en virus - eller en hacker - kan forårsage. Og hvordan man finder ud af, at de er på spil.

Fordraget finder sted torsdag den 10. oktober kl. 13.00

Jan Minche Nielsen

Sikkerhedschef hos Cybercity A/S.

Jan Minche Nielsen fortæller om"IT-sikkerhed og hjemmearbejdspladsen:

Hvilken funktion har hjemmearbejdspladsen? Hvilke sikkerhedsforhold bør en virksomhed overveje, når hjemmearbejdspladser skal etableres? Gennemgang af mulige sikkerhedsløsninger - fordele og ulemper. "

Foredaget finder sted torsdag den 10. oktober kl. 11.00

Jacob Thomsen

Grundlægger og administrerende direktør, NetGroup A/S

Jacob Thomsen introducerer ganske kort NetGroup Data Center og tager så lidt løs snak om at sikkerhed er mange ting. Det er sikkerhed omkring fysisk adgang til servere, det er sikkerhed omkring at sikre sig mod hacker etc. angreb på sine servere ved patchning, firewalls, monitorering etc. og det er sikkerhed i form af redundans og clusterløsninger.

Foredraget finder sted torsdag den 10. oktober kl. 10.00

Iraj Bastar

Sikkerhedskonsulent TDC Internet IT Sikkerhed

Iraj Bastar fortæller om log-opsamling og overvågning.

De fleste virksomheder opsamler idag loginformation fra et væld af systemer. De færreste bruger dog denne information aktivt. Hvorfor er det en god sikkerhedsmæssig foranstaltning at overvåge logfiler, hvilke udfordringer giver det og hvordan kan opgaven løses så den ikke kræver manuel gennemgang af tusindvis af loglinier?

Foredrager finder sted torsdag den 10. oktober kl. 09.00

Poul-Henning Kamp

FreeBSD udvikler, selvstændig.

Poul-Henning fortæller om hvorfor det er så svært at skrive sikre programmer, hvordan man gør det, hvorfor folk ikke gør det, hvordan udsigterne er for at de begynder på det og hvordan man på lang afstand kan se om der er ugler i mosen.

Foredraget finder sted mandag den 7. oktober kl. 14.30

Preben Andersen

UNI•C, leder af DK•CERT

Preben Andersen fortæller om hackerangreb i praksis: Hvilke typer hackere er der? Hvad er de ude efter? Hvordan angriber de typisk? Hvordan beskytter man sig mod hackerangreb?

Foredraget finder sted mandag den 7. oktober 13.00

Henrik Lund Kramshøj

Security Researcher fra IT-sikkerhedsfirmaet Neupart
Formand for Sikkerhedsforum

Henrik fortæller om IPv6

Foredraget finder sted onsdag den 9. oktober kl. 19.00

Henrik Størner

Tidligere Sikkerhedskonsulent hos Neupart og Munkedal, siden Vigilante, arbejder nu som systemadministrator hos CSC

Foredraget finder sted onsdag den 9. oktober kl. 20.00

Lars Neupart

Lars Neupart er idémand og stifter af Neupart A/S
og kendt fra den meget succesfulde virksomhed VIGILANTe - tidligere kendt under navnet Neupart & Munkedal.

Lars Neupart fortæller om Security awareness-programmer.
Hvordan en it-sikkerhedspolitik bliver til et redskab der giver forbedret sikkerhed.
Gennemgang relevante begivenheder og aktuelle trusler og den logiske sammenhæng der er imellem hændelser og awareness-programmer.

Foredraget finder sted torsdag den 10. oktober kl. 14.30

Information om DKUUG

Dansk Unix-system Bruger Gruppe (DKUUG) er en forening for IT-professionelle med interesse i og brugere af åbne systemer. Hvilket vil sige systemer som i stort omfang er bygget op omkring åbne standarder. Foreningen blev stiftet i 1983 og har i dag ca. 450 medlemmer.

Medlemsfordele

Udover det faglige netværk forenings-medlemmer imellem kan nævnes følgende:

- Medlemsblad som udkommer mindst 6 gange årligt
- Rabat på bøger gennem Polyteknisk Boghandel
- Rabat på abonnement på Computerworld og PC World
- Rabat på betalingsarrangementer (kurser, konferencer og seminarer)
- Mulighed for direkte at påvirke fremtidige IT-standarder gennem standardiseringsorganer
- Klubmøder i København den sidste tirsdag i hver måned
- Støtte til at afholde et for foreningen relevant arrangement inden for dit interesseområde

Medlemsskab

Der er fire forskellige medlemstyper alt efter ønsket omfang:

- Stormedlemsskab dækker alle virksomhedens adresser, søster- og datterselskaber og kan modtage op til 12 eksemplarer af medlemsbladet. Alle organisationens medarbejdere kan benytte sig af medlemsfordelene.
  Årligt kontingent kr. 11.024,- eks. moms.

- Organisationsmedlemsskab dækker kun organisationens adresse og kan registrere op til 4 modtager af medlems bladet. Alle organisationens medarbejdere kan benytte sig af medlemsfordelene.
  Årligt kontingent kr. 4.004,- eks. moms.

- Individuellemedlemsskab dækker kun én persons medlemsskab.
  Denne person modtager medlemsbladet på privat eller arbejdsadresse og kun den person medlemsskabet dækker kan benytte sig af medlemsfordelene.
  Årligt kontingent kr. 687,- eks. moms.

- Studiemedlemsskab dækker kun én person mens denne studerer.
  Registrering kan kun ske ved forevisning af gyldigt studiekort.
  Studiemedlemmer modtager medlemsbladet og kan benytte sig af medlemsfordelene.
  Årligt kontingent kr. 130,- eks. moms.

Kontakt:
DKUUG, Hanne Schmidt Vilmann
Fruebjergvej 3, 2100 København Ø
Tel: 3917 9944 Fax: 3920 8948
www.dkuug.dk - sek@dkuug.dk

Sikkerhedsløsning gennem backup

Af Bjarke Alling

I snakken om IT-sikkerhed må man ikke glemme en meget basal sikkerhedsregel, sikkerhedskopiering eller backup. Dette forhold er af afgørende betydning i utroligt mange sammenhænge og bliver ofte undervurderet i snakken om hvordan éns virksomhed eller organisation beskyttes bedst muligt mod uautoriseret adgang. Jeg vil i det efterfølgende komme med en række betragtninger og argumenter for hvorfor sikkerhedskopiering også giver mening i en IT-sikkerheds diskussion.

I gennem de 5-6 år hvor jeg har arbejdet med Linux har jeg set masser af eksempler på at maskiner er blevet kompromitteret. I alle tilfælde har disse hacks været gennemført med henblik på at udnytte serveren som videre springbræt til angreb mod andre servere. Aldrig mod den konkrete server. Ikke at det ikke sker, men jeg har aldrig personligt oplevet det. Adgang er lykkedes via en exploit i en applikation. Lige fra SSH til services som burde være lukket. Nogle gange burde disse hacks være undgået andre gange har det været mere gådefuldt hvordan det er lykkedes at komme ind. Faktum er at det sker og at uanset hvad vi som administratorer gør, vil det ske igen.

Daglig sikkerhed

Jeg er 100% enig i at man skal opdatere så hurtigt som menneskeligt og praktisk muligt, at man skal have en god password-politik, at man skal kontrollere åbne porte og kørende processer, at man skal benytte firewall når det giver mening og endelig benytte krypteret kommunikation. Alle disse metoder er absolut nødvendige og uden dem vil ens servere være lagt ned alt for hurtigt. Det ændrer dog ikke på det andet faktum at der stadig er huller: En enkelt pop3-bruger med et ringe password, en overset applikation som burde være opdateret - men ikke blev det - en ftp-session eller web-applikation uden kryptering eller et fejlagtigt konfigureret program såsom MySQL eller sågar Formmail. Altså masser af potentielle huller i éns omhyggeligt opbyggede sikkerhed.
Hvad kan man så gøre i en situation hvor man uanset éns indsats alligevel kan blive kompromitteret? Jo, én ting kan man i al fald gøre: Tage regelmæssige sikkedshedskopier af hele indholdet på serveren, ikke kun brugerdata, men alle data på alle servere.

