DKUUG

Vejen til viden om Åbne Systemer og Internet

nyt

117/oktober1999

Echelon

Tema om aflytnings-systemet

Stor fremtid for danske satelitter

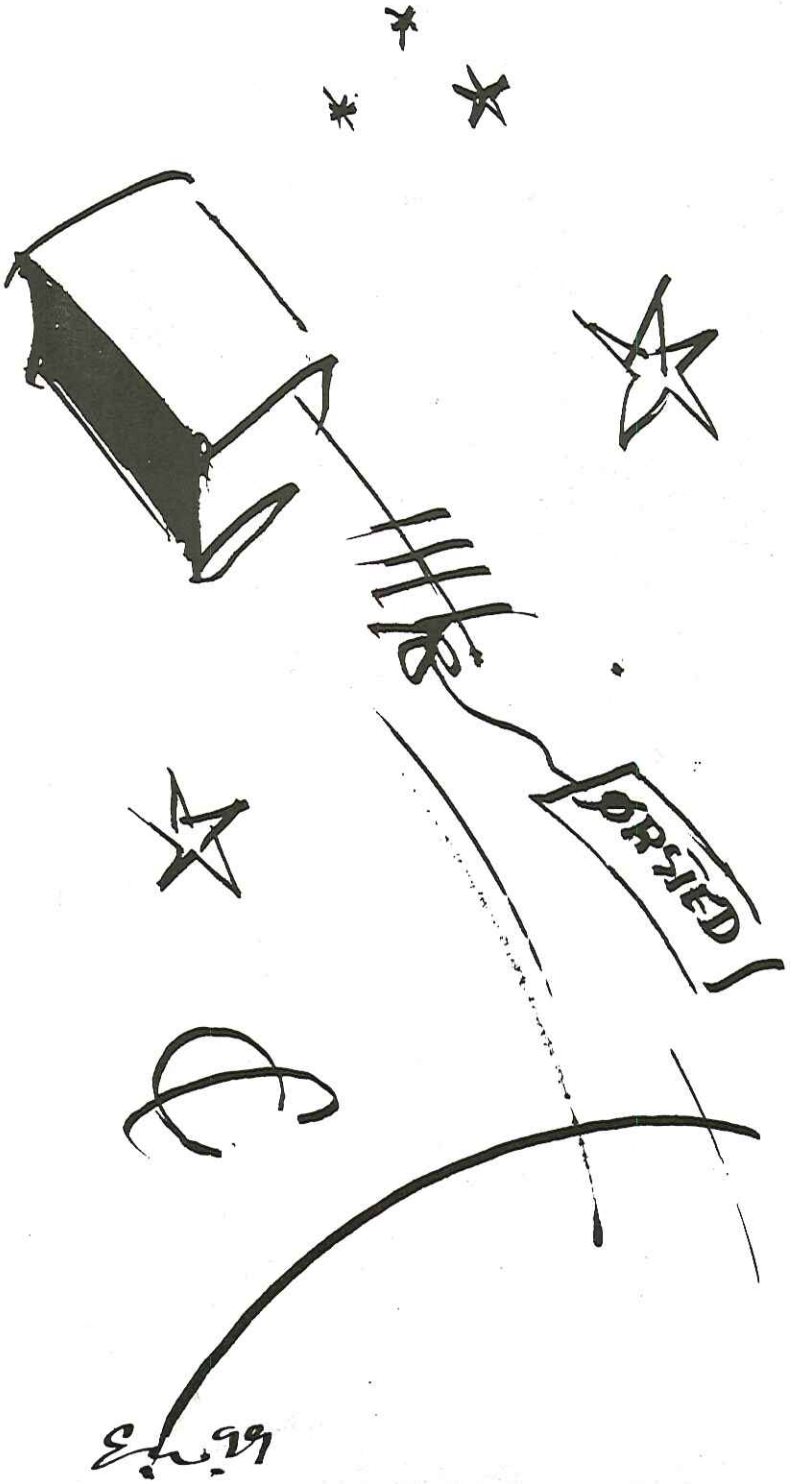
Vi har besøgt firmaet bag Ørsted-satelitten

PGP

Sådan krypterer du dine mails

Storpolitik i DKUUG

Foreningen har været vært for international standardiserings-konference



Indhold

Leder

Vi skal ikke finde os i Echelon

Ligesom de fleste andre havde jeg ikke hørt om Echelon før for en lille måneds tid siden. Da jeg endelig hørte om det, var reaktionen: Åhr, er det ikke lidt paranoidt ? Men et møde med Duncan Campbell overbeviste mig og mange andre om, at Echelon eksisterer og helt rutinemæssigt og automatisk overvåger alt hvad vi siger og mailer.

Og hvad er der så galt med det, vil nogle spørge? Skal efterretningstjenesterne ikke have lov til at bruge aflytning til at afværge terrorist-aktioner (Echelon har sandsynligvis hjulpet til at afværge flere sådanne), fange forbrydere (Echelon hjalp sandsynligvis med at fange terroristen Carlos Sjakalen) og spare menneske-liv i krige (Echelon spillede sandsynligvis en rolle i Golfkrigen og krigen i Kosovo)? Mit svar er nej, det skal de ikke have lov til. Og det er der to grunde til:

1) Det er et utåleligt overgreb mod mine og alle andre´s borgerrettigheder, at vi helt automatisk bliver overvåget og registreret uden den mindste mistanke eller bevis for, at vi begår eller kunne finde på at begå noget kriminelt.
2) Der er tydelige indicier for, at Echelon ikke kun bruges til at registrere kriminelle eller terroristiske aktioner, men også misbruges til industrispionage.

Der må et folkekrav til for at få politikerne til at holde nærmere øje med efterretningstjenesterne og DKUUG, SSLUG og PROSA er sammen om at organisere modstanden mod Echelon. Vi vil ikke finde os i det.

Jeg er overbevist om, at når jeg om lidt sender denne leder pr. e-mail til lay-out, vil en computer et eller andet sted komme på arbejde. Se lige teksten: Echelon, Duncan Campbell, terrorist-aktioner, Carlos Sjakalen, Golfkrigen, Kosovo, industrispionage o.s.v. Måske skulle vi alle fylde vore e-mails med „mistænkelige" ord og håbe på, at Echelon bryder sammen.

Med venlig hilsen
Hans Arne Niclassen

Linux Demo Day på Carlsberg

Endnu et bevis på Linux´ og Unix´ fredelige sameksistens: Niels Svennekjærs Peugeot ved siden af Brian Eberhardts Porsche.

På en solbeskinnet søndag 12. september var det Linux Demo Day i hele verden. I Danmark foregik dagen på Carlsberg i Valby. Mange mennesker havde bestemt sig for at tilbringe en eftermiddag i selskab med pingvinen, lokket af bl.a.. Mads Bondo Dydensborgs demonstration af Linux-spil, Brian Eberhardts introduktion til Linux, Installfest og masser af Linuxpræmier - og så skulle vi hilse og sige pænt tak til Carlsberg for husly, øl og sodavand.

HAN

Stor interesse for spil til Linux

Første danske satellit i rummet

DKUUG-Nyt har besøgt TERMA, firmaet bag Ørsted-satelitten.

23. februar '99 lykkedes det endelig: I 11. forsøg kom den første danske satellit i omløb. Mikrosatellitten Ørsted fylder med sine 60 kilo meget lidt i forhold til „traditionelle" satelitter, der kan veje op til til flere tons, men faktisk er opsendelsen af den første danske satellit en bedrift, der giver dansk forskning og industri store muligheder i fremtiden.

Den første danske satellit i rummet

Hele Danmark fulgte med spænding opsendelses-forsøget af Ørsted-satellitten den 15. januar 1999. Desværre blev opsendelsen aflyst - og de gjorde de ni næste forsøg også.

Peter Hoffmeyer, projektleder på Ørsted-projektet, forklarer: „En Delta-raket skulle bringe Ørsted i kredsløb. Opsendelsen skulle ske fra Vandenberg-basen i Californien, og jeg var tilstede. Derfor oplevede jeg også på første hånd, at der ikke blev taget nogen chancer. Vejret er meget afgørende, især fordi raketten smider ni større fast-stof raketter i de første minutter efter opsendelsen, og de skal jo nødig falde ned i beboede områder. Èt af forsøgene blev afbrudt, da nedtællingen nåede 0 p.g.a. af én måling på en powerkontrol enhed - og det på et instrument, der måles på hvert 15. sekund. En anden gang svigtede kommunikationen med den vejrballon, der var sendt op for at måle vejret i de øvre luftlag. Da forbindelsen var genoprettet, meldte ballonen, at vejret var fint, og raketten kunne sagtens have været sendt op - men da var det for sent. Den endelige opsendelse var derfor en kæmpe lettelse."

Nu har Ørsted altså fløjet rundt i rummet i over et halvt år - og den klarer sig over al forventning. Ørsted leverede de første måleresultater efter en måneds tid, hvor MAGSAT - den sidste satellit, der foretog målinger af Jordens magnetfelt - først leverede data efter ca. seks måneder. MAGSAT havde en levetid på 8 måneder, medens Ørsted forventes at „leve" i 14 måneder. Men hvis det fortsat går, som det gør i øjeblikket, kan Ørsted fortsætte med at arbejde i flere år. „Vi er faktisk overraskede over, at der ikke har været flere problemer", siger Peter Hoffmeyer.

Hvad laver den derude?

Ørsted-satelliten vejer altså 60 kg. og er på størrelse med et gennemsnits-køleskab - hvis man fraregner den 8 m. lange „bom", der først folder sig ud, når satellitten er på plads. Men Ørsted koster unægtelig noget mere end et køleskab: 130 millioner kroner. Ideen om en dansk satellit opstod omkring 1990 i en gruppe, der bl.a. talte TERMA Space Divisions´s direktør Jens Langeland-Knudsen og forskere fra diverse universiteter. Det lykkedes for gruppen at sælge ideen til bl.a. Erhvervsministeriet, Forskningsministeriet og Dansk Industri, der ydede betydelig støtte. Så var det bare at gå igang med at finde ud af, hvad den danske satellit skulle foretage sig i rummet.

Føromtalte MAGSAT er den hidtil eneste satellit, der med succes har foretaget målinger af Jordens magnetfelt, men det ligger helt tilbage i 1979-80, og ideen opstod at lade Ørsted (som den blev døbt) foretage langt mere nøjagtige målinger af Jordens magnetfelt. Nøjagtige

opmålinger af magnetfeltet kan bidrage væsentligt til vores forståelse af, hvad der foregår i Jordens indre, hvilket vi stadig ikke er helt klare over.

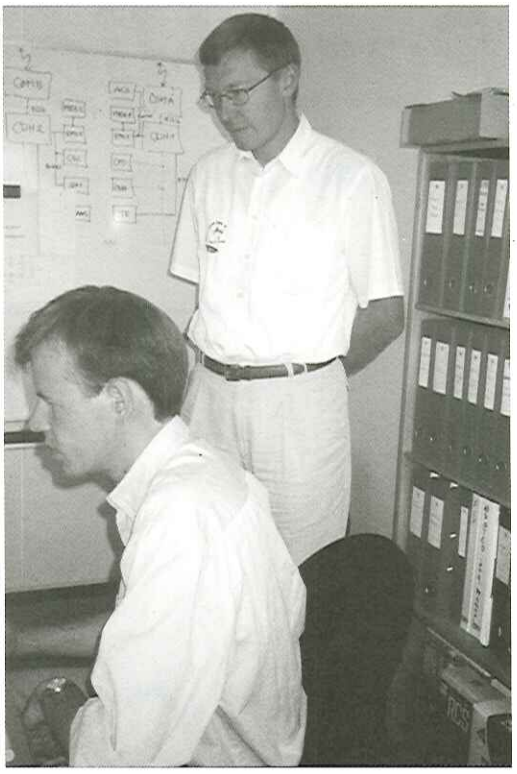
Danske firmaer har faktisk længe beskæftiget sig med rum-projekter. Christian Rovsing er en af pionerne og efter hans konkurs i 1984 blev rum-afdelingen opkøbt og fortsatte som CRI Space Division. CRI konstruerede sammen med firmaerne Per Udsen og TERMA Ørsted-satelitten, indtil de to andre firmaer blev købt af TERMA og alle tre blev samlet i TERMA Group. TERMA beskæftiger ca. 1000 medarbejdere i hele verden indenfor forskellige forretningsområder, med hovedvægten lagt på systemer til militære formål. Og så er der Space Division med ca. 80 medarbejdere i udlandet og 70 i hovedkvarteret i Birkerød. Det er her, Ørsted blev fremstillet og her, Ørsteds informationer bliver modtaget og formidlet videre.

Antikveret EDB i Ørsted-satelitten

Det vil sikkert komme bag på den IT-interesserede, hvad der ligger inden i Ørsted. Afdelingsleder Carsten Jørgensen forklarer:

- „Hjertet i Ørsted er to 16 MHz 80186-computere forbundet med en 485-bus. Hver computer har en harddisk på 8 Mb. De to maskiner deles om opgaverne, men skulle én af dem falde ud, kan den anden automatisk konfigures til at klare arbejdet. Maskinerne samler informationer fra de tilsluttede måleinstrumenter og sender dem 6 - 8 gange i døgnet til Jorden, hvor de i første omgang modtages af DMIs antenne på Østerbro i København. DMI sender måleresultaterne ud til os i Birkerød, og over ISDN-linjer sender vi de bearbejdede data til forskere på forskellige institutioner og tilbage til DMI. Samtidig holder computerne øje med instrumenternes sundhedstilstand og fra Jorden kan vi sende kommandoer til de forskellige instrumenter. Softwaren har vi selv lavet, først og fremmest i ADA (en overbygning på Pascal), men også i C og Assembler. Computerne har 512 kb RAM, hvor 256 kb. bruges til kode. Vi kan fra Jorden uploade nyt software, når det er nødvendigt. Vores „mission control" er kvantitetsmæssigt ikke så imponerende som NASA's, men betydeligt mere effektiv - faktisk består den af tre PC'ere i et kontorlokale.

- Der er flere grunde til, at vi bruger „antikveret" teknologi i Ørsted. For det første begyndte vi at konstruere satelitten i '92-93, og dengang skulle vi have processorer, der kan klare de ekstreme forhold i rummet. Satelitten bliver udsat for kosmisk stråling, og det er der ingen almindelige processorer, der kan holde til. Derfor skal processorerne være af militær standard, og det marked er meget lille. Der bliver ganske vist produceret hurtigere processorer, der er space-qualified, men de er rasende dyre, så der kommer nok heller ikke Pentium-processorer i vores fremtidige satelitter. „Antikviteterne" fungerer også ganske udmærket, men de bliver langsomt ædt op af kosmisk stråling og vil på et tidspunkt holde op med at fungere. Det tidspunkt kan man desværre ikke selv vælge, men sådan er betingelserne."



Peter Hoffmeyer - projektleder på Ørsted-satelliten i „Mission Control".

Fremtid for danske satellitter

De gode erfaringer med Ørsted har givet TERMA lyst til at fortsætte med at konstruere mikro-satellitter.

Afdelingsleder Steen Jappe: „Erfaringerne fra arbejdet med Ørsted har betydet, at der nu er dansk deltagelse i et argentinsk satellitprogram, hvor vi skal levere og integrere en magnetometer nyttelast. Den omfatter en 8-meter bom (lig den på Ørsted), to magnetometre, samt et stjernekamera til bestemmelse af satellittens retning i rummet. Vi har store forventninger til TERMA's stjernekamera produktserie, som omfatter udvikling af komplicerede instrumenter til brug på satellitter i rummet. Disse kan, ud fra genkendelse af stjernemønstre samt beregninger på deriverede data, give meget nøjagtige retningsbestemmelser.

Vi arbejder også med flere studier og projekter inden for området 'atmospheric occultation', hvor man eksempelvis kan beregne sig frem til vigtige meteorologiske data. Her måler man signal forsinkelser (bøjning af signal) grundet atmosfæren mellem to satellitter, hvor den ene er tæt ved jordens horisont set fra den anden."

HAN

Du kan læse mere om Ørsted og TERMA på www.terma.com.