Helt principielt bør der gennemføres en komplet sikkerhedskopi så snart en ny server sættes i drift. Derved er man helt sikker på at have en ren kopi af det aktuelle system. Denne første backup skal naturligvis følges op med regelmæssige daglige sikkerhedskopier. Ydermere bør man producere flere sæt komplette sikkerhedskopier. På denne måde er man 100% sikker på at kunne genskabe et rent system hvis skaden skulle ske og nogen fik uautoriseret adgang.
Nogen vil måske sige, at de har alle systemdata på de originale installationsmedier. Ja, det er korrekt, men i en lidt større installation er det ikke systemdata der fylder voldsomt og det er en klar fordel i restore-sammenhænge, at have et komplet system med alle opdateringer og tilretninger på en samlet sikkerhedskopi fremfor i flere mindre dele. Dette gør arbejdet med en restore mange gange nemmere og meget hurtigere.

Datatab ved et uheld

Når man taler IT-sikkerhed er der også andre aspekter end blot en scriptkiddie der kommer ind på éns systemer; det være et bevidst ønske om at slette data eller mere banalt at data blev slettet ved et uheld. Hvis nogen ønsker at slette data, kan det senere vise sig, endda meget, nyttigt at kunne fremdrage en intakt sikkerhedskopi og fra denne kunne bevise hvornår disse data senest var tilgængelige og hvem som havde tilgang til dem. Oplysninger der i en juridisk sammenhæng er meget værdifulde.
Slettes data ved en fejl, er det ubeskriveligt bekvemt at kunne genskabe dem hurtigt og korrekt.

Alle ovenstående betragtninger giver kun mening hvis det kombineres med et velfungerende backupprogram. I sammenhæng med Unix og specielt Linux har avancerede backupprogrammer ikke været særligt udbredte. Der har naturligvis altid været tar, cpio og dump, flere Open Source løsninger med blandt andet Amanda og Taper samt Arkeia, BRU og Tapeware blandt de mindre kommercielle. Blandt de større kommercielle findes i dag løsninger fra blandt andet Veritas, Legato, HP, Computer Associates (ARCserve)

kommercielle er det fortsat nyt at understøtte Linux, mens de alle har understøttet de forskellige Unix-varianter længe.

Alle løsninger har fordele og ulemper. For nogle gælder, at de ganske enkelt ikke er tilstrækkeligt avancerede, for andre at de er for vanskelige at anvende og endeligt at nogle er for dyre i anskaffelse og drift.

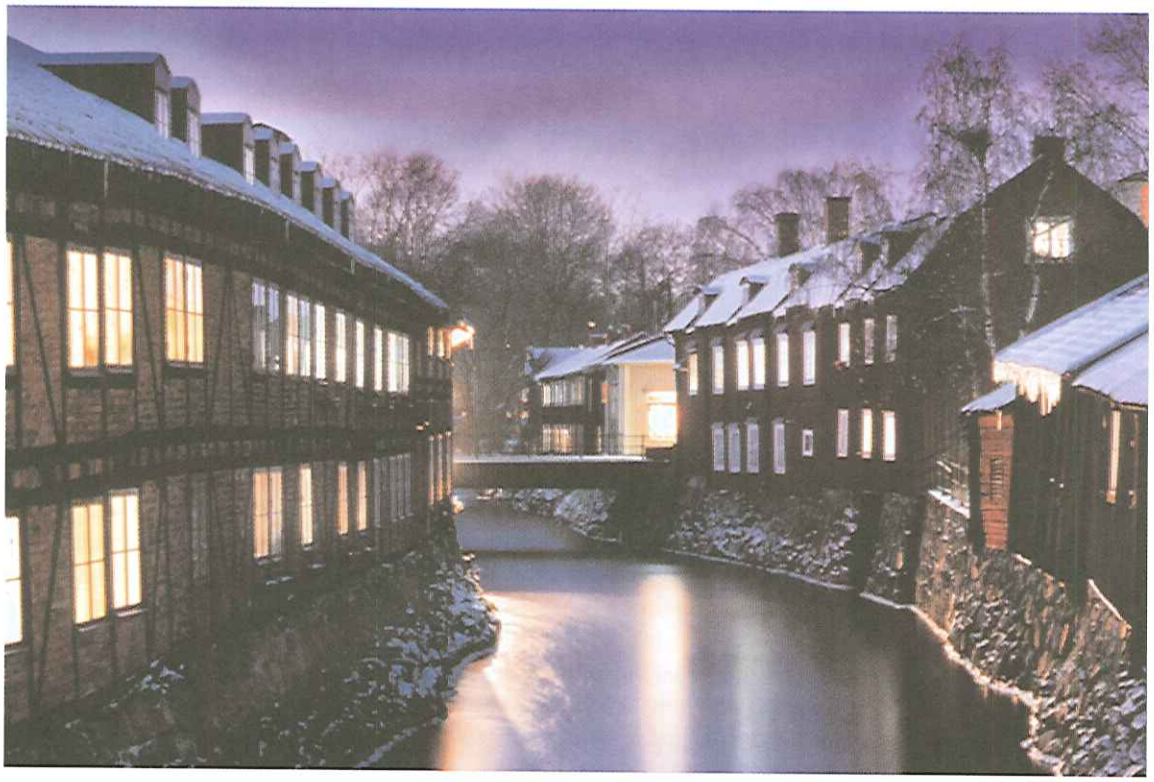
Backupløsning

I Liga LinDist har vi efter flere års søgen omsider fundet et program som vi mener både tilgodeser ønsket om en god kvalitet, avancerede faciliteter og en rimelig pris. Programmet er NetVault fra det engelske firma BakBone.
Med dette program har man som systemadministrator en backupløsning som kan håndtere sikkerhedskopiering i alt fra små netværk, enkelte servere til store anvancerede netværk med forretningsprogrammer såsom Oracle, MS SQL Server, MS Exchange og SAP/R3 eller endda MySQL. Dette til nogle meget fornuftige priser og efter en meget modulær program-opbygning. Ydermere er NetVault designet til at fungere 100% ens uanset hvilket operativsystem det afvikles på. Dette gælder Unix, Linux og Windows platformene. Det er en ægte netværksløsning, således at man som standard kan håndtere flere servere fra én grafisk brugerflade og man kan samtidig afvikle flere backupsessioner til forskellige bånd- eller harddiskenheder.

BakBone NetVault er en meget heterogen sikkerhedskopiløsning som efter min bedste overbevisning er et rigtigt godt fundament at bygge sin IT-sikkerhed på.

Bjarke Alling - Direktør Liga LinDist ApS - bjarke@liga.dk
København den 9. september 2002

Announcement



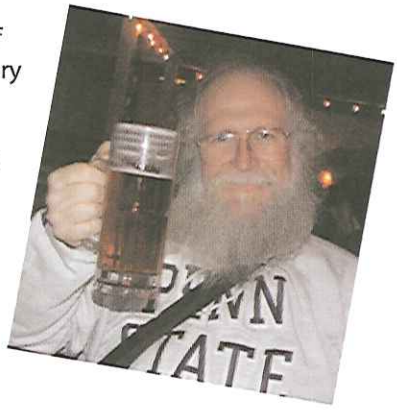
NordU2003 –
The fifth NordU/USENIX Conference
February 10–14, 2003
Aros Congress Center
Västerås, Sweden

NordU USENIX 2003

We would like to welcome everyone to Västerås (100 km east of Stockholm) and to NordU2003 – The fifth NordU/USENIX Conference.

As UNIX and Free Software becomes more and more widely adopted in corporations and academia we see a need to stay ontop of current trends.

The NordU/USENIX Conference offers a venue for developers, administrators and users of UNIX and UNIX like operating systems, to meet, talk and learn.



Jon "maddog" Hall will deliver one of the keynotes. Mr Hall has a long history of being involved in our community. We will take a special look at how Open Source Software, such as GNU/Linux, *BSD, Open Office and GNOME, is being used in government. For developers we have some exciting invited presentations on Java Technology as well as GNU Compiler Collection family of tools.