Pers Hjørne

IT efter år 2000 – En personlig synsvinkel

Hvordan vil anvendelsen af informationsteknologi udvikle sig på den anden side af millennium skiftet? Hvis der i det hele taget er noget IT efter den 1. januar. De mest dystre forudsigelser – måske mest fra USA – er, at katastrofe-lignende tilstande vil opstå, når alverdens edb-systemer bryder ned nytårsaften. Pudsigt nok advarer amerikanske "eksperter" mest imod edb-nedbrud fra verdenen uden for USA, som man mener er mindst forberedte. Og på amerikansk tv kan man samtidig se reklamer, der opfordrer folk til at investere i guld, for det vil beholde sin værdi når verdenen kommer til et stop (det var *inden* faldet i guldpriserne!).

Jeg er nu ikke i tvivl om, at vi vil have edb-systemer efter den opreklamerede nytårsaften. Javel, der vil være en del gener fra systemer, der ikke helt klarer overgangen, men generne vil være mindre og kortvarrige. Nogen katastrofe er der ikke i vente.

Men teknologi er noget mærkeligt noget. Udviklingen går så hurtigt, at man nogle gange helt mister pusten. Udviklingen kan være svær at overskue, og det er måske den virkelige baggrund bag år 2000 hysteriet. Nye teknologier dukker hele tiden op, som for eksempel teknologiske landvindinger som briller med indbyggede skærme og mobiltelefoner, med adgang til Webbet. Samtidig kan Girobank ikke finde ud af at indstille deres systemer, således de huller kontoudskrifter med 4 huller i den korrekte afstand. Jamen, hvor svært kan *det* være?

Dette viser blot, at der stadig er noget, der hedder den menneskelige faktor. Og den er mindst lige så vigtigt som den teknologiske udvikling. Mange er enige om, at Internettet efter år 2000 kommer til at stå for den mest betydende IT udvikling. Vi snakker om 2-3 millioner brugere af Internettet i Danmark blot om få år. Vi snakker om markant voksende handel på Internettet. Om blot få år, vil den såkaldte Internet-økonomi udgøre 10% af hele verdens økonomi!

Samtidig repræsenterer Internettet nogle af de mest grundlæggende ændringer i vores kultur – den menneskelige faktor. På grund af Internettet ændrer vores opfattelse af "tid" sig markant i disse år. Information er til stede alle vegne og lige når vi har behov for det. Begrebet "værdi af information" ændrer sig også voldsomt – det har de mange informationsudbydere på Webbet erfaret på en særdeles negativ måde. Også vurderingen af "informations-kvalitet" er på vej til at ændre sig. De gammeldags kriterier for kvalitet, såsom "gendigen udførelse", holder ikke længere. En hjemmeside kan være fantastisk flot,

gennemført og professionel – og alligevel være fyldt med løgn !

Vore børn skal derfor lære nogle helt andre redskaber i den nye Internet-verden. Det er bare ikke helt gået op for skolesystemet endnu. Elektronisk informationssøgning og ikke mindst vurdering af kvaliteten af elektronisk information skal have en meget mere fremtrædende plads og være tilpasset de ændrede behov.

Og så er Internettet blot begyndelsen på den generelle udvikling, som vi vil opleve med IT i det nye årtusinde. Efterhånden vil IT ophøre med at eksistere om et nærmest selvstændigt område og blive integreret i stort set alt, hvad vi foretager os. Vi kender selvfølgelig allerede brugen af chips i fjernsyn, biler, mobiltelefoner og meget andet. Men for de fleste er "edb" stadig noget med en bestemt enhed – en PC eller en terminal. Resten er "elektronik". Dette ændrer sig, og IT bliver som elektricitet: noget der er generelt tilgængeligt og som man forventer altid er til stede alle vegne.

I fremtiden vil vores mail (fx) ikke være bundet til PC-adgang. Vi vil kunne læse og sende mail allevegne via mobiltelefon, små håndholdte enheder, fjernsynet, bibliotekets søgemaskine, stationære skærmtelefoner, konsollen i bilen osv. Tilsvarende vil vi have adgang til vores databaser allevegne med oplysninger om vores kalendere (og andres i et vist omfang), vores dokumenter, vores økonomi mv.

På forskellige områder vil specifikke IT-systemer dukke op. Et af de første eksempler er GPS systemerne til biler. Andre eksempler er telemedicin og overvågning.

Den mest grundlæggende forudsætning for disse udviklinger er den globale kommunikationsstruktur, der i dag blandt andet repræsenteres ved Internettet og mobiltelefonnettet. Denne struktur udvikler sig naturligvis også, og det vi i dag kender som Internettet er om 10 år sikkert afløst af et andet og mere avanceret, hurtigere, mere pålideligt og intelligent netværk.

Som virksomhed behøver man imidlertid ikke sidde med hænderne i skødet indtil disse visioner går i opfyldelse. Længe inden da vil der være luget ud i erhvervslivet, således at det er de innovative og fremsynede virksomheder, der overlever. Og det vil være de virksomheder, forstår at forene de nye teknologiske muligheder med menneskelig kreativitet. Og så er vi tilbage ved min oprindelige bemærkning om den menneskelige faktor! Teknologien kan ikke stå alene, og kun gennem vores kreativitet og opfindsomhed kan vi blive konkurrencedygtige via teknologien.

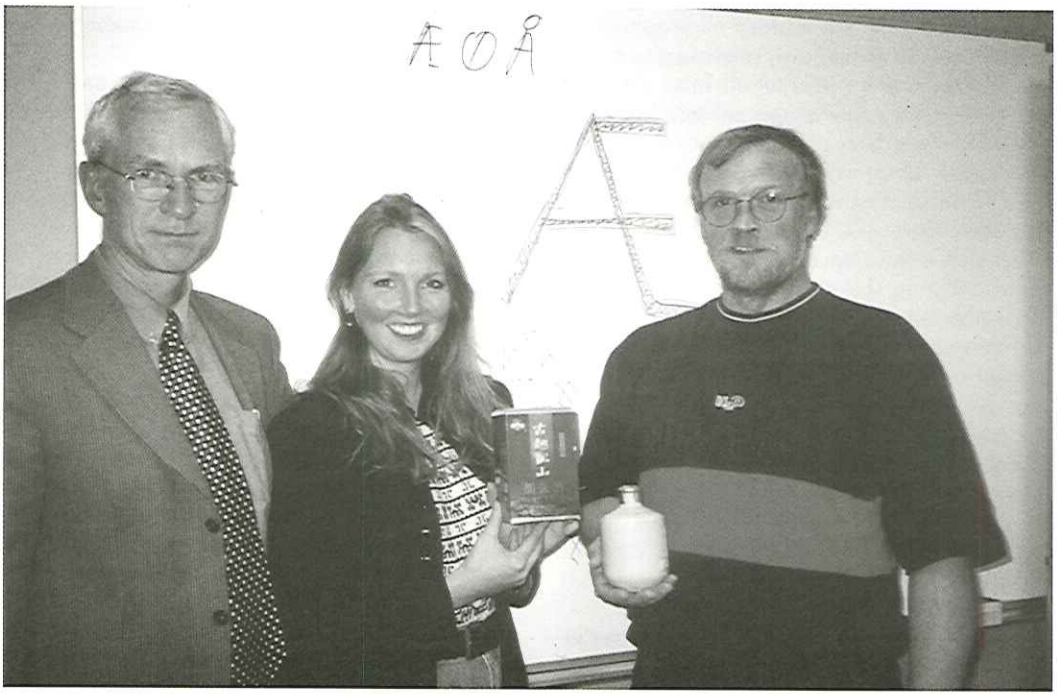
Vi har i Danmark og inden for erhvervslivet længe postuleret, at vores menneskelige resourcer var blandt de førende i verden. Med overgangen til det nye årtusinde er det på høje tid at vise, at vi kan udnytte disse resourcer sammen med de teknologiske muligheder til at bringe os i front i den nye Internet-økonomi.

Generalforsamling

DKUUG afholder ordinær generalforsamling den 25. november 1999.

Skriftlige forslag til generalforsamlingen, herunder forslag fra medlemmer og opstilling til bestyrelsen, skal være sekretariatet i hænde senest den 25. oktober 1998.

Storpolitik i DKUUG



(F.v.) Svend Thygesen, DKUUG-formand Myanne Olesen og Birger Jacobsen fra Dansk Standard med gaven fra den kinesiske delegation: En flaske risvin, som vi her på redaktionen glæder os til at få en smagsprøve på.

Midt i september var DKUUG og Dansk Standard vært for en international standardiseringskonference, der bl.a. skulle fastlægge, hvilke tegn, der skal lægges i fremtidens computere - og det er der storpolitik i.

I dagene 13.-17. september afholdt Dansk Standard international konference i Symbion på Østerbro i København. Der kom 40 deltagere fra hele verden, hvor godt halvdelen var fra Østen, mens resten kom fra Europa og USA. Kina stillede med otte delegerede - heraf to fra Tibet – og Korea og Japan var også mødt talstærkt op. Mødet var nemlig et skridt på vejen til at klarlægge, hvilke tegn, der skal ligge i fremtidens computere, og ingen lande er ligeglade med hvordan deres kulturelle arv behandles. Her vil hvert land kæmpe for, at netop deres tegn kommer til at ligge i fremtidens computere som standard. Og når der alligevel skal hugges en hæl og klippes en tå, så skyldes det, at ikke alle tegn bliver lige tilgængelige.

Globalt tegnsæt

Der var tale om et ekspertmøde for to arbejdsgrupper under det internationale standardiseringsorgan ISO, der skal finde ud af at lave et globalt tegnsæt. Hvorfor det er vigtigt at få sine nationale tegn med, forklarer formand for DKUUGs standardiseringsudvalg, civilingeniør Sven Thygesen: "Gradvist er behovet for at kunne håndtere alle de forskellige kultures skriftsprog dukket op. USA har jo længe dækket verden med løsninger, som brugte bogstaverne A-Z. Først skulle de vesterlandske behov dækkes og herunder de danske bogstaver Æ, Ø og Å. Her var tale om et købedygtigt marked, og det tiltrak

pc-leverandørerne. Det gik imidlertid ikke særlig godt i første omgang, hvor IBM glemte at få Ø'et med kolossale problemer i Danmark til følge. Dette er et eksempel på, hvorfor det er utroligt vigtigt at være vågen når alfabeter, sorteringsregler og tilsvarende grundlæggende elementer standardiseres. Det ved DS og DKUUG og derfor kæmper vi for at sikre os imod tilsvarende kulturelle overraskelser i den formelle standardiseringsverden, som er dækket af ISO. DS og DKUUG kæmpede f.eks. i mere end to år for at få Æ anerkendt som et bogstav, og det lykkedes også til sidst. Vi kunne ellers være løbet ind i en række problemer som f.eks. kunne betyde, at Æ'et ikke blev sorteret korrekt eller at det blev afvist i et navnefelt, fordi det ikke blev betragtet som et bogstav. Vort skriftsprog er en vigtig del af vor kultur, og hvis vi synes, at den er værdifuld, må vi også bruge de fornødne kræfter til at beskytte den mod de mangler og fejl, som international standardisering kan medføre. Her er nemlig et område, hvor der ikke er andre til at varetage vore interesser end netop os selv."

Østasiatiske tegnsæt standardiseret

Nu er de fleste vesterlandske behov dækket og derfor skal der bruges tid på at få de sidste østasiatiske skriftsprog med deres tusindvis af skrifttegn (ideografer) på plads sammen med en række specielle nutidige tegn og den mangfoldighed af historiske tegn, som de historiske annaler gemmer på (NB: runerne er kommet med i tegnsættet over alverdens tegn) - og hvert land vil selvfølgelig forsøge at få så mange af sine tegn med som muligt. Den ugelange konference var et stort skridt på vejen til at få de østasiatiske tegnsæt standardiseret - Kina, Japan og Korea er blevet enige (hvilket i sig selv næsten er en verdensbegivenhed) om at slå deres respektive tegnsæt sammen til ét med „kun" 48.000 tegn, hvilket har gjort, at det nu er realistisk at tale om et globalt tegnsæt. Den nyeste version af Windows NT har 64.000 tegn „indbygget", og da langt de fleste tegnsæt højst benytter 30 tegn, er der god plads.

SE-NR. 19082288

6 37 JAN

TBL 2904/1 CHK 2 GST 8
14SEP'99

8	KRUS QL 1/2 á 40,-	320.00
1	TUBORG	25.00
2	FAD QL 30 CL. 24,-	48.00
1	SORT GULD	29.00
1	GRQFTENS SILD	75.00
2	HANEBRYST 110,-	220.00
1	MULTE	165.00
2	SPRbNGT OX 145,-	290.00
2	SKIPPERLABSKOVES 82,-	164.00
1	STJERNESKUD	88.00
1	DANSKE OSTE	55.00
1	bBLEMOST	20.00
1	SVAMPESUPPE	55.00
1	FISKEFRIKADELLER	85.00
3	CHOKOLADESYMFONI 75,-	225.00
1	DESSERTTALLERKEN	85.00
2	KAFFE 24,-	48.00
2	GL. ALBORG TAFFE 24,-	48.00
	KONTANT	2045.00

409.00 VAT TTL 2045.00
SUBTOTAL 2045.00
BETALT 2045.00
---------6 CHECK CLOSED---------
---------14SEP'99 21:08---------

Regningen fra deltagernes middag i Grøften i Tivoli

Åh - en øjebæ

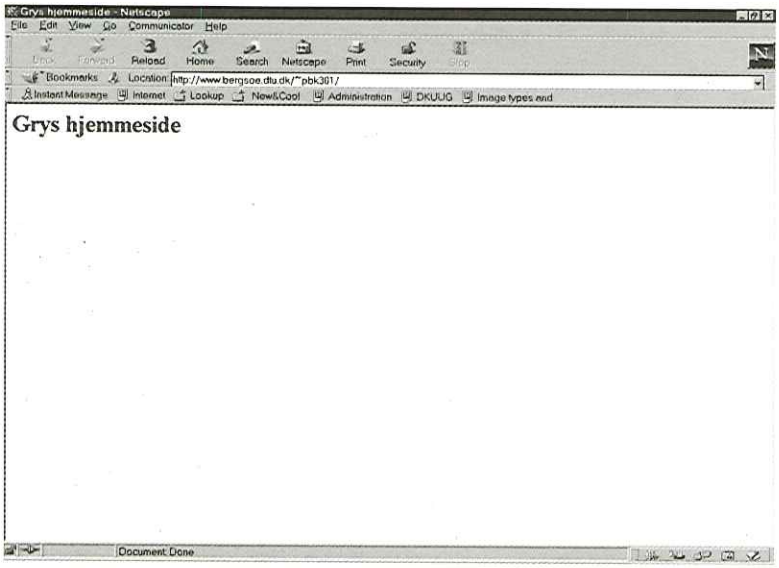
At de lokale tegn ikke er nået ud til alle computere fik konferencedeltagerne syn for, da de var ude at spise i Grøften i Tivoli. Som det ses på regningen nedenunder, drak deltagerne nogle QL, der var én, der fik en bBLEMOST, 2 fik SPRbNGT OX og der var én, der spiste GRQFTENS SILD (så må restaurantens navn vel rettelig være Grqften). I DKUUG-Nyt vil vi for fremtiden hver måned bringe eksempler på udskrifter, der ikke kan klare Æ, Ø og Å under overskriften „Åh - en øjebæ". Så hold øje med dine regninger, kvitteringer o.s.v. og send dem til DKUUG-Nyt - vi skal have Æ, Ø og Å ind i det danske sprog.

HAN

Siden sidst

Månedens hjemmesidebøf

I denne måned går bøffen til Gry, der har en hjemmeside. Desværre ved vi ikke mere om Gry end dette, men man må da sige, hun ikke spilder alt for meget af Nettets båndbredde.



SILD til overfladen

I sidste nummer af DKUUG-Nyt fortalte vi om SILD, den nye kvindegruppe i DKUUG, der er startet af foreningens sekretær Hanne Schmidt. Foreningen har vakt stor interesse blandt kvinder, der gerne vil arbejde seriøst med IT og Hanne har modtaget omkring 25 henvendelser fra interesserede kvinder - deriblandt et par kvindelige journalister, hvilket har ført til omtale i Jyllandsposten og Ingeniøren. SILD er altså en IT-forening for interesserede kvinder på alle vidensniveauer. Der er stiftende møde i SILD torsdag den 21. oktober 1999, kl. 17.00–19.00 i Symbion, Fruebjergvej 3, 2100 København Ø, Lokale M4. Interesserede (kvinder) kan kontakte Hanne Schmidt på tlf. 39 17 99 44 eller e-mail hs@dkuug.dk.

Nørdhumor

Vores opfordring til at sende nørd-jokes ind til DKUUG-Nyt har været en stor succes - så *keep them coming*. Denne kommer fra Kristian Vilmann:

Vedlagt følger en statusrapport fra vores højtuddannede konsulenter vedr. „Y2K" konvertering::

„Our staff has completed the 18 months of work on time and on budget. We have gone through every line of code in every program in every system. We have analyzed all databases, all data files, including backups and historic archives, and modified all data to reflect the change.

We are proud to report that we have completed the „Y2K" date change mission, and have now implemented all changes to all programs and all data to reflect your new standards:

Januark, Februark, March, April, Mak, June, Julk, August, September, October, November, December

As well as:

Sundak, Mondak, Tuesdak, Wednesdak, Thursdak, Fridak, Saturdak

I trust that this is satisfactory, because to be honest, none of this „Y to K" problem has made any sense to me. But I understand it is a global problem, and our team is glad to help in any way possible. And what does the year 2000 have to do with it?

Speaking of which, what do you think we ought to do next year when the two digit year rolls over from 99 to 00? We'll await your direction."

Retningslinjer for e-mail

Dansk Arbejdsgiverforening og HK prøver at blive enige om, hvordan e-mail skal behandles.

DKUUG-Nyt skrev allerede i december sidste år om problemerne omkring manglende retningslinjer for behandling af e-mails. Nu er arbejdsmarkedets parter så småt gået i gang med forhandlinger, der skal slå fast, hvordan man behandler e-mails på arbejdspladsen.

Hvem ejer en e-mail?

Kort fortalt står slagsmålet om, hvem en medarbejders e-mails tilhører. Kan e-mail sidestilles med almindelig post og har arbejdsgiveren lov til at læse sine ansattes e-mail?

I DKUUG-Nyt 108 skrev vi:

„De færreste (forhåbentlig ingen) danske virksomheder ville vel åbne breve, der var adresseret til en medarbejder eller aflytte medarbejderens telefon, selvom firmaet betaler telefonregningen. Det er ikke alene umoralsk, men også strafbart ifølge straffelovens §263, der lyder: *„Med bøde, hæfte eller fængsel i op til 6 måneder straffes den, som uberettiget unddrager nogen et brev, telegram eller anden lukket meddelelse eller optegnelse eller gør sig bekendt med indholdet."* Loven er fra 1972 og nævner naturligt nok ikke e-mail, men en betænkning fra 1985 har sørget for, at også *„uberettiget adgang til programmer og data til elektronisk databehandling"* er blevet gjort ulovligt. Formanden for IT-sikkerhedsrådet, professor, dr. jur Mads Bryde Andersen, tolker loven derhen, at det ikke er ulovligt at se **adressaten** på en andens e-mail, men det er ulovligt at se indholdet.

Et andet spørgsmål er, om e-mail er en lukket meddelelse. Hvis der ikke er tale om en telefonforbindelse, der er reserveret til formålet eller om en krypteret meddelelse, kan en e-mail nemt læses af andre. Som minimum kan afsenderens og modtagerens systemadministratorer læse e-mail'en. Men må systemadministratoren også gøre det?

Nej, ikke ifølge Bryde Andersen. Han mener dog, at der kan være situationer, hvor nogle bliver nødt til at se andres e-mail, eksempelvis hvis en medarbejder har downloadet data, der får systemet til at gå ned - store billedfiler f.eks. I sådanne tilfælde må arbejdsgiveren ifølge Bryde Andersens opfattelse være berettiget til at påtale indholdet, hvis det er utilstedeligt".

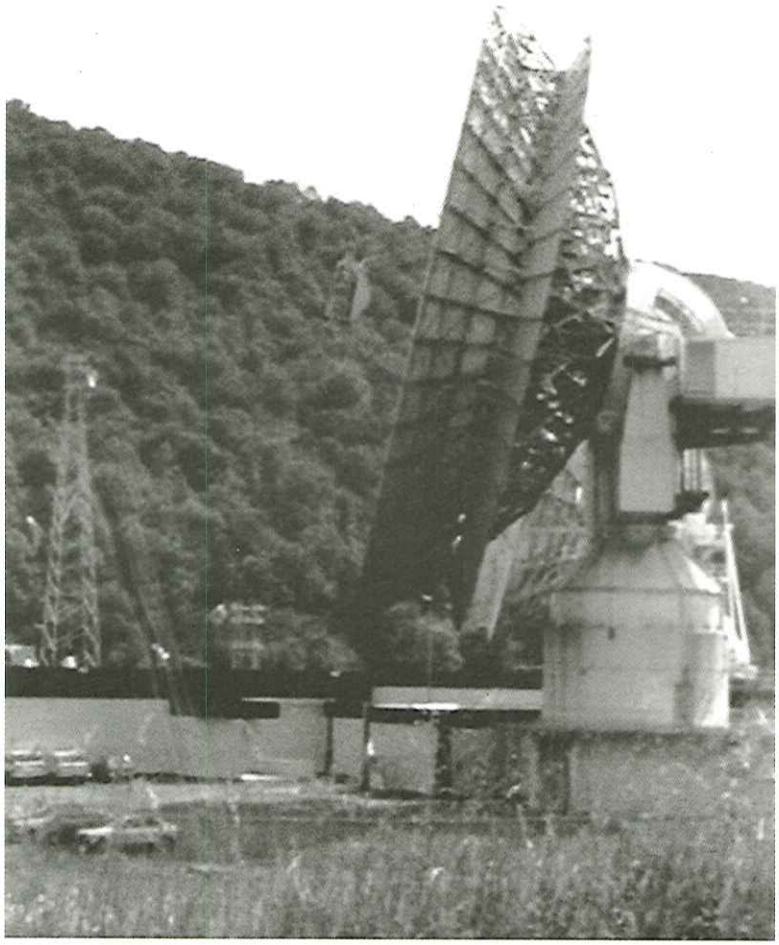
Arbejdsmarkedets parter ikke langt fra hinanden

Faktisk er Arbejdsgiverforeningen og HK ikke langt fra hinanden i spørgsmålet om e-mail. Tilsyneladende har arbejdsgiverne erkendt, at e-mail ikke kan sidestilles med almindelige breve, men mere har karakter af en skriftlig telefonsamtale. Det, som parterne nu skal forhandle om, er retningslinjer for, hvornår virksomheder må åbne en ansat's mail.

Historien melder ikke noget om, hvorvidt katalogisering af e-mail også skal systematiseres. Vi har tidligere fortalt om Karlebo Kommune, der lukkede for e-mail til rådhuset, fordi arbejdsbyrden blev for stor. Kommunen havde nemlig valgt at lade al mail skrive ud og blive journaliseret - gad vide, hvem der haft glæde af at læse de mails. Så indtil videre bliver det nok op til den enkelte virksomhed, hvordan e-mail skal håndteres.

HAN

Echelon - hvad er det?



Vi ser på Echelon´s historie - hvis det altså eksisterer.

Ifølge ordbogen betyder Echelon i militær sammenhæng „trinvis forskudt opstilling". Men på det seneste er Echelon blevet kendt i offentligheden for at være navnet på et globalt aflytningssystem, styret af NSA (National Security Agency) - det amerikanske regeringsorgan, der overvåger elektronisk kommunikation.

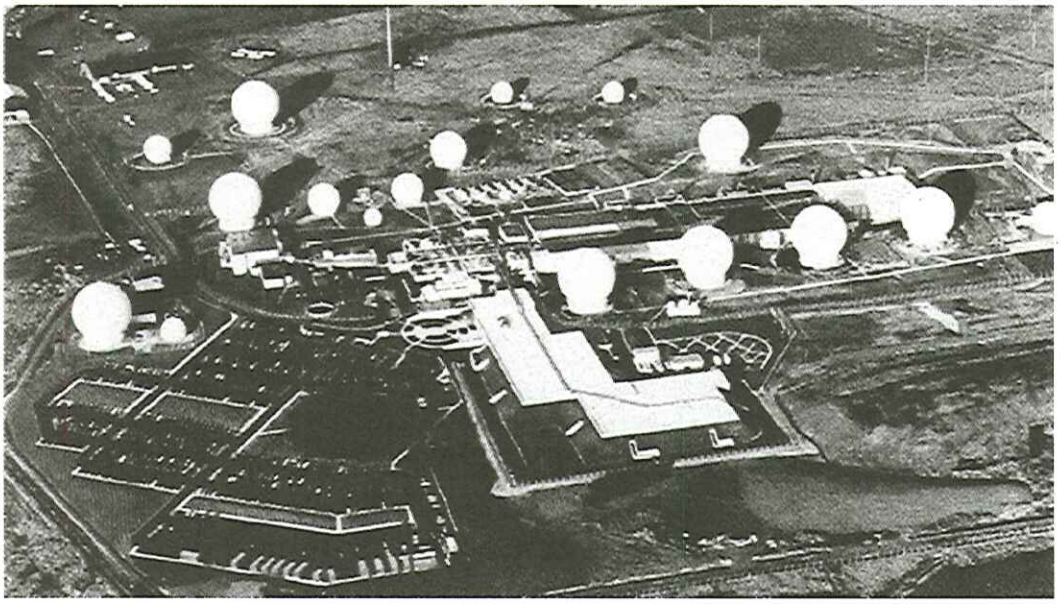
Historien bag Echelon

Efterretningstjenester har drevet Communications Intelligence (Comint) i over 80 år. Før USA trådte ind i 1. verdenskrig i 1917 var den amerikanske efterretningstjeneste begyndt at aflytte de engelske kommunikationskabler under Atlanten, der bar det meste af Europas telekommunikation. I 1920 blev det afsløret, at amerikanerne havde „glemt" at holde op med at aflytte kablerne, selvom England nu var allieret og krigen var overstået - og det blev også afsløret, at den engelske efterretningstjeneste var begyndt at aflytte kommunikationen den anden vej. Det vides med sikkerhed, at den amerikanske efterretningstjenester i mellemkrigstiden og under 2. verdenskrig havde England som vigtigste aflytningsmål. Efter USA og England i 1943 blev allierede i krigen, begyndte de to efterretningstjenester dog så småt at arbejde sammen om Comint.

Aflytning af **venligtsindende** nationer har altså en lang tradition. I 1947 indgik USA og England en hemmelig aftale om at fortsætte samarbejdet med global Comint under navnet UKUSA. Samarbejdet blev tiltrådt af tre andre engelsk-talende nationer - Canada, Australien og New Zealand, som blev „second parties". UKUSA-samarbejdet blev første gang officielt anerkendt i marts 1999, hvor den australske regering bekræftede, at dens efterretningstjeneste DSD „samarbejder med oversøiske efterretningsorganisationer i UKUSA-samarbejdet". Denne udtalelse har bekræftet skeptikere i, at der i mange år har eksisteret et antal (ca. 20) „third parties"- lande, der deltager i samarbejdet. Ifølge journalisten Duncan Campbell (mere om ham andetsteds) tiltrådte Danmark UKUSA i 1952.

Echelon´s fødsel

UKUSA-samarbejdet overvågede i begyndelsen telefonlinjer og radiokommunikation, hvilket er forholdsvis enkelt at opfange. Ifølge de nyeste oplysninger indså NSA og CIA i slutningen af 1960´erne, at kommunikation fra rummet ville blive et effektivt kommunikationsmiddel, og der måtte findes et middel til at overvåge satellitter. Et aflytningsssystem blev etableret, men tjenesterne opdagede hurtigt, at det var alt for effektivt - mængden af informationer oversteg langt, hvad de ansatte kunne klare at analysere (NSA praler ellers at have verdens største koncentration af analytikere, kodeeksperter o.s.v.). Derfor udviklede UKUSA et computersystem, der automatisk filtrerer informationer og det er dette system, der blev døbt Echelon. Systemet må have



Verdens største aflytningsstation, Menwith Hill i England

været i brug meget tidligt, for et af beviserne på Echelons eksistens er fra en officiel liste over databanker i verdens største aflytningsbase, Menwith Hill i England, der i 1979 viste, at man bruger systemet **Echelon 2.** Det er i øvrigt muligt, at systemet i dag hedder noget helt andet, for efterretningstjenesterne skynder sig at skifte kodenavne, når et sådant bliver offentligt kendt.

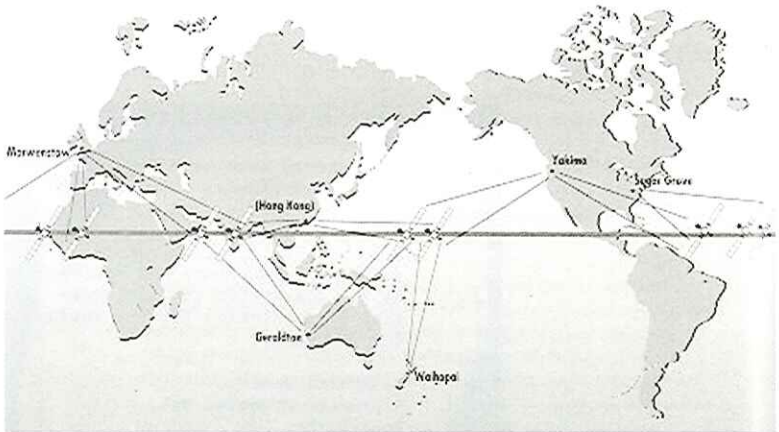
Sådan fungerer Echelon

Kritikere mener, at det verdensomspændende Echelon-system opsnapper en meget stor del af verdens e-mail-, fax- og telefonkommunikation. Dette må resultere i datamængder, der umiddelbart virker uoverskuelige, men her kommer computerne til hjælp. Echelon filtrerer atomatisk ved hjælp af søgeord - ligesom søgemaskiner på Internettet. Stadigvæk må datamængden være enorm, men alligevel - i 1992 redegjorde tidligere NSA-direktør William Studeman for efterretningstjenesternes muligheder for opsnapning:

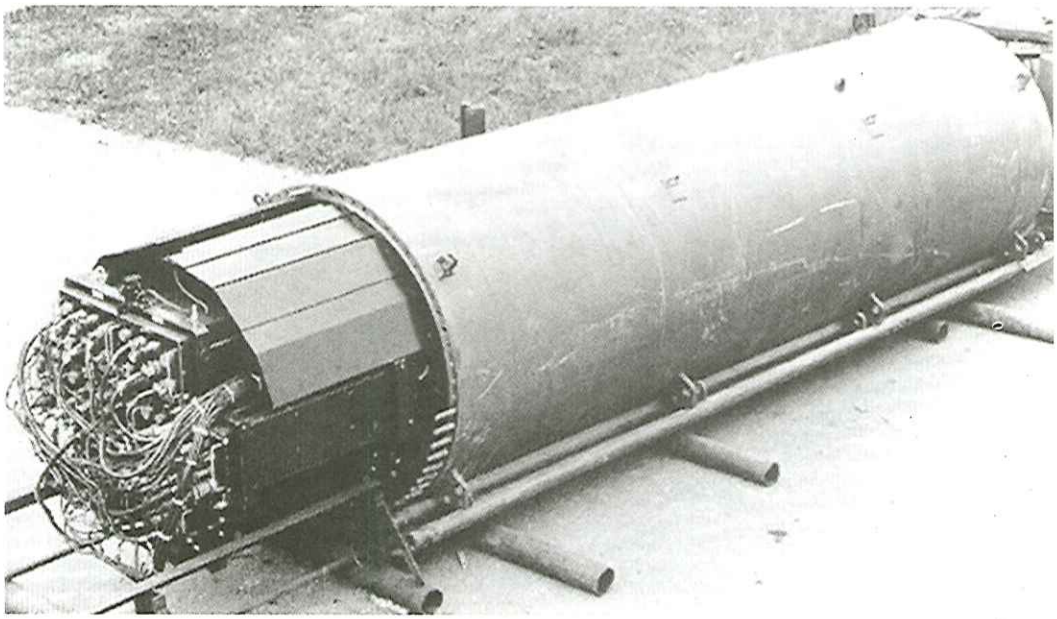
„One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence." Hvis der her tale om realistiske tal, er datamængderne jo til at have med at gøre.