We look forward to meeting you all in Västerås!

http://www.nordu.org/NordU2003/

Programme

Monday, February 10 – Wednesday, February 12
Tutorial Programme

Thursday, February 13 – Friday, February 14
Technical Programme
Refereed Papers
Exhibition
Sponsors Presentations

Topics that will be covered:
Security
Operating Systems
Desktop
Tools
Backup Solutions
Applications
Open Source/Free UNIX
Interoperability

NordU2003

DKUUG har samlet en perlerække af danske sikkerhedseksperter. Det fulde program kan ses på www.dkuug.dk, hvor der også er mulighed for at tilmelde sig til de forskellige dage.

Program for 7. oktober 2002

Hacker – en hjælp eller en trussel ?

Kl. 08.30	Registrering og kaffe
Kl. 09.00	Ulf Munkedal - IT-sikkerhedsekspert
Kl. 10.00	Carsten Stenstrøm - IT-Sikkerhedschef i Danske Bank
Kl. 11.00	Ib Alfred Larsen - IT-chef i Datatilsynet
Kl. 12.00	Frokost
Kl. 13.00	Preben Andersen - UNI•C, leder af DK•CERT
Kl. 14.00	Kaffe med kage
Kl. 14.30	Poul-Henning Kamp - FreeBSD udvikler, Selvstændig.
Kl. 16.00	Afslutning

Pris for deltagelse incl. forplejning for medlemmer kr. 495,-
Ikke-medlemmer kr. 667,-
Tilmelding sendet den 3. oktober 2002

Program for 9. oktober 2002

Nørdet aften - gratis arrangement

Kl. 19.00	Henrik Lund Kramshøj – Ipv6
Kl. 20.00	Henrik Størner

Program for 10. oktober 2002

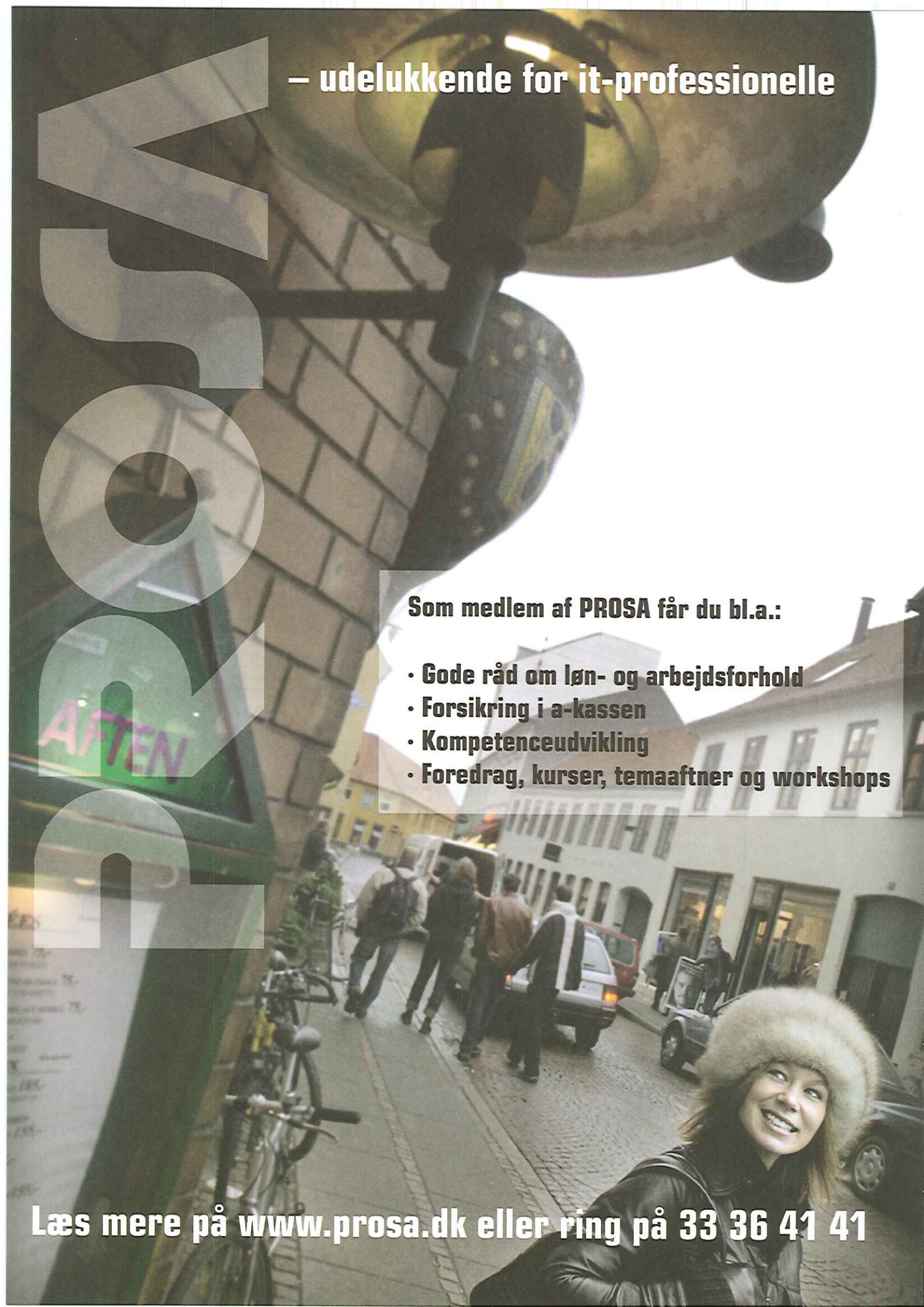
Hvordan kan man sikre sig ?

Kl. 08.30	Registrering og kaffe
Kl. 09.00	Iraj Bastar - Sikkerhedskonsulent TDC Internet IT Sikkerhed
Kl. 10.00	Jacob Thomsen - Direktør i NetGroup
Kl. 11.00	Jan Minche Nielsen - Sikkerhedschef, Cybercity A/S
Kl. 12.00	Frokost
Kl. 13.00	Ken Willen – Teknisk chef i Fort Consult
Kl. 14.00	Kaffe med kage
Kl. 14.30	Lars Neupart – Direktør i Neupart A/S
Kl. 16.00	Afslutning

Pris for deltagelse incl. forplejning for medlemmer kr. 495,-

Ikke-medlemmer kr. 667,-

Tilmelding senest den 8. oktober 2002


PROSA
– udelukkende for it-professionelle
Som medlem af PROSA får du bl.a.:
• Gode råd om løn- og arbejdsforhold
• Forsikring i a-kassen
• Kompetenceudvikling
• Foredrag, kurser, temaaftner og workshops
AFTEN
Læs mere på www.prosa.dk eller ring på 33 36 41 41

Trusselsbilledet er i hastig udvikling

Af Ulf Munkedal,
IT-sikkerhedsekspert og grundlægger af Fort Consult

Mange flere sårbarheder
Som ansvarlig for IT-sikkerheden i en virksomhed kan det være vanskeligt at overskue de mange nye sikkerhedstrusler, der bliver kendte hele tiden - så man kun bruger tid på at håndtere dem, der er relevante for ens egne systemer. Alene i år 2001 var der over 2400 nye sårbarheder – svarende til en stigning fra i gennemsnit 39 nye sårbarheder rapporteret pr. måned i 1999 til 203 pr. måned i 2001. Det svarer til ca. 10 nye trusler pr. arbejdsdag i år 2001. Og jeg forventer, at tallet vil stige til over 375 pr. måned i år.

Eksempler på alvorlige sårbarheder
Web server angreb (såkaldte defacements) er stadig en af de mest populære typer hackerangreb. I første halvdel af 2002, blev der fundet graverende sårbarheder i de to mest populære web server platforme, Apache og Microsoft IIS. Andre alvorlige sårbarheder har drejet sig om OpenSSH, en open source implementation af Secure Shell remote login protokollen.

Hacker scripts bliver tilgængelige hurtigere
Tiden fra, at disse sårbarheder blev kendte, og til, at man på nettet kunne finde såkaldte exploits og hacker scripts - altså grydeklare værktøjer, der kan udnytte sårbarheden - var bemærkelsesværdig kort. En trend, som jeg desværre tror fortsætter i den kommende tid. Vi må indse, at der er kommet meget fokus på nye sårbarheder - ikke kun fra sikkerhedsfolk og virksomheders side.

Eksempler på orme
Vi så også en del orme i første halvdel af 2002. En af de mest udbredte i årets første måneder blev uden tvivl den såkaldte JS/SQLSpida orm, der går målrettet efter de mange Microsoft SQL servere, som er tilsluttet nettet. I juli måned så vi en orm, der gik efter en af de nævnte Apache-sårbarheder (chunked encoding) på UNIX platformen BSD. Noget usædvanligt, fordi langt de fleste orme ellers har været rettet mod Microsoft systemer i de sidste 18 måneder.

Flere og farligere vira
En anden kategori er vira, og her er tendensen den samme som for sårbarheder. Ifølge sikkerhedsfirmaet MessageLabs er vi allerede oppe på dobbelt så mange vira, som distribueres via e-mail i år 2002 i forhold til hele sidste år. Dette viser en rapport, de offentliggjorde i juni 2002. Mange af de vira, der er kommet i udbrud, opsnappes heldigvis af antivirusprogrammerne, men opdateringerne når ikke altid ud til alle virksomheder i rette tid. Jeg kan fx nævne de meget omtalte Klez-varianter fra april/maj måned. Klez.H-virusen spreder sig eksempelvis via Outlook adressebogen, ICQ-databaser og lokale filer, og den har forvoldt stor skade i mange virksomheders IT-systemer.
Antivirusprogrammerne kunne ikke nødvendigvis modstå den i alle dens varianter. Samtidig er der i stigende grad tale om, at brugerne selv forårsager problemet i de såkaldte hoax-vira, når de fejlagtigt gør skade på deres egne systemer ved fx at slette vigtige filer.

Normalt god tid til opdateringer
Det kan lyde voldsomt og skræmmende med det stigende antal vira og sårbarheder - kombineret med at der er flere og flere, der forsøger at udnytte dem - og nemt kan gøre det ved hjælp af de lettilgængelige hackerprogrammer og orme. Og selv om de grydeklare værktøjer kommer på banen hurtigere, er der som regel rimelig god tid fra en ny type sårbarhed eller virus opdages, til de bliver en nævneværdig trussel - nemlig når hacker scripts bliver tilgængelige eller en virus for alvor begynder at sprede sig. Så det handler i virkeligheden om at organisere sine arbejdsprocesser, så den eller de sikkerhedsansvarlige i en virksomhed kan få nem adgang til informationer om nye sårbarheder og vira samt workarounds og patches til opdatering af dem - og sørge for at systemerne bliver omkonfigureret eller opdateret hurtigst muligt.

En skov af informationer
Det lyder forholdsvist nemt, men erfaringerne viser, at det ikke altid er det i praksis. Pga. det meget høje antal af sikkerhedstrusler, der bliver opdaget hver dag, bliver omfanget af de informationer, der skal holdes styr på, ret uoverskueligt. En virksomhed skal ikke blot sørge

for at fange de informationer, der er relevante netop for deres systemer, de skal også sikre sig, at de får det hele med. Og dette i sig selv er en kæmpe-opgave selv for større og mellemstore virksomheder. Hertil kommer, at de sikkerhedstrusler, som vurderes til at være relevante, skal prioriteres, så de mest alvorlige håndteres først. Og endelig skal hvert system, som truslen berører, opdateres på den rigtige måde - og det kræver, at der er tilstrækkeligt præcise oplysninger om, hvordan man håndterer sikkerhedstruslen, da de færreste virksomheder har specialister ansat, der selv kan udtænke workarounds og lave patches.

Uoverskueligt at følge med

Udover at bruge de workarounds og patches, som systemleverandørerne sender ud til deres kunder, er det nødvendigt at følge med på forskellige mailinglister og web sites for at være sikker på at få det hele med - og i god tid. Det kan være en ret uoverskuelig opgave for den IT-sikkerhedsansvarlige at skulle indsamle, sortere og vurdere alle de mange sikkerhedsinformationer fra alverdens forskellige kilder. Nogle af oplysningerne er måske irrelevante for virksomhedens IT-systemer, og nogle er for gamle eller for upræcise til, at man kan bruge dem. Og jeg oplever, at disse spredte informationer kan være med til at skabe panik, fordi man ikke er sikker på at få det hele med og selv skal kigge alting igennem og vurdere det. Mange frygter - og med god grund - at de har overset noget.

Early warning systemer hjælper

For at afhjælpe disse problemer og gøre livet lidt lettere for IT-sikkerhedsfolkene er forskellige såkaldte early warning systemer blevet udviklet og introduceret på markedet i løbet af det sidste års tid. Fort Consult har fx udviklet 2. generations early warning systemet StayAlert baseret på amerikanske SecurityFocus's anerkendte sårbarhedsteknologi. Systemet giver IT-sikkerhedsfolk nem adgang til informationer om de sikkerhedstrusler, som er relevante for deres virksomhed, lige fra det øjeblik truslerne er blevet kendte, så de har god tid til at håndtere dem. Da SecurityFocus har verdens største team af sikkerhedseksperter, der overvåger nye sårbarheder og vira på verdensplan, er der god sikkerhed for, at informationerne i StayAlert er tidligt ude, og at der ikke er noget, der bliver overset.

Forskellige systemer på markedet

Mulighederne for at håndtere sikkerhedstruslerne bliver hele tiden bedre - i takt med at antallet af sikkerhedstrusler stiger voldsomt. StayAlert er således det nyeste men ikke det eneste early warning system på markedet i dag. Udover Fort Consul har både CERT, TDC og Virus112 lanceret deres bud på en early warning service - nogle med fokus på vira og nogle med fokus på sårbarheder. Jeg skal ikke komme ind på, hvad fordelene og ulemperne er ved hvert system, men opfordre danske virksomheder med et ønske om at være på forkant med sikkerhedstruslerne til at afprøve og evt. sammenligne systemerne. Derved bliver det i hvert tilfælde nemt at se, hvor mange sikkerhedstrusler man rent faktisk modtager, hvor tidligt i deres forløb, og hvor godt filtreringen og databasesøgningen efter gamle sikkerhedstrusler virker i praksis.

Ulf Munkedal uddyber hvilke sikkerhedstrusler, som er blevet kendte i år 2002, i sit indlæg på DKUUGs seminar den 7. oktober 2002.

IT-sikkerhedslabyrinten

Af Lars Neupart,

Direktør i Neupart A/S, medlem af Dansk Industris og ITEK's it-sikkerhedspanel.

Lars.neupart@neupart.dk, www.neupart.dk

IT-sikkerhed er blevet en sand labyrint. En labyrint som alle virksomheder skal igennem for at finde frem til en passende sikkerhed. En labyrint hvor der er mange blindgyder og mange vejskilte. Nogle af skiltene peger tilmed i forskellige retninger. Skiltene er opsat af en lang række leverandører som har næsten uendelig mange bud på hvordan virksomheders IT-sikkerhed bedst muligt opnås eller bevares.

Virksomheder har brug for et navigationssystem for at finde vej i labyrinten. Med et ordenligt navigationssystem undgår man at spilde tid, penge og troværdighed i de mange blindgyder. Inden jeg beskriver den i øvrigt spændende labyrint vil jeg gå direkte til een af mine pointer: En sikkerhedspolitik er et effektivt navigationssystem, som gør det muligt at navigere hurtigt og sikkert igennem it-sikkerheds-labyrinten. Alle virksomheder – private såvel som offentlige – bør have en sikkerhedspolitik. For deres egen skyld.

Labyrinten

Lad os studere labyrinten nærmere. IT-sikkerhedslabyrinten er svær at finde rundt i fordi den er kompleks med dens blindgyder. Der står flere leverandører på hvert eneste hjørne og ved hvert eneste vejkryds i labyrinten. På nogle hjørner er de ved at falde over hinanden, så mange er der. Den ene leverandør siger at du skal til højre. Den anden siger du skal til venstre. Den første siger at virus-beskyttelse er det vigtigste for din virksomhed at få styr på. Den anden siger, at uden et ordenligt backup-system får du alvorlige problemer. Du tror, at de begge har lidt ret, men vælger at fortsætte lidt på egen hånd; du går ligeud. Så møder du en forhandler som fortæller dig, at det allervigtigste for dig er at du får hurtig og klar besked om de allerseneste sårbarheder, for at du dernæst kan installere de seneste sikkerhedsrettelser. Ved siden af forhandleren står der en konsulent. Han siger at hacker-truslen langt fra er så stor som medierne gør den til. Han anbefaler at du i stedet vurderer dine interne rutiner og arbejdsgange. "Truslen kommer indefra", siger han. Det er sikkert rigtigt, tænker du og drejer lidt til højre.