Interception - opsnapning

Der findes ikke et rigtigt godt dansk ord for interception (hvilket måske siger noget om danskerne), men vi har valgt at kalde det opsnapning. Telefonaflytning har været kendt, sålænge der har eksisteret telefoner. Faktisk er de danske telefonselskaber ifølge retsplejeloven forpligtede til at muliggøre aflytning på telefoncentraler - men kun til politiet og kun ifølge retskendelse. Om det så kun er politiet, der lytter med, kan man jo kun gisne om. Selvom man ikke skulle have adgang til en telefoncentral, er der jo stadig muligheden for at sætte aflytningsapparater på selve kablerne, hvilket giver mulighed for aflytning af telefonsamtaler, e-mail og fax. Sandsynligvis er automatisk talegenkendelse endnu ikke så udviklet, at man kan overlade til computerne at sortere telefonsamtaler efter kodeord, men e-mail og fax er nemt at opsnappe og sortere. Aflytning af mobiltelefoner er et kapitel for sig - tilsyneladende er det svært, men ikke umuligt. Det er derimod ikke særligt svært at opsnappe kommunikation til og fra satellitter.



Oversigt over Echelons overvågnings af Intelsat-satelitterne

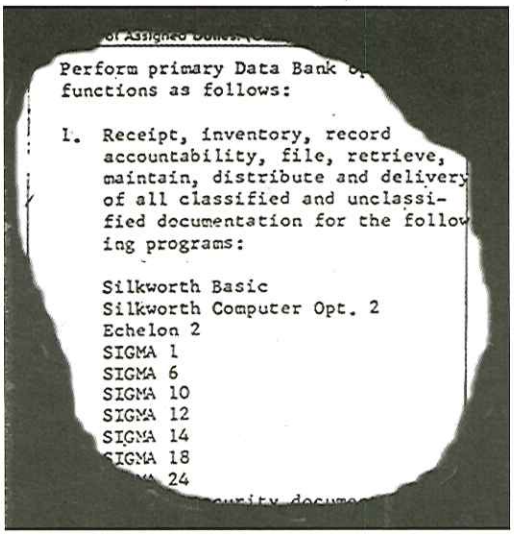


Ivy-bells aflytnings-sonden, som den amerikanske marine brugte til aflytning af russiske telefonlinjer ved Kamchatka

Beviser på Echelons eksistens

Det er svært at finde beviser på Echelons eksistens, da det officielt ikke findes, men der er dog efterhånden mange indicier. Ifølge officielle amerikanske dokumenter blev der i 1990 etableret en „ECHELON training department" på Sugar Grove-basen i Virginia. Da træningen var overstået, blev basens formål „to maintain and operate an ECHELON site". Så der findes altså noget, der hedder Echelon.

En anden officielt bekræftelse på noget, der hedder Echelon, findes i et hemmeligtstemplet dokument fra det amerikanske flyvevåbens efterretningstjeneste, Air Intelligence Agency. I et afsnit med overskriften „Activation of Echelon Units" fremgår det, at to nye stationer vil blive aktiveret 1. januar 1995. Ifølge seniorforsker Jeffrey Richelson fra tænketanken National Security Archives ligger de to omtalte stationer i hhv. Osan, Sydkorea og Misawa, Japan.



Perform primary Data Bank o
functions as follows:

1. Receipt, inventory, record accountability, file, retrieve, maintain, distribute and delivery of all classified and unclassified documentation for the following programs:

Silkworth Basic
Silkworth Computer Opt. 2
Echelon 2
SIGMA 1
SIGMA 6
SIGMA 10
SIGMA 12
SIGMA 14
SIGMA 18
24

Omtale af Echelon 2 i officielt dokument fra 1979

I 1996 offentliggjorde forfatteren Nicky Hager bogen „Secret Power: New Zealand´s Role in the International Spy Network". Bogen skabte for første gang større opmærksomhed om Echelon, da den sandsynliggjorde, at New Zealand var en del af en verdensomspændende aflytningsring. Mere specifikt bidrager New Zealand til Echelon med at opsnappe information fra de to Intelsat-satellitter, der dækker Stillehavet. En meget stor del af klodens e-mail, fax og telex´er går gennem de 20 Intelsat-satelitter, der kredser omkring Jorden ved Ækvator, og det er altså Hager´s påstand, at satelitterne overvåges fra stationer spredt over hele jorden, der sender informationerne videre til NSA. New Zealand´s premierminister fra 1984-89, David Lange, skrev forordet til Nicky Hager´s bog. Han var ellers i årevis irriteret på Hager, men i forordet skriver han: „State-sponsored terrorism was a crime against humanity as long as it wasn't being practiced by the allies, when it was studiously ignored. In the national interest it became necessary to say „ouch" and frown and bear certain reprisals of our intelligence partners. We even went to the length of building a satellite station at Waihopai. But it was not until I read this book that I had any idea that we had been committed to an international integrated electronic network."

I 1997 lykkedes det for en reporter og en kameramand at bryde ind på Waihopai-basen og filme ind i basens kontrolcenter gennem halvt lukkede gardiner. Bemærkelsesværdigt nok bestod kontrolcentret af endeløse rækker af ubemandede terminaler. På et af bordene lå en teknisk manual til Intelsat-satellitten, hvilket for skeptikerne er bevis på, at basen overvåger de to Intelsat-satellitter, der dækker Stillehavet. Offentliggørelsen skabte ramaskrig på New Zealand, for hvad var det helt præcist, basen overvågede? New Zealand har ingen militære

fjender og bortset fra Australien ingen naboer i en omkreds af flere hundrede kilometer.

Bruges Echelon til industrispionage?

Hvis vi antager, at Echelon eksisterer og er styret af NSA, melder spørgsmålet sig selvfølgelig hvad et anlæg, der overvåger venligtsindende nationer, skal bruges til. Hvad har Storbritannien, Canada, Australien og New Zealand (for nu at tage de anerkendte medlemmer af UKUSA-samarbejdet) ud af at overvåge deres naboer og sende informationerne videre til USA? Svaret kan være: Industrispionage.

STOA-rapporten, som Duncan Campbell afleverede til Europa-parlamentet i foråret, opregner et antal sager, hvor Echelon kan være brugt til „Comint ecenomic intelligence":

1) Thomson CSF og Brasilien.

I 1994 opsnappede NSA telefonsamtaler mellem det franske firma Thomson-CSF og Brasilien angående SIVAM, et overvågningssystem til Amazonas´ regnskov med et budget på 1,3 milliard $. På trods af, at Thomson skal have bestukket medlemmer af den regeringskommission, der skulle vælge udbyderen til projektet, gik kontrakten alligevel til det amerikanske firma Raytheon Corporation, der pudsigt nok også vedligeholder NSA´s Echelon-station i Sugar Grove. NSA har ikke benægtet, at de har opsnappet og videregivet det franske tilbud og har faktisk forsvaret sig med, at den slags er nødvendigt, da amerikansk lov ikke tillader udbetaling af bestikkelse noget sted i verden.

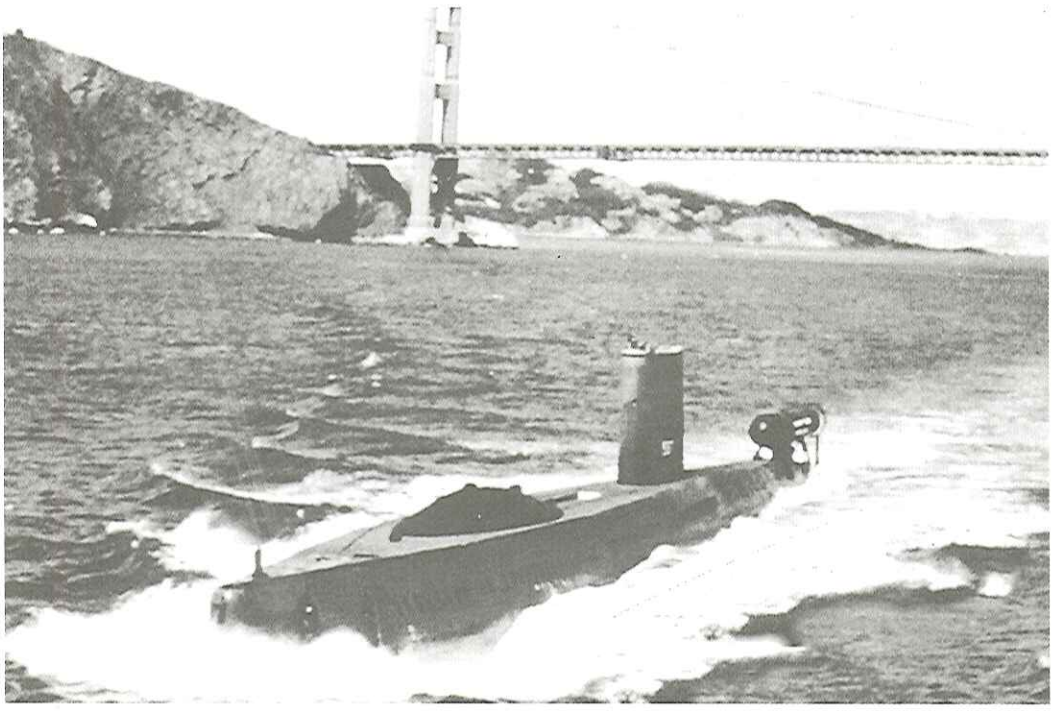
2) Airbus Industrie og Saudi-Arabien.

NSA opsnappede faxer og telefonsamtaler fra en kommunikationssatellit mellem det franske konsortium Airbus, det Saudi-Arabiske flyselskab og den Saudi-Arabiske regering. Tilsyneladende tilbød Airbus bestikkelse til en Saudi-Arabisk embedsmand i forbindelse med en ny kontrakt til 6 milliarder $. NSA gav oplysningerne videre til Boeing og McDonnell Douglas, der pressede deres tilbud og fik kontrakten.

Mange andre pålidelige rapporter melder om tilfælde, hvor USA har brugt Comint for at få en fordel overfor andre handelspartnere. NSA er mistænkt for at lække oplysninger til amerikanske firmaer i forbindelse med udviklingen af mindre forurenende biler i Japan (tilsyneladende beordret af præsident Clinton selv, der aldrig har lagt skjul på, at Comint er en legitim fremgangsmåde, når det gælder om at skaffe USA handelsforspring), spionage mod VW og BMW, forhandlinger om import af luksusbiler i Japan, den franske deltagelse i GATT-forhandlingerne og meget mere.

Og hvad har så samarbejdspartnerne ud af at levere oplysninger til NSA, der potentielt kan være skadelige for deres eget lands industri? Dette spørgsmål stillede Søren Møller Christensen, tidligere redaktør på det militærkritiske tidsskrift forsvar Forsvar, til Duncan Campbell ved mødet i medborgerhuset i Ahlefeldtsgade 13. september. Campbell svarede, at efterretningskulturen er domineret af USA og NSA, derfor gør man det. Søren Møller samtykkede og udtalte til Information: „Det kan være et udslag af behovet for at finde nye fjender og mål. De (*efterretningstjenesterne - Red)* må være hårdt ramt af freden."

HAN



U-båden USS Halibut med Ivy-bells-aflytningssonden monteret bagerst

Danmark og Echelon - er vi med?

Aflytningsbasen Aflandshage på Amager

Efter afsløringen af Echelon-samarbejdet, er det store spørgsmål herhjemme - er Danmark med?

Før hans besøg i Danmark midt i september mente Duncan Campbell ikke, at Danmark var med i Echelon-samarbejdet. Men en tur til sydspidsen af Amager, Aflandshage, overbeviste ham om noget andet.

Her ligger nemlig en stor dansk base, der lige er blevet udvidet kraftigt, bl.a. med en kæmpe golfbold. „Det ligner nøjagtigt en, jeg har set på New Zealand - den her er bare meget større", siger Duncan Campbell.

Den base, Campbell hentyder til, er Waihopeibasen på New Zealand, en lyttestation i Echelon-samarbejdet. Så hvad laver basen på Amager?

Aflandshage

På Amagers sydspids - lige syd for Kongelunden - har siden 1950 ligget Danmarks lyttestation 3. Dengang havde stationen 80 ansatte, men op gennem 60´erne voksede antallet af ansatte ifølge grundlæggeren, kommandør Mørch, til ca. 1000. Selvom den Kolde Krig har været overstået i snart 10 år, er der ikke noget der tyder på, at der er blevet færre ansatte i systemet - og hvad laver de så? Og hvorfor er det blevet nødvendigt med en gevaldig udvidelse (nogle siger en tredobling), når man formodentlig ikke skal overvåge Østblokken med samme styrke som før? **HVEM ER DET HELT PRÆCIST DANMARK AFLYTTER?**

Danmark samarbejder med andre efterretningstjenester

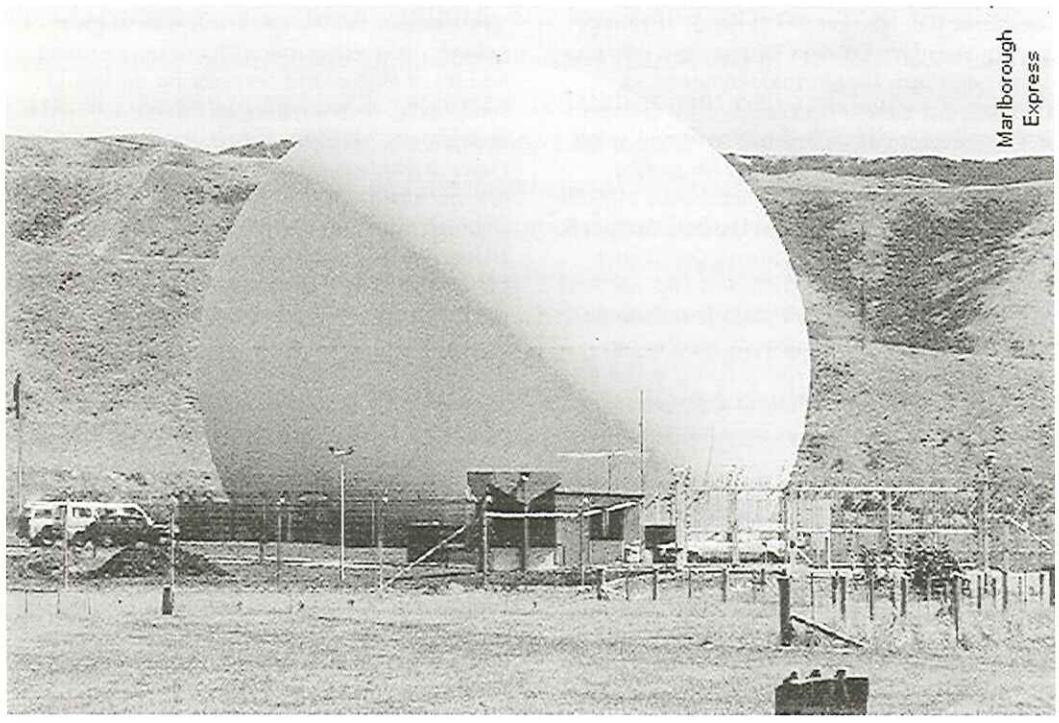
Efterretningstjenester er i sagens natur hemmelighedsfulde - derfor vil ingen udtale sig om basen på Amager. Det står dog fast, at Danmark har en række aflytningsstationer. Ifølge Duncan