Senere i labyrinten møder du din revisor. Det var hende, der ved sidste revision fortalte din direktør, at jeres "kontroller på de interne brugerrettigheder er for svag, og at I bør få lavet en forretningsanalyse, en risikoanalyse og en sikkerhedspolitik". Det virker omfattende, synes du.

Nå, men du tror du er på rette vej igennem labyrinten, for du får jo ingen direkte dårlige råd. Du bliver påvirket af alle de forskellige råd – det hele virker jo fornuftigt nok. Du går lidt til venstre og lidt til højre. Du zig-zagger lidt, men er på vej fremad. På din videre færd i labyrinten læser du lidt i Computerworld online. Der er igen en "sikkerhedsekspert" der udtaler, at antallet af virus og sårbarheder er i kraftig stigning. Pudsigt tænker du, fordi i sidste måned kunne man læse at antallet af virus i første halvdel af 2002 har været lavere end tilsvarende periode i 2001. Den oplysning var især overraskende fordi sidste års rigtige store begivenheder, Code Red og Nimda, fandt sted i andet halvår 2001 og derfor ikke tæller med i de tal der er sammenlignet.

Du gå nu lidt til venstre, lidt vestpå. Der står en større gruppe sælgere der vil sælge dig bade automatisk og manuelt udførte sikkerhedstest . Hvis du ikke prøver din sikkerhed af, så kan du ikke vide om du er sikker, hævder de. Det lyder meget fornuftigt, men du mangler at finde ud af om du skal testes hele tiden eller bare en gang hvert halve år? Eller en kombination, måske. Det er jo ikke gratis, selvom sikkerhedstest er kommet lidt ned i pris på det sidste. Senere møder du en sælger fra Neupart A/S, han sælger ikke sikkerhedstest men siger, at sikkerhed er en kæde med to led – det produktmæssige, teknologiske led og det menneskelige, adfærdsmæssige led. De helt almindelige brugere er det svage led i kæden, fordi deres ofte utilsigtede handlinger kan medføre sikkerhedshændelser af forskellig karakterer. Selv korrekt konfigurerede firewalls kan nemt omgås - tilsigtet og utilsigtet - fordi trojanske hestes kommunikation ser ud som lovlig trafik, f.eks. http, og https. Awareness-programmer er løsningen, der hjælper det svage led i kæden siger, den energiske sælger og

fortsætter; "jeres brugere skal vide hvad de skal gøre og ikke skal gøre og de skal kende bagrunden for jeres sikkerhedsregler - og nu har vi en praktisk løsning på denne problemstilling". Endnu et godt råd der lyder meget fornuftigt, tænker du.

På din vej igennem labyrinten har du også modtaget tilbud på bedre og mere sikre internetforbindelser, en række forskellige typer store og små, hardware og software firewalls, VPN-boxe, intrusion-detection-systemer, krypteringsprodukter, sikre hjemme-pc'ere, single sign-on systemer, token-baserede engangspassword-løsninger, PKI-baserede certifikater og naturligvis også backup-tjenester, sikre mail-tjenester, overvågnings-tjenester leverandører, og konsulent-tjenester der kan hjælpe dig med at designe sikkerhedsløsningerne og installere dem for dig.

Kunsten at sige nej

Det er, som ovenstående beskrivelse illustrerer, ikke nemt at tage stilling til de mange tilbud man møder i labyrinten. Mange af dem bidrager jo godt nok til bedre sikkerhed. Det eneste problem er bare, at de alle koster både tid og penge, og at du og din virksomhed derfor er nødt til at prioritere. Ingen har uendelige ressourcer, og kunsten er at bruge de tilgængelige ressourcer rigtigt. Kunsten er at sige nej til alle de tilbud du ikke har råd til og tid til og alligevel stadig opnå en passende IT-sikkerhed. Med passende mener jeg, at i kan leve op til de krav som i selv og jeres omgivelser stiller. Hermed opnår i *den balancerede investering* i sikkerhed.

Definition på sikkerhedspolitik

Sikkerhedspolitikken er jeres navigationssystem. Politikken omfatter både nogle overordnede mål, der viser hvor vil virksomheden hen med dens sikkerhed, og en regelbaseret del, der konkretiserer jeres krav indenfor relevante områder.

Det er et overordnet mål er om vil man være i blandt de mest sikre i sin branche eller om ønsker man et mere afslappet, praktisk forhold til informations-sikkerhed. Om man vil overholde en standard – der findes både en dansk, en engelsk og en international standard (DS484, BS7799 og ISO 17799), eller måske blot blive inspireret fra en standard.

Politikken skal også indeholde en række konkrete regler, der beskriver jeres krav. Nogle krav vedrører jeres slutbrugere. Det kan være, at de ikke selv må installere software på deres computere, det kan være at de aldrig må åbne vedhæftede filer af bestemte typer. Eller at de skal bruge nogle fil-formater, som er mere sikre eller mere brugbare på tværs af platforme og produkter. F.eks er rtf-filer mere sikre end ms-word filer fordi sidstnævnte i mange eksempler er blevet brugt til at distribuere skadelige makroer. Pdf format kan også med fordel anvendes. Brugen af passwords er også en regel der er relevant for slutbrugerne.

Andre regler beskriver jeres krav til brug af anti-virus, sw-opdatering af eksternt og internt tilgængelige servere og arbejdsstationer, back-up, eller beskriver hvorvidt data skal krypteres over netværk og når det gemmes på bærbare computere.

En god sikkerhedspolitik dækker også områder som vi ikke altid tænker på i forbindelse med it-sikkerhed. F.eks fysisk sikkerhed, ansættelses-procedurer og beredskabsplaner. Det nytter ikke at have høj it-sikkerhed og sjusket fysisk sikkerhed. Det er meningsløst hvis informationerne er godt beskyttet imens de befinder sig på en server, men at i det øjeblik dokumenterne bliver printet ud må de ligge på et tilfældigt skrivebord i et kontorlandskab hvor "gæster" også har adgang.

I jeres sikkerhedspolitik vedtager i hvilke områder i vil beskytte og hvilke regler der skal gælde. Efterfølgende er meget enklere for jer at sige ja tak de sikkerhedstilbud, der er rigtige for jer og afslå dem der ikke passer til jeres behov.

Risikovurdering

Udgangspunktet for en god sikkerhedspolitik er en vurdering af hvilke hændelser i betragter som sandsynlige imod jeres systemer. Hændelser er alt fra hackerangreb og virus over utilsigtede brugerfejl til brand og oversvømmelse. Med systemer mener jeg både netværksudstyr, servere, arbejdsstationer og ikke mindst de data der ligger på dem. F.eks. CRM-systemer , økonomisystemer

eller udviklingssystemer. De systemer, der er kritiske for jer og hvor der er størst risiko for at de uønskede hændelser sker, dikterer i al væsentlighed hvilke regler der er vigtigst at inkludere i jeres sikkerhedspolitik.

Sådan får din virksomhed en sikkerhedspolitik

I har mindst tre muligheder: I kan skrive den selv, I kan bede en konsulent om at gøre det, eller I kan købe et værktøj der hjælper dig.

Hvis du vælger at skrive den selv kan du med fordel finde nogle check-lister. En god checkliste er en af de nævnte standarder – de kan købes hos Dansk Standard - , eller du kan måske få adgang til en anden virksomheds-sikkerhedspolitik til at blive inspireret. Der findes også kurser hvor du lærer at udarbejde en sikkerhedspolitik. Et godt råd: Det er særdeles vigtigt at få opbakning til sikkerhedspolitikken fra ledere og medarbejdere. Du kan derfor med fordel inddrage andre interessenter i vedtagelsen af politikken og dens regler. Der findes mange sikkerhedskonsulenter der hjælper dig med hele eller dele af processen. Husk bare, I er nødt til at deltage i et vist omfang selv, ellers kommer i til at mangle den brede nødvendige opbakning til politik og regler. Den nyeste og sikkert den enkleste måde at få en sikkerhedspolitik, er at bruge et værktøj – en "Policy Manager". Mit firma har udviklet sådan et redskab. Der findes også nogle få amerikanske virksomheder der sælger "policy management". Formålet med Neupart's værktøj er simpelt hen at gøre det nemt for den sikkerhedsansvarlige at etablere, vedligeholde og kommunikere indholdet af en sikkerhedspolitik. Det er en J2EE applikation der også indeholder konkrete forslag (templates) til sikkerhedspolitikker på dansk og engelsk.

Sådan bruger du jeres sikkerhedspolitik

Når du har fået etableret din sikkerhedspolitik er det vigtigt at kommunikere den. Lad være med at lave den klassiske fejl og læg den på jeres intranet og forvent at brugerne nu læser den og begynder at leve efter de nye regler. Det er næsten lige så ineffektivt som at sikkerhedspolitikken blot ligger i din skuffe.

I står nu overfor en kommunikationsopgave, der går ud på at få dine brugere til at kende og acceptere sikkerhedsreglerne. Denne disciplin hedder "awareness-programmer" (på godt dansk), og er et helt emne for sig selv – så det kommer til at fylde for meget i dette indlæg.

I det daglige, hjælper sikkerhedspolitikken jer der skal navigere i labyrinten med at træffe de rigtige beslutninger og få en mere effektivt it-sikkerhed.

Labyrinten udvikler sig

Er sikkerhedspolitikken nu svaret på alle sikkerhedsproblemer? Nej selvfølgelig ikke. Stol aldrig på nogen der lover dig 100% sikkerhed eller "alt bliver lettere herefter". Det er sagt før, men det er stadigt rigtigt. Sikkerhed er en proces. Det er ikke en boks eller et stykke software. Sikkerhed involverer mennesker. Processen er vedvarende; den er ikke et projekt der slutter på en planlagt dato. Man kommer derfor aldrig helt ud af labyrinten – truslerne, teknologien og kravene ændrer sig alt for hurtigt. Labyrinten udvikler sig løbende! Dermed siger jeg ikke, at det er umuligt at opnå en passende sikkerhed. Der er flere virksomheder, som er kommet godt igennem labyrinten, som har et ønsket sikkerhedsniveau. Men for at bevare et passende sikkerhedsniveau, skal i med jævne mellemrum på nye rejser i labyrinten. I skal derfor også kunne navigere i den ændrede labyrint, og der vil derfor være behov for at du med passende intervaller opdaterer dit navigationssystem.

Den evige opgradering

Af
Henrik Lund Kramshøj

Ekstra, ekstra, advarsel, bål, brand, ulven kommer!!!
Idag kom der igen en ny advarsel, advisory, exploit i produkt XXYYZZ.

Hver dag kan vi læse nye skræk-historier om sikkerhedshuller i software, sårbarheder i virksomheder og tidens seneste trend om sikkerhed.

Når vi læser disse nyheder bliver vi urolige, vores chefer bliver urolige og generelt bliver hverdagen mere stresset. Er det nødvendigt?

Vi læser ofte at vi kan installere hint software, opdatere produkt X til seneste version og så er den hellige grav velforvaret - ihvertfald indtil næste gang der er fundet
en fejl...

Status idag

Idag opdateres Common Vulnerabilities and Exposures (CVE®) med ca. 100 nye sårbarheder (kandidater til optagelse på listen) og der sendes dagligt mange e-mail om sikkerhedsemner på lister som Bugtraq, Full-Disclosure og FreeBSD-security.
Der er altså en strøm af information som det forventes at man som sikkerhedsbevidst administrator er bekendt med.

Hvem kan nå at følge med i det hele?

Ingen!
- ihvertfald ingen der holder weekend, har børn, har et arbejde eller måske har et liv udenfor skærmens elektromagnetiske stråling :)

Hvis vi nøjes med at se på software og opdateringer til disse vil jeg prøve at remse nogle problemer op med opgradering/opdatering af disse - set udfra et sikkerhedsmæssigt synspunkt. Opdatering skal forstås meget bredt idet en ændring af konfigurationsparametre kan være et eksempel på en sikkerheds-opdatering, der "lukker af" for en sårbarhed.

Det kan godt være at opdatering af et enkelt produkt/operativsystem/program/server kun tager et øjeblik, men det er vigtigt at tage hensyn til at dette ofte forventes gjort NU og HER! Uanset om klokken så er 18:00 fredag aften og man havde planlagt besøg hos svigerfamilien for første gang.

Ulemperne ved opgradering

Lad os lige rekapitulere hvad der sker når man opdaterer et IT-system?
En opdatering betyder at man ændrer på systemer, der udfører en funktion - et eller flere programmer ofte i et mere komplekst samspil.

Løser en opdatering problemet?
Der er en del eksempler på at visse opdateringer ikke har haft den ønskede virkning eller ikke tog højde for varianter af sårbarheden - og derfor var virkningsløse overfor afledte problemer. Et eksempel på dette er den nylige Apache sårbarhed, hvor ISS producere en patch uden at konsultere med Apache programmørerne. Det betød at rettelsen ikke tog højde for alle problemer(CAN-2002-0392, se ISS og Apache patch)

Ustabile systemer er ligeledes et problem som bør tages alvorligt. Indenfor sikkerhed taler man jo ofte om CIA, Confidentiality Integrity and Availability, og hvis et system som følge af opdatering bliver ustabilt er dette måske også et sikkerhedsproblem.
Eksempelvis var der for nyligt en sårbarhed i OpenSSH, hvor brugen af UsePrivilegeSeperation kunne gøre en usårlig overfor problemet - hvis den altså var tilgængelig på den platform man benyttede! OpenSSH benyttes på mere end 80 platforme og ikke alle understøttede UsePrivilegeSeperation - altså en relativt uafprøvet funktion på mange platforme.

Fejlbehæftede programmer.
Den nye eller opdaterede version af programmet kan have fejl, måske endda mere graverende end den eksisterende version - i det specifikke miljø.

En opdatering er derfor ikke altid løsningen på det specifikke problem, men mere en

løsning på symptomet - at nogen blev urolig(e) og beordrede opdatering for at "gøre noget".

Hvis man ukritisk opdaterer sine systemer risikerer man derfor at skabe problemer i IT-miljøet.

Alternativet til opgradering

Findes der et alternativ til den evige opgradering?

Når nu vi læser at der jævnligt efter offentligørelse af en sårbarhed kommer orme og andre automatiserede værktøjer til masse-ødelæggelse må man forvente at en sårbar server der efterlades uden opsyn i en periode VIL være inficeret.

Hvis man en dag falder over en forladt server på nettet - der ikke er blevet opdateret siden installationen - bør man se med kritiske øjne på denne. Især hvis der er adgang til serveren fra Internet er sandsynligheden for at en sårbarhed har været udnyttet bestemt til stede.

Der er altså en periode hvor systemerne er i risikogruppen. Populært kaldes dette for "window of exposure", og er beskrevet godt af eksempelvis Bruce schneier.
Alt dette taler jo for at haste alle opdateringer igennem, men jeg mener at det er et alternativ, at udsætte opdatering - i kortere eller længere tid.

Ja, man kan samle disse opdate-ringer og foretage planlagte opdateringer! uha planlagt er det ikke et fyord?

Hvorfor kan de planlagte være bedre end 100m spurt til nærmeste terminal og feberredninger og brandslukning på de systemer der idag er de vigtigste?

Fordi:
Alle systemer gennemgås
Ansvaret for udførelse placeres - og logning af det udførte arbejde dokumenteres.

Alt taget i betragtning mener jeg det har større værdi for miljøet, at der arbejdes struktureret på at sikre netværket gennem seriøs drift - end brandslukning med små vandballoner kan gøre.

Eskaleringsprocedurer

Når jeg nu har sagt at man skal udskyde sine opdateringer er der selvfølgelig situationer, hvor opdatering ikke kan udsættes! Det kan dog være en god ide at sætte sig ned en stille dag, den ene gang om året det sker, og så prøve at tænke på hvad der kendetegner en "katastrofe/ nødsituation", hvem skal informeres, hvad er kriterierne for at smide alt og råbe panik?