NSA´s Sugar Grove-base i Virginia

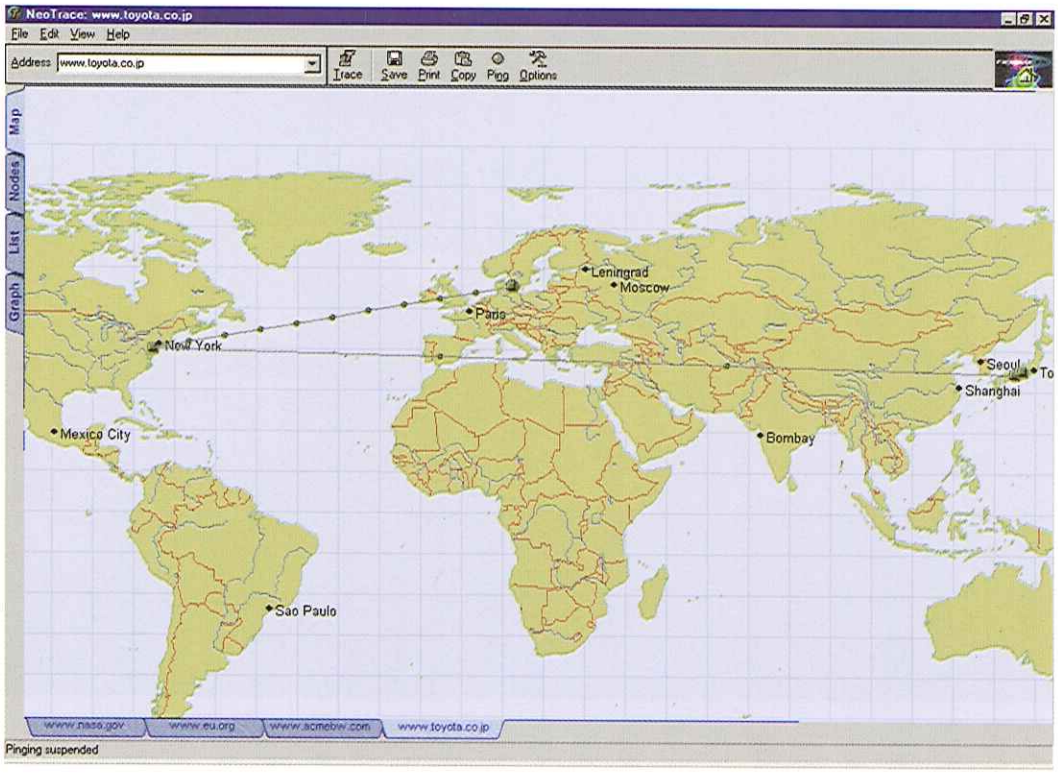
Campbell har Danmark aflytningsbaser følgende steder:

- Aflandshage
- Bornholm (2)
- Gedser
- Hjørring
- Løgumkloster
- Skagen

Både justitsministeren og forsvarsministeren har hidtil hævdet, at de aldrig har hørt om Echelon, men i et samråd den 17. september ville forsvarsminister Hans Hækkerup ikke afvise, at det eksisterede - kun kendte han ikke andet til det, end han havde læst i pressen. Derimod bekræftede Hækkerup, at stationen på Aflandshage bruges til aflytning af elektronisk kommunikation og at Danmark har „en lang række samarbejdspartnere blandt andre landes efterretningstjenester". Men Hækkerup siger, at det ikke har noget med Echelon at gøre, og iøvrigt har han ikke læst Duncan Cambell´s



Waihopei-basen på New Zealand



Kortlægning af en søgning på Toyota - bemærk, at man fra København skal til New York for at komme til www.toyota.co.jp i Tokyo.

rapport. Det finder SF´s Holger K. Nielsen meget mærkeligt: „I en sag som denne skulle man tro, at han i hvert fald ville have læst den", siger han.

Forsker: Echelon eksisterer

Dr. phil. Poul Villaume, lektor på Institut for Historie på Københavns Universitet er ekspert i den danske efterretningstjeneste. Han bekræfter overfor DKUUG-Nyt, at det er sandsynligt, at Echelon eksisterer. „Det hedder nok noget andet nu, hvilket sandsynligvis er grunden til, at forsvarsministeren med god samvittighed kan hævde, at han ikke kender til noget aflytningssystem ved navn Echelon." Ifølge Poul Villaume viser nyligt offentliggjorte dokumenter, at Danmark har været en særdeles aktiv deltager i NATOs aflytning af radiokommunikation siden 1950´erne. Derfor anser han det for ganske sandsynligt, at Danmark har været aktiv i UKUSA-samarbejdet siden 1952, som Duncan Campbell hævder. Hvad de danske aflytningsstationer foretager sig nu, efter Østblokkens fald, har Poul Villaume ingen idé om. „Aflytningsstationerne bruges sikkert til at overvåge terrorister og slyngelstater, men udfra min erfaring er det ikke usandsynligt, at Danmark også deltager i økonomisk spionage og at informationerne går til NSA."

Poul Villaume opfordrer til større parlamentarisk kontrol med efterretningstjenesterne. Tysklands efterretningstjeneste, Bundesverfassungsschutz, er underlagt streng parlamentarisk kontrol, og det samme er den norske efterretningstjeneste for nylig blevet efter en række skandaler. Denne holdning deles af en række danske politikere fra begge sider i Folketingssalen, hvor både Enhedslisten, Venstre og de radikale opfordrer til større kontrol med efterretningstjenesterne.

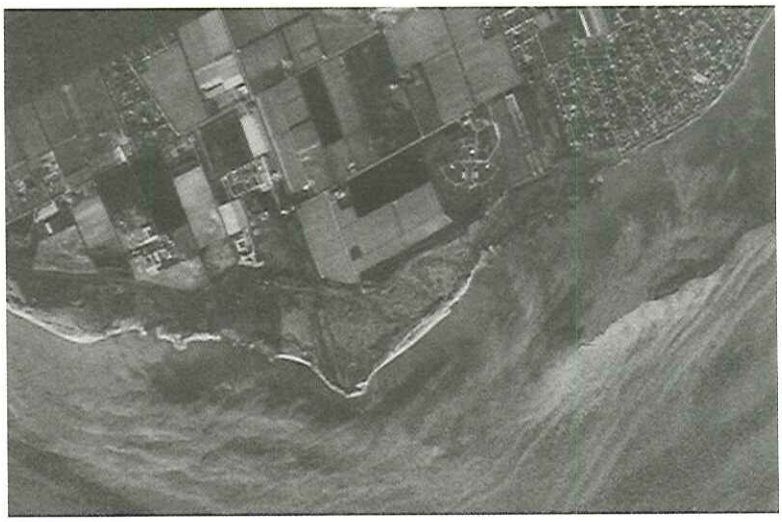
Sikkerhedschef: Echelon eksisterer

På PROSA og Informations borgermøde med Duncan Campbell bekræftede Tele Danmarks koncernsikkerhedschef Jørgen Bo Madsen, at Tele Danmark aflytter danskernes telefonsamtaler. „Jeg er overbevist om, at Echelon eksisterer og det har jeg været i årevis", udtalte han. Men Tele Danmark bidrager ikke til det. „Vi og de andre teleselskaber skal ifølge retsplejeloven give politiet - ikke efterretningstjenesterne - mulighed for at aflytte vore centraler og det gør vi selvfølgelig. Men aflytningen foregår kun efter retskendelse." Madsen kunne ikke udtale sig om, hvorvidt efterretningstjenesten lytter med, men han har siden udtalt til Information, at Tele Danmark ikke bliver aflyttet af NSA. Siden afsløringen af Echelon har det ellers vakt en del bekymring, at Tele Danmark er købt af amerikanske Ameritech, som NSA har et aflytningspunkt hos. „Men det betyder ikke, at de *(NSA-red.)* har en slange inde i Danmark", siger han.

Hvadenten Tele Danmark aflyttes eller ej, opfordrede Jørgen Bo Madsen kraftigt til at bruge kryptering. Aftenens eneste diskussion kom, da Madsen hævdede, at mobiltelefoner ikke kan aflyttes. Det var Duncan Campbell uenig i, da han bl.a. mente, der var lagt en svækkelse ind i selve GSM-krypteringsstandarden A5, der muliggjorde aflytning. De eksperter, DKUUG-Nyt har talt med, er vildt uenige om mulighederne for aflytning af mobiltelefoner - det ser vi nærmere på i næste nummer.

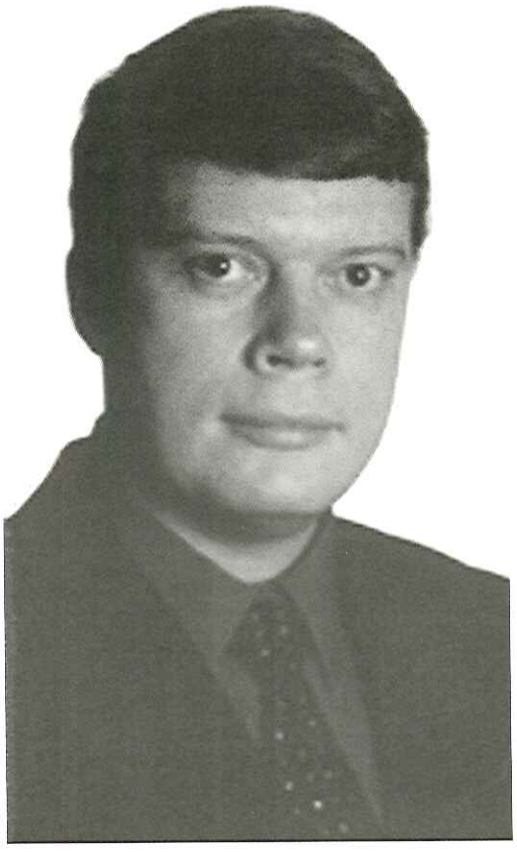
Skalkeskjul for Echelon?

Siden 1993 har repræsentanter for ordensmagten i mange europæiske lande og de fleste UKUSA-nationer holdt regelmæssige møder i en indtil for nylig ukendt organisation, ILETS, der er oprettet af FBI. I ILETS udveksles erfaringer indenfor opsnapning af elektronisk kommunikation, men EU-politikere har længe ment, at ILETS er et skalkeskjul for noget helt andet, nemlig NSA´s forsøg på at indsamle krypteringsnøgler. Forhistorien er denne: I 1990 og -91 blev den amerikanske regering bekymret over, at AT&T var begyndt at markedsføre et telefonsystem, der ikke kunne aflyttes. AT&T blev overtalt til at trække systemet tilbage, og i stedet tilbød regeringen, at firmaer kunne indbygge NSA´s „Clipper" chip i telefoner. Chippen skulle fremstilles af NSA og skulle registrere og videresende krypteringsnøgler til NSA og andre offentlige organer. Forslaget mødte kraftig modstand og blev trukket tilbage. I stedet fik den amerikanske regering vedtaget, at ikke-statslige organisationer skal opbevare kopier af alle brugeres krypteringsnøgler i et system, der først hed „key escrow" og nu hedder „key recovery". Mange mener nu, at NSA har brugt ILITS til at overbevise europæiske ordenshåndhævere om at anvende deres „key recovery"-system. David Herson, chef for EU Senior Officer´s Group on Information Security, udtale i 1996: „"Law Enforcement" is a protective shield for all the other government activities...We´re talking about foreign intelligence, that what´s it´s all about. There is no question (that) law enforcement is a smokescreen." I det hele taget har EU-politikere og embedsmænd været voldsomt irriterede over ILITS-samarbejdet, der foregår helt uden politisk kontrol - hvilket giver mindelser om Wassenaar-traktaten. ILITS har siden 1993 holdt en stor årlig konference med repræsentanter fra 12-15 lande´s ordensmagt og Danmark har været med hvert år undtaget 1995.



Aflytningsbasen Aflandshage på Amager

I denne forbindelse fremhæver Duncan Campbell, at der er forskel på de tekniske, legale og organisatoriske retningslinjer for ordenshåndhævere og efterretningstjenester. Ordenshåndhævere - politiet, PET o.s.v. - vil normalt ønske at overvåge en bestemt person eller gruppe og skal normalt retfærdiggøre deres holdninger for en juridisk eller administrativ instans. Efterretningstjenester opererer udfra meget generelle retningslinjer og skal ikke retfærdiggøre deres handlinger - de skal ikke engang sandsynliggøre, at overvågningsobjektet har kriminelle eller skadelige hensigter.



Jørgen Bo Madsen, koncernsikkerhedschef i Tele Danmark

Overvåger NSA danskerne?

Ifølge Duncan Campbell er risikoen for at blive registreret i Echelon ikke stor, sålænge man holder sine telefonsamtaler og e-mail´s indenfor Danmarks grænser, bl.a. fordi dansk talegenkendelse ikke er ret langt fremme (det er noget andet med engelsk). Problemet er bare, at man ikke kan være sikker på, hvilke servere hvor i verden, ens kommunikation bliver sendt igennem. Vi prøvede her på redaktionen at kortlægge søgning på forskellige servere rundt i verden, og det viser sig, at langt det meste af Internettes kommunikation på et eller andet tidspunkt går gennem en af de store amerikanske Internetudbydere - faktisk kan man med adgang til tre amerikanske udbydere overvåge langt det meste af verdens elektroniske kommunikation. Selv mails fra Danmark til Sverige kan gå over servere i USA - og det er jo ikke særligt betryggende.

HAN

Duncan Campbell: Ét-mands-korstog

Læs mere om Echelon og kryptering

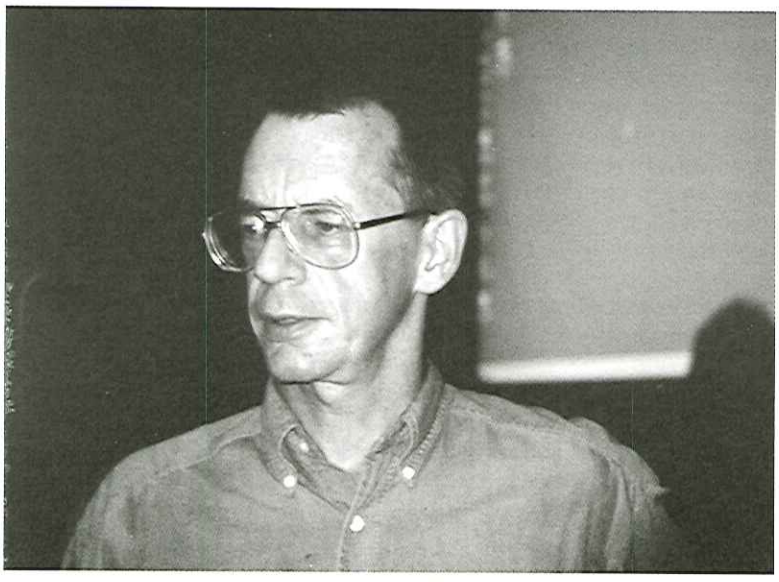
På www.dkuug.dk har vi samlet en række links om emnet under punktet Echelon.

Links:

Dagbladet Information har behandlet Echelon i en række artikler, der er samlet på www.information.dk. PROSA har også behandlet emnet på www.prosa.dk. Duncan Campbell,s hjemmeside kan findes på www.gn.apc.org/duncan Campbell´s EU-rapport „Interception Capabilities 2000" kan læses på www.ittvreports.-mcmail.com/-ic2kreport.htm

I over 20 år har tv-journalisten Duncan Campbell været en torn i øjet på vestlige efterretningstjenester, og på det seneste er de sikkert blevet endnu mere sure på ham. Vi tegner et portræt af Duncan Campbell - og det er faktisk en temmelig utrolig historie.

Oprindeligt var Duncan Campbell fysiker, men „jeg havde ikke lyst til at lave atombomber", siger han. I stedet har han siden slutningen af 70´erne brugt sine evner som opsøgende journalist til at følge efterretningstjenesterne nøje. Uanset hvem man taler med - politikere, embedsmænd, forskere - står der respekt om Duncan Campbell og hans utrættelige kamp for at afsløre efterretningstjenesternes systematiske aflytning af borgerne. Når man har oplevet Campbell „live" falder respekten bestemt ikke - han fremlægger sine synspunkter stringent og overbevisende og er f.eks. ikke bange for at gå ind i en diskussion med Tele Danmarks koncern-sikkerhedschef om GSM A5-standarden har sat nogle bits til 0 med deraf følgende svækkelse af krypteringen - noget, der i hvert fald gik hen over hovedet på Deres udsendte. Men hvem er han egentlig, denne mand?



Duncan Cambell ved borgermødet 13. september 1999

Første anholdelse

På vej hjem fra et interview med en tidligere ansat i den britiske efterretningstjeneste blev Duncan Campbell for første gang anholdt. Det var i 1977. Han og en kollega blev sigtet for at have forbrudt sig mod den engelske lov om åbenhed i forvaltningen „the Public Secret´s Act" med en straframme på op til 30 års fængsel. Først to år senere fik Campbell og kollegaen rettens ord for, at de ikke havde gjort noget forkert.

Ti år senere var Campbell igen i konflikt med myndighederne. Han lavede en tv-udsendelse om den projekterede engelske spionsatellit Zircon - der i øvrigt blev for dyr til at blive fremstillet - men den engelske efterretningstjeneste pressede BBC til at undlade at sende programmet. I stedet skrev Campbell en artikel i tidsskriftet New Statesman, men dagen før bladet skulle komme på gaden, konfiskerede regeringen hele oplaget. New Statesman´s produktionsleder fik trykt et nyt oplag et andet sted og Duncan Campbell flygtede på cykel til Underhuset, hvor Robin Cook (senere udenrigsminister for New Labour) skjulte ham, til artiklen kom ud. Samtidig sendte de kopier af BBC-filmen i omløb.

TV-drama om Duncan Campbell

I 1989 udsendte BBC et „drama" om en efterladende, utroværdig journalist, der bedrager sine kilder, ernærer sig som butikstyv, ikke vil indrømme sin homoseksualitet og fornøjer sig med at klæde sig ud i dameundertøj. Duncan Campbell lagde sag an - og vandt (!). BBC måtte hoste op med 500.000 kr. i erstatning.

Dette er bare nogle eksempler på den forfølgelse, Duncan Campbell har været udsat i årenes løb. Men forfølgelsen har ikke fået ham til at opgive kampen mod efterretningstjenesternes aflytning af almindelige borgere. Hans to Echelon-rapporter til Europaparlamentet har affødt politisk ønske om mere kontrol med efterretningstjenester. Iflg. Information har Campbell det mål, at „EU skal indføre, at information som standard skal være krypteret." Hele ideen om, at man skal kunne aflytte hvad som helst alene af den årsag, at det kan hjælpe i kriminel efterforskning - hvilket de hemmelige tjenester ofte forsvarer aflytningsmetoderne med - forekommer ham lettere absurd. „Man forbyder jo heller ikke biler, bare fordi kriminelle også bruger dem." siger Duncan Campbell.

HAN

Sådan bruger du PGP

Vil du gerne bestemme, hvem der kan læse dine e-mails? Sådan bruger du krypteringsprogrammet PGP.

af Nicolai Gylling

PGP (Pretty Good Privacy) er den mest udbredte form for kryptering af dokumenter på internettet. Herunder vil jeg gennemgå hvordan man bruger PGP til kryptering af email.

PGP fungerer ved at man har 1 sæt nøgler, bestående af en public key og en private key. Public key'en giver man til den, som har behov for at sende PGP-krypteret email til dig, og private key'en holder man for sig selv.

Lad os sige, at A ønsker at sende en krypteret besked til B. A skal så have fat i B's public key, enten fra B selv, eller en af de nøgleservere der findes rundt om i verdenen. Så tager A og bruger et PGP-program, der krypterer emailen med B's public key. Når B så modtager emailen i krypteret format, starter B sit PGP-program, som genkender emailen som PGP-krypteret og dekrypterer den for ham.

Installation under Windows:

1. Først skal du bruge et PGP-program, f.eks. PGP 6.5.1 til Windows 95/98/NT, som du kan hente fra DKUUG's ftp-server på www.dkuug.dk.
2. Unzip og kør Setup.exe
3. Efter de første indledende spørgsmål, får du mulighed for at vælge forskellige komponenter, bl.a. plugins til forskellige mailere, Eudora, OutLook, Exchange, men desværre IKKE til NetScape. Jeg har testet det med Eudora.
4. Så kommer der et spørgsmål om du har nogle eksisterende PGPkey-filer. Hvis du har kørt med PGP før, har du en fil med public og private key's, du kan importere.
5. Så er det tid til at starte PGPKeys og generere sig et key-sæt. Først skal du indtaste navn og emailadresse.
6. Så skal der vælges en PGP-type. Her anbefales det at benytte Diffie-Hellman/DSS.
7. Keypair size skal MINIMUM være 2048.
8. Herefter kan du vælge om dit key-sæt kan udløbe efter en given dato. Jeg valgte nej.
9. Så skal du vælge en passphrase, som skal indtastes hver gang, du vil dekryptere en besked.
10. Efter lidt beregningstid, får du mulighed for at lægge din public key ud på internettet på en keyserver.

Du er nu klar til at bruge PGP-kryptering, når du sender emails.

PGP-programmet er lagt ned i taskbaren nederst på skærmen, hvor du har adgang til de forskellige funktioner ved tryk på venstre museknap.

Eksempel

Lad os sige du vil sende en krypteret besked til din ven.

Først starter du dit favoritmailprogram, og skriver din mail som du plejer. Så lige inden du sender det, vælger du *PGP/Current Window/ Encrypt*. En box med de nøgler som du har dukker så op, og du vælger her hvem du vil sende til. Hvis du ikke har en public key fra den du vil sende til, kan du prøve at finde den på en af de nøgleservere der findes, ved hjælp af *PGP/ PGPKeys*. Ellers må du bede din ven om at sende dig sin publickey, som du så kan importere. Når din mail er krypteret, kan du trygt sende den afsted over nettet, velvidende at det kun er indehaveren af den tilsvarende privatekey, som kan læse den.

Dekryptering

Når du modtager en PGP-krypteret email i dit emailprogram, vælger du blot PGP/Current Window/Decrypt & Verify, hvorefter du bliver bedt om at indtaste den passphrase, som du valgte dengang I lavede dit nøglesæt. Du vil så se den dekrypterede email i et særskilt vindue.

Hvis du er så heldig at bruge en af de emailklienter som er understøttet af PGP vha. plugins, bliver dit liv en del nemmere, idet du får alle PGP-funktionerne indlagt i programmet, så det at sende og modtage PGP-krypteret email, bliver en ganske enkel sag.

INTRODUKTION TIL SIKKERHED - ARTIKEL 1

Sikkerhed på Linux

af Hanne Munkholm
<hanne@aub.dk>

og Peter Toft
<pto@sslug.dk>

Denne artikel er den første i en serie på 6 artikler om sikkerhed på Linux, som kan findes på http://www.sslug.dk/artikler/Linux_sikkerhed

Introduktion

For få år siden var computersikkerhed et emne, de færreste behøvede at tænke på. Med den hastigt voksende udbredelse af Internet i dag er det et område, man ikke længere kan tillade sig at overse. Flere og flere computere kobles til Internet eller et lokalnet, og kan let blive ofre for ødelæggende indbrud, aflytning m.m. Sikkerhed er for mange et emne, de ved, at de burde tænke på, men de finder det svært at komme igang med at at lære et så komplekst område. Da sikkerhed er et meget stort område, ved man ikke rigtig, hvor man skal starte, og det virker meget svært i begyndelsen. På Internet er der mange informationer at finde, men de findes spredt rundt omkring, og det er ikke altid let at forstå, hvor de enkelte „brikker" passer ind i det store puslespil.

Vi skriver disse artikler i håb om at hjælpe andre i gang med emnet, som er både spændende og til at forstå, når man først kommer i gang. Selvom du ikke lige nu har brug for at lære om sikkerhed, kan du alligevel være interesseret i at læse videre, idet du kommer til at lære hvor meget, din Linux maskine kan på et netværk, og hvordan det kontrolleres.

Hvem er vi?

Forfatterene af artikelserien er begge interesserede Linux brugere. Vi har ikke beskæftiget os specielt med netværkssikkerhed før, men mente, at vi burde vide mere om det. Vi har sat os ind i emnet efter bedste evne i processen med at skrive disse artikler, og vi vil gerne have hjælp og rettelser fra læserne til at gøre artiklerne endnu bedre. Vi håber derfor, at eventuelle fejl er blevet opdaget og rettet før du læser dette, og at vi på trods af manglende ekspertise og erfaring på området kan beskrive de udvalgte områder korrekt.

Alle de emner, der beskrives i disse artikler, er noget vi har fra alment tilgængelige kilder: Bøger, Internet og Linuxsystemet selv. Har du kommentarer, så skriv til os begge: Hanne Munkholm <hanne@aub.dk> og Peter Toft <pto@sslug.dk>.

Oversigt over planlagte artikler

Vi har planlagt følgende artikler i serien:

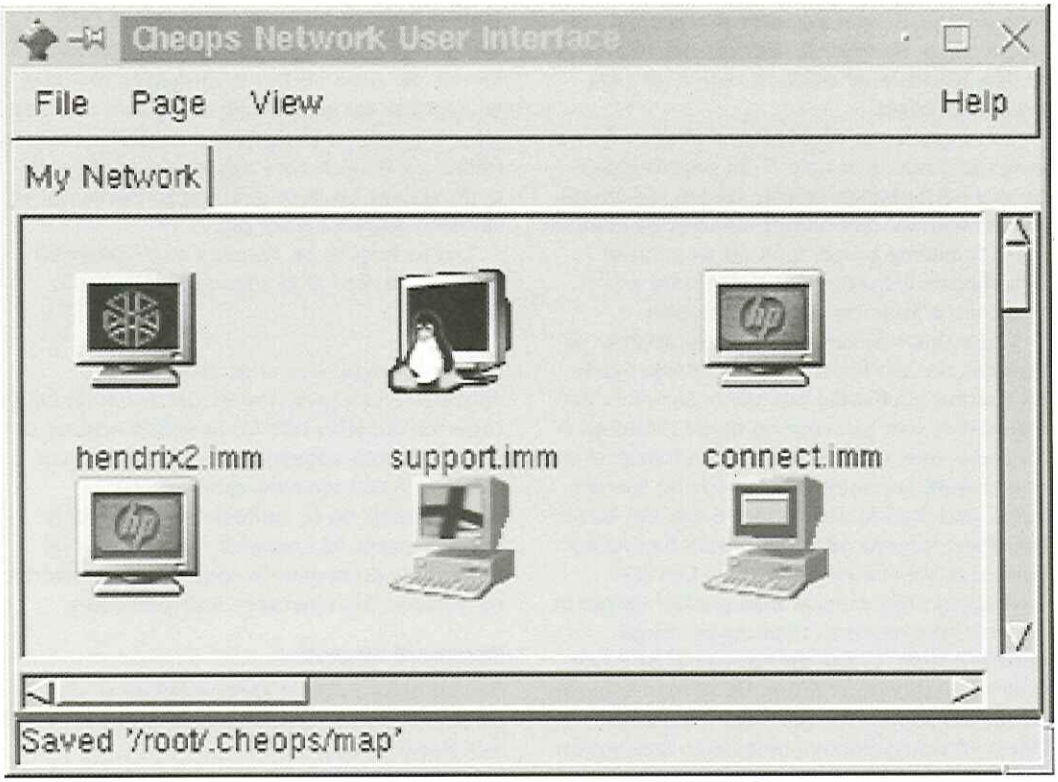
1. Introduktion til sikkerhed (denne artikel).
I denne artikel ser vi nærmere på, hvordan Linuxverdenen behandler sikkerhedsproblemer. Vi ser også på hvilke typer trusler, der findes, og nærmere på, hvor udsat dit system er for trusler imod sikkerheden.

2. Services - at slå services fra og begrænse adgang.
Hvis du har installeret en standard Linuxmaskine, kan der allerede være mange services åbne for dit netværk. Dette kan give en form for adgang til maskinen fra nettet, f.eks. SMTP. Disse udgør en potientiel risiko. På de fleste systemer er det ikke alle disse services, som behøver at være åbne.

3. Root access - hvem, hvordan og hvorfor ikke?
På Linux findes en speciel bruger, „root", som har ubegrænset adgang til hele maskinen, herunder adgang til at ødelægge alt. Vi ser på hvordan og hvornår, du skal anvende root kontoen, nemlig kun når det er nødvendigt. Vi ser desuden på programmer, der kører med root rettigheder.

4. Remote login og netværksaflytning
En Linuxmaskine er født til at kommunikere via netværk. Problemet er bare, at de fleste af de programmer, man anvender, er designet med henblik på stabilitet og ikke sikkerhed. Derfor ser vi bl.a. på problemer med telnet og ftp, og hvordan du kan installere og anvende sikre alternativer såsom ssh (secure shell).

5. Systemovervågning, læsning af log-filer
Hvordan opdager du, hvis der har været nogen inde på Linuxmaskinen og lave slemme ting bag din ryg? Vi ser på måder at kunne læse mange af Linuxsystemets log-filer effektivt, og hvordan du sikrer dig, at systemfiler ikke er ændrede.



6. Firewall

Er dit netværk koblet til Internet, bør du beskytte det med en firewall. Vi vil se på, hvad en firewall er, hvilke værktøjer du har til rådighed og hvordan firewall'en kan konfigureres.

Hvorfor er netværk usikkert?

Din maskine har ofte en del netværksservices åbne på forskellige „porte", når du har adgang til Internet. En port er ikke en fysisk port, men en logisk indgang til din maskine via netværksenheden (modem eller netværkskort). Disse „åbne porte" benyttes til at udføre netværkskommunikation, hvis maskinen tilbyder netværksservices som f.eks. ftp. Men de kan også misbruges, så uautoriserede personer kan komme ind på din computer via nettet. Dette kan ske, hvis der er fejl i den software der styrer netværksportene, eller hvis du lader dem stå helt åbne uden nogen form for adgangskontrol. Det kan også ske selvom du har adgangskontrol, hvis folk har mulighed for at opsnappe dit brugernavn og password via nettet. Ofte kan man direkte samle brugernavne og passwords op på nettet ved at bruge et „sniffer" program, som lytter til trafikken på et givent sted.

Dette er bare en forsmag på de emner, vi vil komme nærmere ind på i de kommende artikler.

Er Linux et usikkert system?

Nogen har anklaget Linux for at være et meget usikkert system, idet alle kan læse kildeteksten. Når man kan læse kildeteksten til f.eks. netværksprogrammer og se hvordan, de fungerer, er det nemt finde eventuelle fejl. Disse kan bruges til at lave angreb på Linuxmaskiner. Dette er delvis sandt! Men alligevel ikke. Vi ser på hvorfor.

For at knække sikkerheden på et UNIX system, skal man enten kende en fejl i systemopsætningen eller lede efter fejl. For en kommerciel leverandør er en fejl ofte et prestigetab, og derfor er det måske ikke alle fejl, som bliver offentligt kendt. Hvis ingen kendte de fejl, der er i de lukkede UNIX systemer, ville alt være godt. Men ofte bliver fejl i lukkede UNIX systemer opdaget og kendt. Det kan skyldes at nogen udefra opdager fejlen ved et tilfælde, eller måske leder de bevidst efter fejl - eller at nogen indefra lækker information eller taler over sig. Så ender fejlen måske på en Internethjemmeside eller som en artikel i en avis - og så har du problemet: Hvis den, der vil bryde ind, kender fejlen, og du ikke kender den og tager højde for den, kan han komme ind på dit system.

Det er nok nærmest umuligt at gardere sig imod at en sikkerhedsbrist bliver offentligt kendt.

Ud over kendte sikkerhedshuller kan den, der vil bryde ind, selv lede efter fejl. I en lukket UNIX er det langt sværere at lede efter fejl end i Linux, fordi man ikke har kildeteksten. Men en måde at finde sikkerhedsfejl på, er at prøve gamle sikkerhedshuller af på nye maskinopsætninger -

men med ændringer svarende til nye ideer. Nogle gange sker det så, at der er bid. Et system er ikke sikkert imod crackere, bare fordi kildeteksten er lukket.

Erfaring viser, at nogle af de helt store firmaer er meget ringe til at oplyse om sikkerhedsfejl - de skal helst negligeres eller skjules. Sikkerhedsbristerne findes ofte hurtigt refereret på Internet, mens firmaerne bruger lang tid på at lukke sikkerhedshullet ordentligt. I al den tid er maskinerne åbne for sikkerhedsangreb.

Linuxverdenen vender alle disse dogmer på hovedet. For det første findes al relevant kode på Internet til offentlig beskuelse. Så nok er der mennesker, som kan læse og bryde sikkerheden for andre, men Linuxverdenen er indrettet, så der er en meget stor prestige i at finde og specielt lappe sikkerhedshuller. Derfor vil folk, der finder fejl, oftest fortælle offentligt om de fundne fejl fremfor at gemme informationen. Det kan selvfølgelig også være, at man i stedet vælger at udnytte informationen til at bryde ind på nogens system. Så kan det være et af de første „ofre" der rapporterer fejlen. Da vil man fokusere på hvilken service, der gav sikkerhedshullet. Oftest vil Linuxverdenen indlede en klapjagt for at få fjernet problemet og udgive nye versioner af de berørte programmer. Det bliver en slags „trofæ" at komme først med den korrekte rettelse. Normalt er man nede på dage eller ofte timer, fra en sikkerhedsfejl er rapporteret, til den er fundet og rettet, hvilket er markant mindre end på nogen af de andre systemer.