Hvis man samtidig har overblik over hvilke systemer der findes, hvilke opdateringer der allerede er foretaget/udført kan man mere målrettet sætte ind overfor en trussel der kræver hurtig reaktion.

Analyser jeres IT-miljø

Det kan være en stor hjælp til minimering af arbejdsbyrden med opgradering at se med kritiske øjne på hele IT-miljøet.
Se kritisk på infrastrukturen og vurder om det er nødvendigt med 20 forskellige typer af udstyr, eller om man ved at vælge de 10 kunne dække virksomhedens behov.

Crunchy outside, soft on the inside

Mange virksomheder har fokus på skalsikring og virksomhedens eksterne forbindelser, men glemmer at tage hensyn til flere aspekter af sikkerheden. Hvis man aldrig kommer rundt i hjørnerne med en hovedrengøring vil der være en masse systemer, der er godbidder for enhver der forstår at udnytte kendte sårbarheder.

Det er efter min mening også omsonst at have en dyr firewall og så aldrig rydde op i de brugerprofiler og adgange der engang er givet - og aldrig fjernet fra systemer på indersiden.

Vær realist

Når man taler seriøst om sikkerhed findes 100% ikke - der findes ingen 100% sikre firewalls, antivirus systemer, operativsystemer. Det bedste bud på en 100% sikker firewall findes i en artikel af Marcus J. Ranum på adressen der er vist nedenfor.

Når man bruger IT-systemer, indtaster data og forbinder systemet til andre - via Internet eller lignende udsætter man det for en risiko - uanset om man bevidst har taget stilling til denne.

Det er derfor vigtigt at indse, at uanset hvad man gør for at sikre sine systemer kan der ske uheld. Der kan være en opdatering der fejler, en procedure der kikser - eller udefra kommende påvirkninger.

Det er derfor yderst vigtigt ikke blot at tage forholdsregler, men tage stilling til hvorledes brud på sikkerheden håndteres.

Hvor ofte checker man ved en opdatering om systemet rent faktisk allerede **er** ramt af den sårbarhed man forsøger at beskytte imod?

Planlægning og backup!

Jeg vil nu slutte af med en opfordring til at I planlægger jeres katastrofer, træner i brandslukning og sørger for at tage backup af de data der er vigtige for jer.

Hvis det brænder idag, så brænder det sikkert også imorgen - planlæg hellere at fastmontere en brandhane i serverrummet mandag. Så kan du hurtigere slukke de ildebrande der vil opstå i fremtiden ;-)

PS
Jeg har selv under skrivningen af denne artikel sat en backup af e-mail igang, da også jeg må regne med at der kunne ske noget med mine data ... og det er vist "noget tid siden" :-)

Links:
CVE listen
http://cve.mitre.org

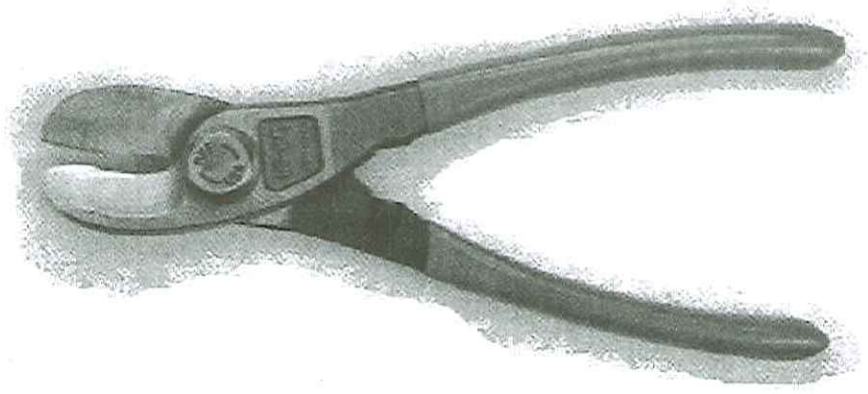
Full-Disclosure listen
http://lists.netsys.com/full-disclosure-charter.html

FreeBSD Security
http://www.freebsd.org/security/

OpenSSH PrivilegeSeperation http://www.openssh.com/txt/preauth.adv

Bruce Schneier Window of exposure http://www.counterpane.com/crypto-gram-0009.html#1

The ULTIMATELY Secure Firewall http://www.ranum.com/pubs/a1fwall/



The ULTIMATELY Secure Firewall
Ifølge Macus Ranum

Web-servere er populære hos hackerne

Af Torben B. Sørensen, journalist, UNI•C/DK•CERT

torben.b.sorensen@uni-c.dk
Læs mere på www.cert.dk

Web- og FTP-servere tegner sig for næsten halvdelen af de systemer, hackerne angriber. Men SSH er også et populært mål.

En web-server gør det nemt at finde oplysninger om en virksomhed eller organisation. Web-siderne fungerer som et virtuelt salgsvindue. Men nogle brugere er ligeglade med varerne i vinduesudstillingen: De vil hellere benytte vinduet som en bagdør til systemerne.
Ifølge bogen "Web Hacking: Attacks and Defense" er 65 procent af alle angreb rettet mod web-servere. Det er mere, end DK•CERT typisk registrerer, men web-tjenester er gerne blandt de mest populære.
Når web-serveren ofte er et yndlingsoffer for hackerne, har firewalls en del af skylden. Før firewalls blev udbredte, kunne en hacker finde mange spændende porte at skyde på, når han scannede systemer på internettet. Men firmaer med en firewall lukker af for trafik til alle andre porte end dem, som det er nødvendigt at holde åbne. Derfor indskrænkes hackerens råderum til tjenester som web, e-post, FTP (File Transfer Protocol) og måske Telnet.

Web-servere er fyldt med huller

En anden årsag er, at web-serverprogrammer har været fyldt med sårbarheder. Især Microsofts Internet Information Server (IIS) har adskillige kendte huller. Microsoft har således udsendt ikke færre end 39 advarsler om sikkerhedsproblemer i version 4 af programmet. Det har fortalere for open source brugt som argument for at skifte over til Apache. Men det sidste halve års tid har afsløret et par alvorlige sårbarheder også på denne platform. For eksempel blev der i juni offentliggjort en sårbarhed i måden, serveren håndterer "chunked encoding" på. Samme emne er i øvrigt også årsag til en af IIS-sårbarhederne.
Selve web-serverapplikationen er imidlertid ikke den eneste vej ind i en web-server. Næsten alle web-servere afvikler programmer til at generere web-sider dynamisk. I Microsoft-verdenen hedder det ASP-sider, hvor man på Apache ofte anvender PHP. Også her er der gode muligheder for at udnytte sårbarheder. For eksempel kan man indtaste kommandoer direkte i URL-strenge og se, hvilken effekt de har.

Orme udnytter sårbarheder

En del af de angreb, DK•CERT registrerer, skyldes udbredte orme som Code Red, Klez og Nimda. De udnytter de kendte sårbarheder i web-servere. Hvis ens IIS-server er blevet udsat for angreb fra Code Red, kan det ses i logfilen, hvor der vil være en linie af typen
/default.ida?NNNNNNNNNNNNNNNNN -
efterfulgt af en masse N'er og andre tegn.
De mange tegn afslører, at der her er tale om en såkaldt bufferoverløbssårbarhed. Ormen fylder en buffer i serverens arbejdslager, så data flyder over. Nogle af dataene placeres et sted, hvorfra de kan udføres som kommandoer.
Når hackerne først har fået adgang til en web-server, griber nogle af dem lejligheden til at prale. Det gør det ved at overplastre indgangssiden med graffiti i en såkaldt "defacement". I den senere tid har især brasilianske hackere været meget aktive med at placere deres eget indhold på servere, de har hacket. Det er blandt andet gået ud over Økonomi- og Erhvervsministeriet.

FTP distribuerer piratkopier

Den anden af de mest populære tjenester blandt hackere er FTP. Her udnytter de det faktum, at der stadig findes servere, som tillader anonym login. Desuden er der også kendte sårbarheder i flere FTP-servere.
Har en hacker fået kontrol over en FTP-server, omdanner han den ofte til digital hælercentral: Her kan hackeren og hans venner placere piratkopier af programmer, musik og film, som andre kan hente.
Dermed får virksomheden, som det går ud over, pludselig to problemer: Ikke nok med, at deres server er blevet hacket - de risikerer også sagsanlæg for medvirken til distribution af piratkopier.