Alt dette lyder meget rosenrødt, men hvis din Linuxmaskine har en kendt sikkerhedsbrist, og maskinen er på et usikkert netværk såsom Internet, så er der er en pris at betale. Du skal opdatere din maskine, når der er fundet sikkerhedsbrister, og den tilsvarende sikkerhedsrettelse er publiceret. Ellers har du reelt set nul sikkerhed! Alle kan jo se hvad, der er galt i din kode - det har været diskuteret på Internettet, for at man har kunnet lave rettelsen. På http://www.rootshell.com ligger der oftest anvisninger af både problemets omfang, karakter, udnyttelse og reparation.

Hvilke angreb kan jeg blive udsat for?

Der er flere forskellige typer angreb, der kan ramme din maskine. Der er forskellige metoder, en angriber kan benytte sig af, og som man kan gøre noget for at beskytte sig imod. Der er også forskel på, hvilken type adgang en angriber får til dit system, og hvor alvorlige konsekvenser et vellykket angreb har for dig.

Lad os først se på, hvordan en angriber kan bære sig ad med at få adgang til dit system.

Exploits

Det mest almindelige er at gå efter nogle netværksservice programmer, der er fundet fejl i. Disse fejl udnyttes ofte for at få fuld adgang til maskinen (root-adgang). Som tidligere nævnt skal man holde øje med annoncerede sikkerhedsfejl, og få opdateret de anfægtede programmer. Vi vil i artikel 2 - Services - at slå services fra og begrænse adgang - se på hvorfor og hvordan, du minimerer disse problemer.

Password angreb

Den klassiske måde at komme ind på et system på er at få fat i et brugernavn og password (helst root passwordet).

Packet sniffing

Man kan opsnappe brugernavne og passwords, hvis disse sendes i klar, ukrypteret form over nettet - se „man-in-the-middle angreb" herunder. Vi kommer desuden tilbage til emnet i Artikel 4: Remote login og netværksaflytning.

Brute force

Man kan knække et svagt password med rå computerkraft. Se Artikel 3 Root access - hvem, hvordan og hvorfor ikke?.

Social engineering angreb

Ofte kan en angriber slutte sig til ting ud fra sin viden om menneskelig adfærd. F.eks. at en bruger vil benytte det samme passwords til mange ting for at slippe for at huske så mange passwords. Så har man et password fra en telnet session, man har overvåget, kan det sikkert bruges til andre ting også.

Man-in-the-middle angreb

Her er tale om at angriberen befinder sig et sted på netværket, hvor dine data-pakker kommer forbi. F.eks. hos din Internetudbyder eller på dit lokalnetværk. Eller i princippet et vilkårligt sted på Internet, hvor dine pakker kommer forbi.

Packet sniffing

Det mest almindelige man-in-the-middle angreb er, at angriberen kigger på dine data-pakker for at opsnappe information. Det kan f.eks.være brugernavne og passwords, som sendes i klar tekst over nettet, eller dine firmahemmeligheder, hvis du kunne finde på at sende dem ukrypteret afsted.

Session hijacking

En anden type man-in-the-middle angreb er, at en angriber går ind og overtager en igangværende session f.eks. en telnet session. Dette er i praksis meget vanskeligt på Internet, da det enten kræver at target-maskinen bruger forudsigelige tcp sekvens-numre, eller at man kan aflytte trafikken. Det første er ikke muligt i Linux, og hvis man kan det andet, er det meget nemmere blot at sniffe brugernavn og password.

IP spoofing

IP Spoofing går ud på at få systemet til at tro, at angriberens computer er en autoriseret computer, der har lovlig adgang. Dvs. at angriberens computer udgiver sig for at være en autoriseret host ved at bruge dennes IP-adresse. Dette kan bruges til at indsætte angriberens data i en datastrøm. Hvis angriberen ønsker at opnå tovejskommunikation, hvor han modtager de pakker, der er tiltænkt den, han udgiver sig for, er det sværere. Så skal han ind og ændre routing tabellerne.

Trojanske heste

„Trojanske heste" er programmer, der indeholder skjult funktionalitet. Et velkendt program på dit system kan se helt uskyldigt ud og udføre sin normale funktion. Programmet kan imidlertid være modificeret, så det ud over sine normale opgaver f.eks. mailer navne og passwords til en fast modtager eller lader ukendte personer logge ind på maskinen uden, at dette skrives i systemets logfiler. „Trojansk heste" kan være programmer efterladt af en angriber, der har været inde på dit system. De kan skjule hans spor og lette hans adgang næste gang (backdoors). Det kan imidlertid også være programmer, du selv har download'ed og installeret. Du tror, du installerer et almindeligt program, men i virkeligheden er det en modificeret udgave, du har fået fat i. Heldigvis medfører traditionen med Open Source programmer, at vi har adgang til kildeteksten, og at man i praksis ikke kan skjule disse problemer for os. Downloader du binære programmer (såsom RPM pakker), så bør dette kun ske fra betroede steder, hvor du kan regne med at der bliver holdt styr på sikkerheden - men det er altid en risiko, du må løbe. Ydermere findes der PGP-nøglesignaturer i alle RPM-pakker, som man kan bruge til at checke, hvem der har lavet den enkelte pakke. Heldigvis er problemerne i Linux verdenen meget små i forhold til det niveau, som Windows verdenen er udsat for med virus i programmer og selv i Word dokumenter. Et velkendt eksempel på en trojansk hest fra i Windows verdenen er „Back orifice". Hvis det først er installeret, giver det folk udefra fuld kontrol over den inficerede maskine via Internet.

Vi har nu set på forskellige metoder, en angriber kan bruge til at få adgang til dit system. Men hvad kan han bruge det til? Lad os dele angrebene op efter resultatet - hvad opnår vedkommende, og hvor farligt er det for dig.

Læseadgang

Angriberen kan stjæle (kopiere) dine data. Dette er alvorligt, hvis du har hemmelige data, som kan udnyttes af andre på en måde, der skader dig. Læseadgang kan f.eks. opnås ved packet sniffing - hvis der er værdifuld information i pakkerne. Man kan beskytte sig ved at kryptere sine data. Læseadgang kan også opnås ved IP spoofing, hvis angriberen f.eks. giver din maskine besked om at videresende en vigtig email til ham. Endelig kan det opnås, hvis angriberen opnår login på dit system f.eks. ved at have skaffet sig et brugernavn og tilhørende password. Har man login på maskinen, kan man naturligvis også skrive men kun i de filer, der er adgang til for den bruger, man er logget ind som.

Skriveadgang

Ud over at dine data kan blive stjålet, kan du risikere, at de er ændret, og at dit system er modificeret. Dette er meget alvorligt. Dit system er kompromitteret. Skriveadgang kan opnås, hvis angriberen opnår login på systemet. Han kan modificere de data, som det anvendte brugernavn har adgang til. Hvis han er inde som root, har han fuld adgang til at ødelægge eller modificere dit system. Root adgang kan ud over at opsnappe eller knække root passwordet opnås ved at udnytte et sikkerhedshul i en netværksservice f.eks. sendmail. En angriber kan også opnå skriveadgang til dit system ved IP-spoofing - hvis man kan ændre indholdet af pakker, der bliver sendt over nettet, uden at modtageren opdager det, så har man effektivt forfalsket data.

Det kunne også være kommandoer til systemet. Har en angriber først haft skriveadgang til dit system, skal du være meget forsigtig. Du ved ikke hvilke data, der er ændret - måske er de programmer, du kontrollerer dit system med, selv modificeret, og du kan ikke regne med dem længere. Du ved måske ikke med sikkerhed, hvornår han første gang har været inde, og dine backups kan være inficeret et stykke tid tilbage. Vi kommer tilbage til, hvad du skal gøre for at opdage et indbrud i Artikel 5: Systemovervågning, læsning af log-filer

Har en angriber lokket dig til at installere en trojansk hest, er det også en slags skriveadgang - dit system er modificeret.

Denial of Service angreb

Denial of Service (DoS) angreb har til formål at få din maskine til at holde op med at gøre det, den er sat til. Dette er knap så alvorligt som et reelt indbrud på systemet, men kan alligevel godt koste meget tid og mange penge. Eksempler på DoS angreb er Pentium F00F fejlen, ping of death eller teardrop, som får maskinen til at låse. Disse fejl er rettet i nyere Linux systemer. Ved SYN flooding og Ping flooding udsættes maskinen for en voldsom belastning fra en eller flere angribere med at svare på netværksforespørglser, og det er ikke muligt at bruge andre netværksservices på grund af overbelastning. Ved smurfing er det netværket, der overbelastes. Disse problemer kan der dæmmes op for ved fornuftig router-konfiguration. Der er også angreb, hvor der uploades meget store mængder data til en anonym ftp konto, hvor formålet er at få diske til at løbe fulde. Disse problemer kan der dæmmes op for med disk kvoter og/eller smart partitionering (eller at upload af filer disables).

Fra den mere muntre ende kan vi lige vise lidt om DoS angreb fra User Friendly strippen den 7/8 99.

Har mit system sikkerhedsproblemer?

Nu skal vi se på, hvor meget du udsætter din maskine for, når du tilslutter den til Internet. Vi tager udgangspunkt i en Linux maskine, som har en netværksopkobling enten via modem eller fast forbindelse. Det er reelt ikke så vigtigt, at det er en Linuxmaskine - alle systemer med netværk har samme karakteristiske træk.

Lad os inddele verden efter:

„On and off" : Opkobling sker med modem og f.eks. PPP. Der hentes emails og surfes minimalt på Internet.

„Seriøs surfing" : Opkobling sker med modem og f.eks. PPP. Der hentes emails jævnligt, og der surfes en del. Denne situation kan også gælde for en maskine, som via automatiske services laver internetopkobling for et helt lokalnet. Til Linux er det ofte „diald", som bruges til dette.

„Fast opkobling" : Maskinen har fast opkobling til Internet via ethernet, ISDN eller anden forbindelse.

On and off

Du har ikke så meget at frygte, selvom du måske ikke har styr på din sikkerhed på maskinen.

Når du laver en modem opkobling til Internet, får du tildelt en IP-adresse, dvs. en adresse, som alle kan tilgå din maskine på. Men den adresse er forskellig fra gang til gang når du laver opkobling. Derfor bliver det i praksis umuligt at checke din maskines sikkerhedshuller fra en anden maskine, før du igen har lukket forbindelsen. Der er dog oplagt, at den risiko, du løber, svarer nøje til den tid du er koblet på Internet.

Seriøs surfing

Du er tilkoblet Internet i længere tid ad gangen men stadig med forskellig IP-adresse hver gang, så du er ikke helt nem at finde. Men i modsætning til „On and off" brugeren er du på så lang tid, at der godt kan laves skanning på din maskine. Hvis der findes en usikker service, kan den måske give oplysninger om svagheder i dit system, og dermed kan din netværkssikkerhed rammes. Du bør tænke på hvilke åbninger, der er i dit system. Du bør lære noget om grundlæggende netværkssikkerhed. Læs f.eks. resten af artiklerne i denne serie.

Fast opkobling

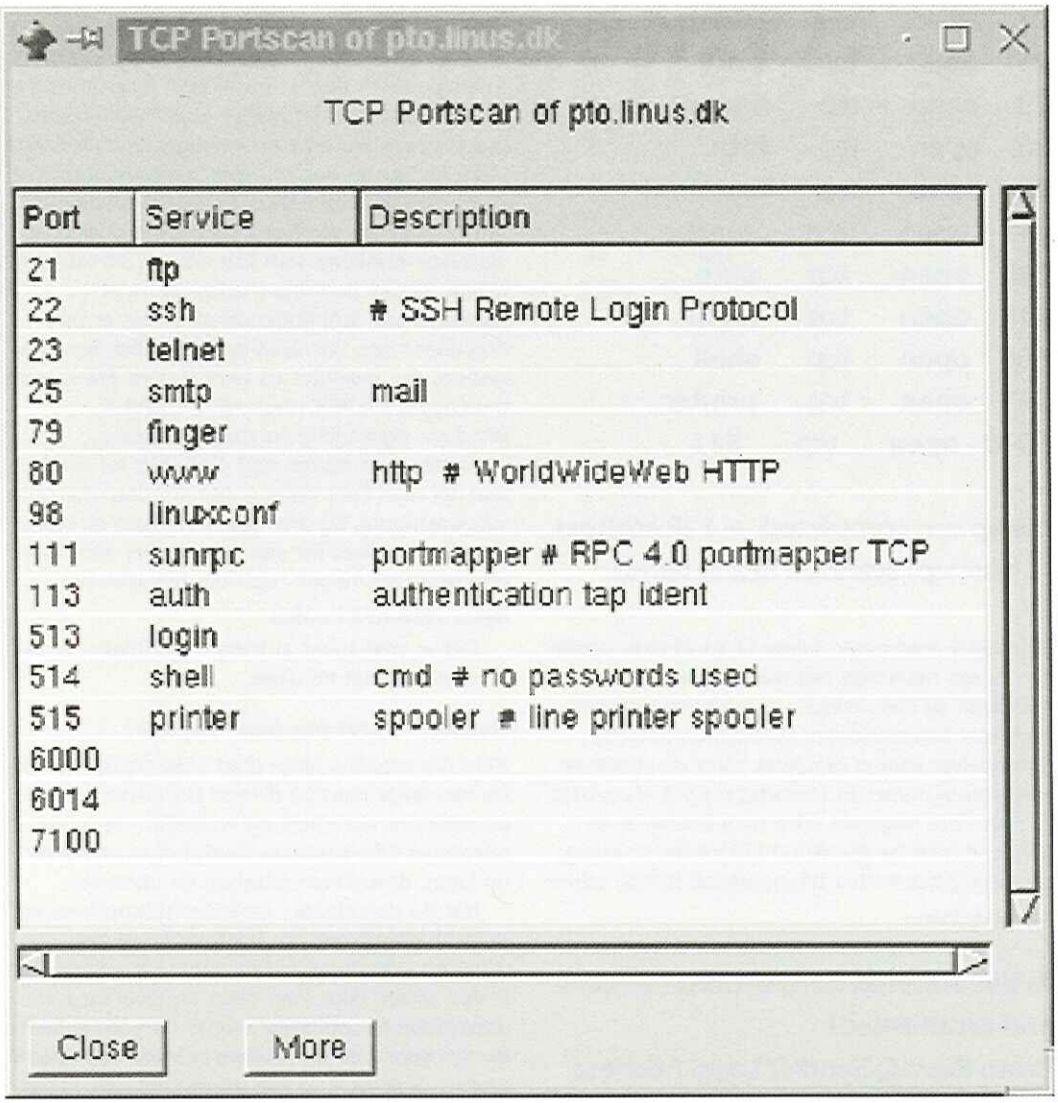
Du kan skannes fra en enhver maskine på Internet medmindre der er firewalls eller såkaldte proxy servere imellem. Du kan ikke overvåge alt 24 timer i døgnet. Maskinen efterlades. Du må checke dine log filer! Slå overflødige netværksservices fra og begræns adgangen til dem, der er tilbage. Du bør lære noget om sikkerhed. Læs f.eks. som en start de kommende artikler i denne serie. På Internet er der også masser af information, og der findes gode bøger om emnet.

Crackere gider ikke ramme min maskine

Lad os antage, at din maskine har direkte adgang til internet uden firewall eller anden beskyttelse. Vi vil nu se på, hvorfor din maskine kan være udsat, og hvordan andre finder ud af, at du har en maskine på nettet. At det netop er din maskine, som er udset til et crackerangreb, kan skyldes mange ting: Tilfældigheder, at du anses for at ligge inde med interessante data, eller at du ikke har vedligeholdt din Linux maskine og fået lukket de kendte sikkerhedshuller.

En angriber har flere måder at finde din maskine på. En er f.eks. at studere headerne i dine emails. En anden er at hente listen over hostnavnene i dit domæne vha. DNS (navneservere). En mere direkte måde er at bruge ping.