SSH giver kontrol over maskinen

Ofte dukker port 22 op på hitlisterne over de mest angrebne porte. Her går hackerne efter en teknologi, der faktisk er lavet for at forbedre sikkerheden: Secure Shell. Med en SSH-

forbindelse krypteres kommunikationen mellem to computere, så uvedkommende ikke får glæde af at aflytte den.
Men de udbredte SSH-serverprogrammer har en række sårbarheder. Der er således et par bufferoverløb i OpenSSH, som angribere kan bruge til at få afviklet kommandoer på computeren.
Hvor angreb mod FTP ofte er et forsøg på at finde lagerplads til piratkopier, er SSH-angreb oftere udtryk for, at hackeren vil have kontrol over en maskine. Det ultimative mål er at få administratorrettigheder, det vil sige på root-niveau.
I sommer oplevede brugerne af SSH-programmet OpenSSH en usædvanlig form for sårbarhed: Da en bruger hentede seneste version, opdagede han, at checksummen ikke stemte. En nærmere undersøgelse viste, at programmet havde fået indføjet en trojansk hest. Der var lagt en IP-adresse ind i programmet. Hvis en angriber forbandt sig fra den pågældende adresse til en server med den sårbare version, ville han have direkte adgang ind bag ved SSH-krypteringen. Den sårbare version var dog kun tilgængelig et par dage, før det blev opdaget.

Pakkeløsninger letter hackerens arbejde

Umiddelbart kan det lyde som hårdt arbejde at skulle finde frem til lige præcis den rigtige kombination af tegn, der udnytter et bufferoverløb. Men her kommer teknologien hackerne til hjælp: De udvikler løbende programmer, som kan hjælpe andre hackere med at udnytte kendte sårbarheder. Derfor behøver man ikke have det store systemkendskab for at hacke et system.
Når hackeren først er kommet indenfor og har fået administratorrettigheder, starter han gerne med at gøre systemadministratoren en tjeneste: Han installerer de seneste opdateringer og patches til systemet. Årsagen er enkel: Når det er lykkedes ham at komme indenfor, kan andre gøre ham kunsten efter. Derfor lukker han sikkerhedshullet efter sig.
Dernæst installerer hackeren gerne et såkaldt rootkit. Det gør det nemt for ham at vende tilbage til maskinen, idet det indeholder en bagdør. Det kan for eksempel være i form af en modificeret udgave af login-programmet. Et rootkit, der blev fundet på en Solaris-maskine, indeholdt også en fuldskærmseditor - måske et tegn på, at hackerne ikke følte sig fortrolige med vi?

Brevsprækken står åben

Ingen oversigt over udbredte angrebstyper er komplet uden e-post. Dog kan man diskutere, om der er tale om hacker-angreb, når det handler om udsendelse af spam (uønskede reklamer). Afsenderne af spam vil som regel ikke sende det fra deres egen server, da deres internet-udbyder så hurtigt vil smide dem ud. I stedet søger de efter åbne mail-relæer, der videresender e-post, uanset hvem det kommer fra. Et åbent mail-relæ skyldes som regel en forkert konfigureret server. Derudover findes der en række sårbarheder i postprogrammer, der kan udnyttes til andre former for ulykker. Især Sendmail har haft en tradition for mange sårbarheder, men andre postservere kan også være med.

SQL begynder at melde sig

DK•CERT har registreret en interessant udvikling fra første til andet kvartal i år: Nu er port 1433 med på topti-listen. Den anvendes af Microsoft SQL Server, og når den overhovedet dukker op, skyldes det sandsynligvis en orm, der blandt andet går under navnet Spida. Denne orm udnytter en udbredt konfigurationsfejl, hvor databaseprogrammet er installeret med en brugerkonto ved navn "sa" uden noget password.
Microsoft tegner sig også for en anden populær port, 139. Den anvendes, når fildeling i Windows-netværk kører SMB (Server Message Block) over NetBIOS. Men på det seneste er også port 445 begyndt at vise sig. Den findes i de nyere Windows-systemer, hvor SMB kører direkte på TCP uden NetBIOS imellem. Begge porte vil det som regel være en god ide at lukke af for i firewallen. Ellers udsætter man sig blandt andet for risikoen for Denial of Service-angreb: En enkelt datapakke sendt til en af disse porte kan lægge en Windows-pc ned, så den skal genstartes.

Ingen platform er sikker

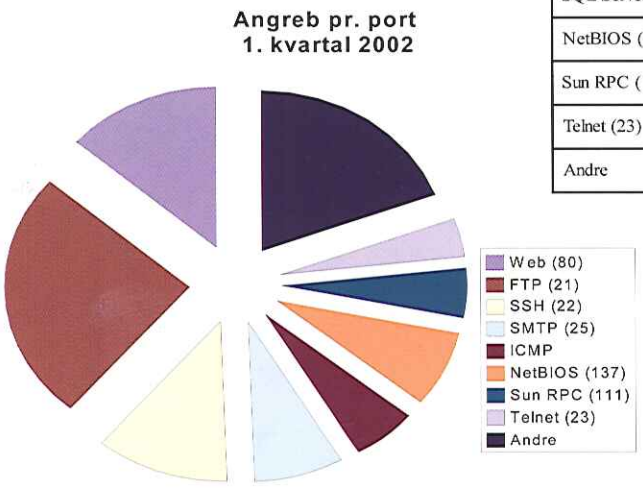
Skønt navnet Microsoft optræder mange gange i ovenstående, betyder det ikke, at man er på den sikre side, hvis man kører Linux. Computere med Linux og Unix kan også være sårbare, og de kan køre sårbare applikationer. Hvis man vil sikre sig, skal man sørge for at installere nye patches, så

snart de udkommer. Derudover skal man ikke bare installere en firewall, man skal også kontrollere, at den er konfigureret rigtigt. Og så kan antivirusprogrammer spare virksomheden for mange timers arbejde, hvis blot de er opdateret med de seneste virusdefinitioner.

Angrebsstatistik 1. og 2. kvartal 2002

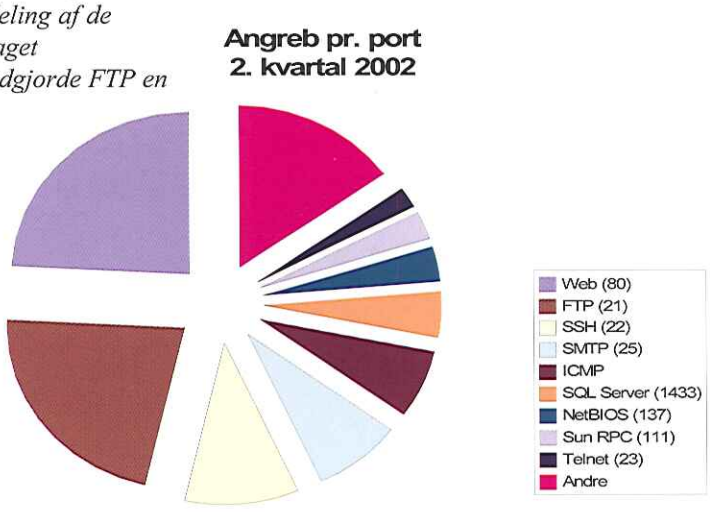
Tallene viser den procentvise fordeling af angreb og scanninger rettet mod bestemte netværksporte.

Port	2. kvartal	1. kvartal
Web (80)	24%	14%
FTP (21)	22%	26%
SSH (22)	10%	12%
SMTP (25)	8%	8%
ICMP	7%	6%
SQL Server (1433)	4%	0%
NetBIOS (137)	3%	8%
Sun RPC (111)	3%	5%
Telnet (23)	2%	4%
Andre	15%	20%



Første kvartal:

Grafen viser den procentvise fordeling af de angreb, som DK•CERT har modtaget anmeldelser om. I første kvartal udgjorde FTP en fjerdedel af alle angreb.



Andet kvartal:

Angrebsstatistikken fra andet kvartal 2002 viser, at scanninger efter SQL Server-porten nu er med på topti-listen.