En cracker kan derefter spørge din maskine, hvilke services den tilbyder, og måske finde et sikkerhedshul. Som eksempel kan vi tage ssh, som tilbydes på port 22. Med telnet kan man logge ind på port 22 og få versionsnummeret på ssh. I det følgende eksempel finder vi ud af, at



det er ssh version 1.2.27, der kører. Kan crackeren f.eks. på Internet finde en beskrivelse af en sikkerhedsfejl i den version af ssh, kan han udnytte dette til at angribe dit system med.

[robin@sherwood robin]$ telnet locksley 22
Trying 172.17.0.3...
Connected to locksley
Escape character is '^]'.
SSH-1.5-1.2.27

Normalt er det nødvendigt, at din maskine har nogle af de mange netværksservices kørende, da de bruges til at kommunikere med andre maskiner via netværk. Ofte kan de fleste af dem dog slås fra, se Artikel 2: Netværkssikkerhed - Services.

I stedet for, at en cracker manuelt skal gennemse alle dine porte for mulige huller, kan han gøre det nemmere og meget hurtigere ved at installere programmer såsom nmap. Nmap kan hentes på http://www.insecure.org/nmap. Med nmap kan man dels se hvilke maskiner, der er i live, men også hvilke porte, der er åbne. Nedenstående eksempel viser, at maskinen „locksley" har (alt for) mange porte åbne.

[robin@sherwood robin]$ nmap locksley
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on locksley.herne.dk (172.17.0.3):

Port	State	Protocol	Service
21	open	tcp	ftp
22	open	tcp	ssh

```
23    open    tcp    telnet
25    open    tcp    smtp
79    open    tcp    finger
80    open    tcp    http
98    open    tcp    linuxconf
111   open    tcp    sunrpc
113   open    tcp    auth
513   open    tcp    login
514   open    tcp    shell
515   open    tcp    printer
6000  open    tcp    X11

Nmap run completed — 1 IP address (1 host up) scanned in 2 seconds
```

Eksemplet med nmap svarer til, hvad man udefra kan se om maskinen. Har man adgang til maskinen, så kan „netstat -a" også være interessant, idet kommandoen viser alle de netværksforbindelser, som er etableret, samt de ventende serverprogrammer. Et forkortet output af „netstat -a" kan være følgende, hvor man kan se, at en telnet session fra sherwood til locksley er igang, og serverprogrammer ssh, sendmail (smtp), telnet og ftp er klar.

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 locksley.herne.dk:telnet sherwood.herne.dk:1074  ESTABLISHED
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
```

Man kan også have interesse i at bruge det grafiske program cheops, som findes på ftp://ftp.marko.net/pub/cheops/RPMS/. Programmet er skrevet sådan, at det grafisk viser hvilke maskiner, som er i live, og evt. overvåger, at de forbliver i live. Cheops er nok primært beregnet til at give systemadministratoren et hurtigt overblik over netværket, men det kan også bruges til at udse sig svage maskiner, som kan crackes. På følgende billede er vist, hvordan cheops ud fra et domænenavn selv finder ud af, at der er seks maskiner i live. Det vises grafisk hvilket operativsystem, der anvendes på hver af dem. Fra venstre mod højre: SGI, IRIX, Linux, HP/UX, HP/UX, Windows og endelig en speciel maskine.

Flytter man musen ned på ikonet for maskinen, får man flere oplysninger om den ofte også versionsnumre, og man kan yderligere direkte skanne maskinen for alle oplysninger. Man kan ofte se alt for meget - især når folk ikke har deres sikkerhed i orden.

Det er altså nemt at trække informationer ud af en ubeskyttet maskine.

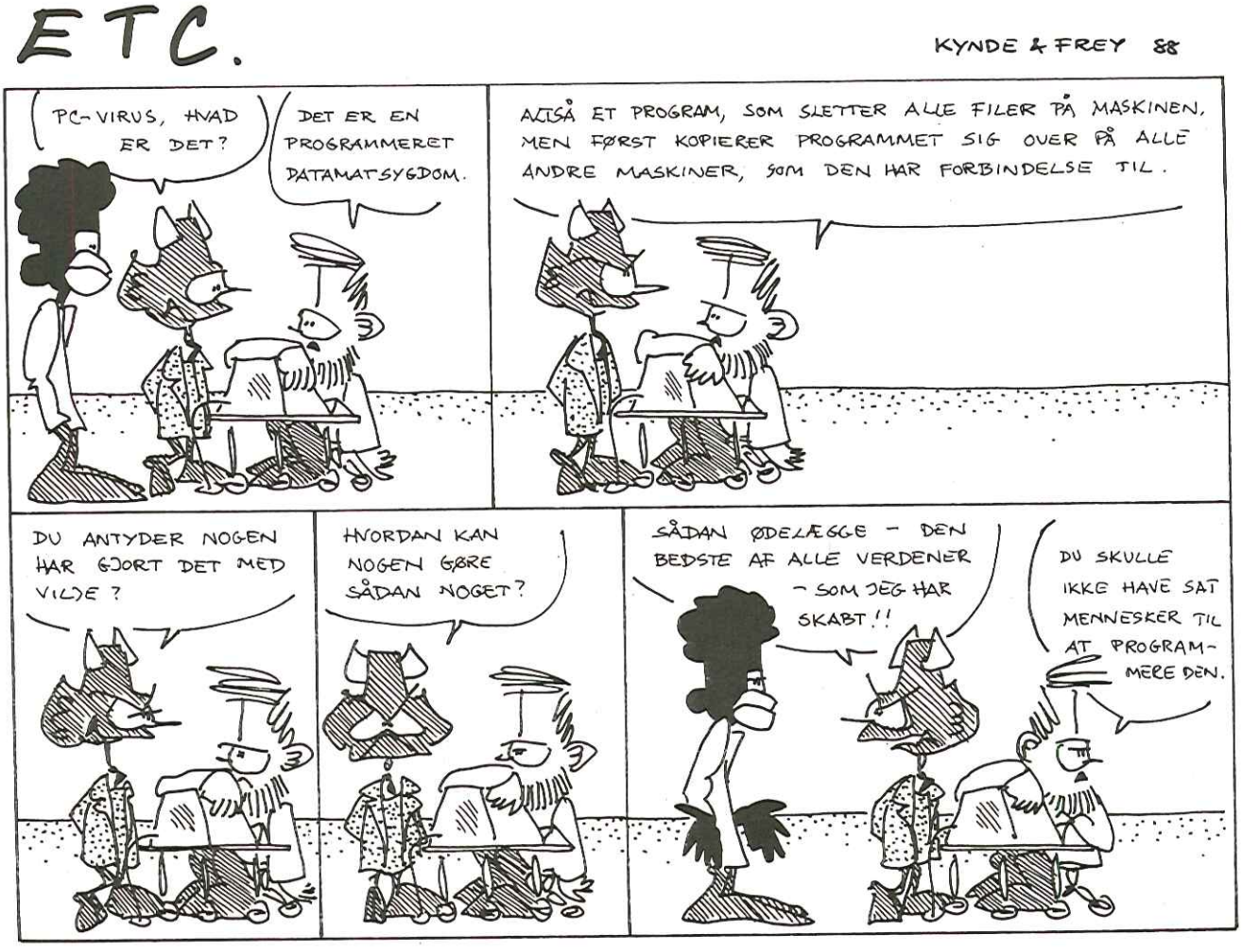
Hvordan sikrer jeg min maskine?

Hold din maskine ajour med sikkerhedsrettelser. Du kan følge med på diverse postlister/nyhedsgrupper om sikkerhed, og websider - se under referencer. Ofte kan man hurtigt efter en fejl er opdaget, downloade rettelsen fra Internet.

Når du downloader en sikkerhedsopdatering, så tænk lige på om den kommer fra et sted, du stoler på - den kunne i princippet være falsk. Det er den sikkert ikke, men nøjes alligevel med at downloade fra „officielle" steder. Den første lektie, du skal lære, hvis du vil have et sikkert computer system, er at være en lille smule paranoid. :-) Der er intet på nettet, der er helt sikkert.

Referencer:

Gode steder at starte
Linux Administrator's Security Guide (LASG) by Kurt Seifried. Denne bog er guld værd - og kan findes på http://securityportal.com/lasg/.
Linux Security HOWTO - http://sunsite.auc.dk/ldp/HOWTO/Security-HOWTO.html
Annonceringer af fejl i flere af de kendte Linux distributioner:
Debian http://www.debian.org/security/ Lister sikkerhedsrelaterede fejl i Debian.
SuSE http://www.suse.de/security/index.html har liste over sikkerhedsfejl i SuSE.
Red Hat http://www.redhat.com/corp/support/errata/index.html Generel entry til fejllisterne. Du bør nok også se på den nyeste (pt.) http://www.redhat.com/corp/support/errata/rh60-errata-general.html
Steder som ellers bør eller kan følges
Bugtraq http://www.securityfocus.com bør du følge med på for at læse om de nyeste exploits.
Root Shell http://www.rootshell.com har alt indenfor diskussion af sikkerhed.
Linux Today http://linuxtoday.com bringer også sikkerhedsbrister frem sammen med andre nyheder.
http://www.securityportal.com/ er et andet interessant sted, som interesserer sig for sikkerhed.
Linux Security WWW - http://www.aoy.net/Linux/Security, med mange Linux-relaterede sikkerheds annonceringer, FAQ og links.
Linux Security Home Page http://www.ecst.csuchico.edu/~jtmurphy/
Reptile's Linux Security Page - http://www.reptile.net/linux
Infilsec Vulnerability Engine - http://www.infilsec.com/vulnerabilities/ - generelt om sikkerhed.
Munitions - http://munitions.polkaroo.net/ - stor samling af viden og programmer om kryptering af data og netværkstraffik til Linux.



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

Udgiver:
DKUUG
Fruebjergvej 3,
2100 København Ø.
Tlf: 39 17 99 44
Fax: 39 20 89 48
email: sek@dkuug.dk
Sekretariatet er åbent:
Mandag-fredag
kl. 9.00-17.00

Direktør:
Bo Folkmann

Redaktion:
Hans Arne Niclasen
(ansvarshavende)
Gitte D'Arcy
Søren Oskar Jensen
Jacob Bække
Peter Holm
Bo Folkmann

Tryk:
Palino Print

Annoncer:
Kontakt DKUUGs sekretariat

Oplag:
1500 eksemplarer

Artikler m.v. i DKUUG-Nyt er ikke nødvendigvis i overensstemmelse med redaktionens eller DKUUGs bestyrelses synspunkter. Eftertryk i uddrag med kildeangivelse er tilladt.

Deadline:
Deadline for næste nummer nr. 118 er fredag d. 8. oktober 1999

Medlem af Dansk Fagpresse

DKUUG-Nyt
ISSN 1395-1440

Aktivitetskalender

Oktober:

11. Linux@work
21. Stiftende møde i SILD
26. Klub København: PHP

November:

25. Generalforsamling
30. Klub København: Python (+ Zope?)

Se www.dkuug.dk for nærmere oplysninger

Afholdte aktiviteter

Januar:

24. Klub Fyn (FLUG) - Eric Raymond-foredrag
24. Klub København - Eric Raymond-foredrag
26. Linux-seminar

Februar:

04. Klub Odense - Installation af Linux
09-12. Konference - Nordic EurOpen/Usenix
18. Klub Odense: Opsætning after installation
23. Klub København: DNS & BIND
25. XML-seminar

Marts:

04. Klub Odense: Shellscripts og CVS
09. Windows Refund Day
17. Klub København (ekstra): Harddiske m. Thomas Gemal, Quantum Corp.
18. Klub Odense: Linux som server
21. Klub Århus: European Linux Yearbook (ELY)
30. Klub København: Intranet

April:

01. Klub Odense: Opsætning af serverpakker og „The Dotfile Generator"
08. Seminar: Linux - et reelt alternativ
09. DNS & sikkerhed m . Cricket Liu
15. Klub Odense: Emacs
20. IP Telefoni deminar
27. Klub København: Emacs
27. Klub Odense: Perl
30-02. Konference: Open Networks - ON99

Maj:

04. Gnome m. Miguel de Icaza
06. Kerne opsætning og X11 m. Jesper Pedersen (jews)
11. Staroffice m. Roar Hylleberg

Juni:

01. The Dotfile Generator m. Jesper Pedersen - (blackie)
03. Klub København: KDE m. Kalle Dahlheimer
05. Klub Odense: KDE m. Kalle Dahlheimer
08. EKSTRA: Klub København: DNS & sikkerhed med Cricket Liu
09-11. Netværk Telecom 99 i Bella Centret
10. Klub Odense: TDGs procmail modul m. Jesper Pedersen (blackie)
14. Seminar: DSDM-blik på en verden med objekter og komponenter m. Paul Turner
15. XML-seminarer
15-18. Seminar: DSDM Practitioner og projektlederkursus
21.-25. Konference: Europæisk Oracle Bruger Gruppe i Bella Centret
22. Klub Århus: Emacs med Jesper Pedersen
25. Klub Odense: Cd brænding m. Jesper Pedersen (jews)

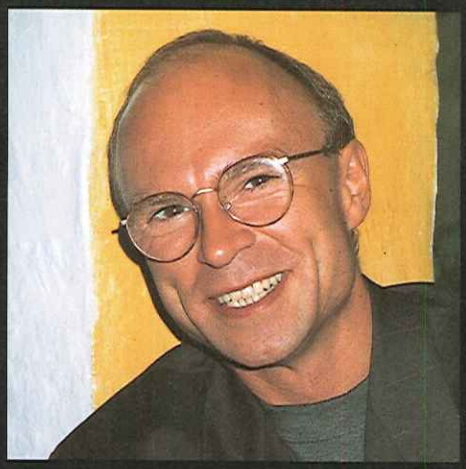
August:

05. Hvad sker der ved Linux boot m. Jesper Pedersen - (blackie)
31. Klub Kbenhavn: Beos m. Claus Nyhus Christensen

September:

12. Linux Demo Day
20. DSDM & Internetudvikling
21.-22. Workflow management & elektronisk dokumenthåndtering
27.-28. Intranet ,99
28. XML-seminar
29. Netware Perspective Conference 99

SuperUsers a/s
Karlebogaard · Karlebovej 91 · DK-3400 Hillerød
Tel.: +45 48 28 07 06 · Fax: +45 48 28 07 05
Giro 458-2764 · E-mail: super@superusers.dk
URL http://www.superusers.dk



Brian Eberhardt, Direktør

SuperUsers a/s

SuperUsers a/s, en 100% dansk virksomhed med ca. 35 medarbejdere, har mange års erfaring inden for åbne netværk, operativsystemer og programmeringssprog:

- UNIX, Windows NT/ 98/CE, NetWare
- Internet/Intranet baseret på TCP/IP
- C/C++ /Java/Perl/ActiveX/HTML/CGI
- ORACLE og andre åbne databaser

SuperUsers a/s leverer viden og løsninger i form af undervisning og konsulentydelser inden for systemnære områder:

- System Drift
- System Support
- System Management
- System Integration
- System Udvikling

Her ses SuperUsers anno 1999 i rokoko stemning på gamle Karlebogaard.

Kurser

Åbne kurser: SuperUsers a/s afholder løbende ca. 115 forskellige kurser inden for internet, åbne netværk, operativsystemer og programmeringssprog.

Specialkurser: Derudover tilbyder vi at afholde kurser tilpasset efter kundens individuelle ønsker. Ved at plukke dele af eksisterende kurser og sammensætte disse, kan næsten ethvert behov opfyldes.

Kursusforløb: Vi hjælper gerne med at vurdere og sammensætte flere kurser, således at der opnås et sammenhængende forløb.

SuperUsers a/s er:

- Sylvan Prometric Testcenter og tilbyder/afholder tests, som fører frem til følgende certificeringer:
  Microsoft: MCP, MCSE og MSCD
  Novell: CNA, CNE og Master CNE.
- Microsoft Certified Technical Education Center (CTEC)
- Novell Authorized Education Center (NAEC).

Konsulentydelser

SuperUsers a/s har konsulenter indenfor:

- Drift: Support og konfiguration
- Udvikling: Analyse, design, programmering og test

Faste opgaver: Konsulenter til udførelse og styring af drift i større installationer.

Tilkald: Et af specialerne er udrykning med sekunders varsel til hasteopgaver - ofte opgaver, hvor andre har givet op.

Telefonsupport: Endelig tilbyder vi pakkeløsninger inden for "online support".