DKUUG

Vejen til viden om Åbne Systemer og Internet

nyt

120/februar 2000

Nyt forum for kollegier og boligforeninger

og nyt om millionkrav for piratkopiering

Arrangementer i DKUUG

Det er sket i foreningen siden sidst

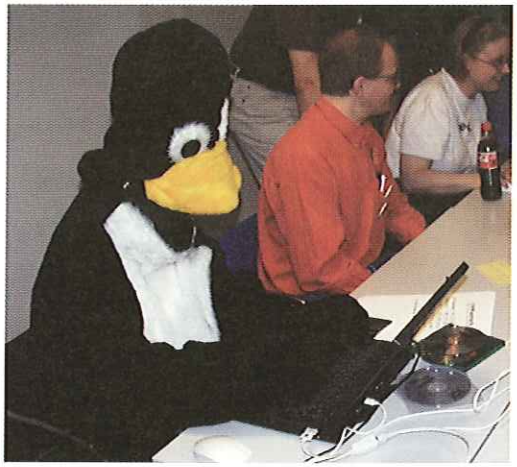
Linuxforum 2000

Se programmet for den årlige Linux/FreeBSD konference

Generalforsamling i DKUUG

Dette skete på den ordinære generalforsamling

Indhold



Tux på arbejde under ON99 - nu skal Tux snart på arbejde igen, denne gang til Linuxforum 2000

Leder

Hej igen. Det er jo et par måneder siden sidste nummer af DKUUG-nyt, og i mellemtiden er det blevet år 2000 (jeg skal nok vare mig for at sige et nyt årtusinde – det kom jeg til at skrive i en mail og modtog 30 sekunder senere en berigtigelse). Og vi overlevede. Der skete ikke noget. Nada. Ikke så meget som en kaffemaskine, der doserede forkert eller et vækkeur, der ikke ringede (nå jo, det kan i øvrigt godt være – jeg hørte i hvert fald ikke mit den 1. januar).

Så hvad siger omverdenen nu? Var det hysteri at bruge så mange penge på år-2000 problemet? Eller lykkedes arbejdet til UG med kryds og slange? Jeg tror på det sidste, for der kom jo trods alt rapporter om år-2000 svigt rundt omkring (nyfødte, der blev hundrede år gamle, en 106-årig, der blev indkaldt til første skoledag o.s.v.). Der var en alvorlig trussel, som det kun med en målrettet indsats lykkedes at afværge. I dette tilfælde var det en fordel, at år-2000 problemet kun gik ud over veludviklede lande med en infrastruktur, hvor det kunne lade sig gøre at lave en organiseret indsats.

Så nu er det tilbage til "business as usual" – og det er også spændende nok (selvom der stadig skal holdes øje med kritiske datoer). Nu er et årsskifte jo ofte en tid for at se tilbage – og frem – men det er svært at forestille sig, hvordan udviklingen indenfor computerbranchen vil blive i de kommende år. Kunne man for fem år siden forestille sig, hvor meget Internettet betyder for vores hverdag? Eller hvor meget kommunikation, der foregår via e-mail i vore dage? På det allerseneste er Internetfirmaerne begyndt at opkøbe film-, tv- og pladeselskaber og sammen med udviklingen af hurtigere kommunikationslinier vil det formodentlig accelerere udviklingen henimod en sammensmeltning af computer, TV, telefon, køleskab o.s.v. – noget man for ganske få år siden kaldte fremtidsmusik. Det er en spændende tid, vi lever i.

Med venlig hilsen
Hans Arne Niclasen.

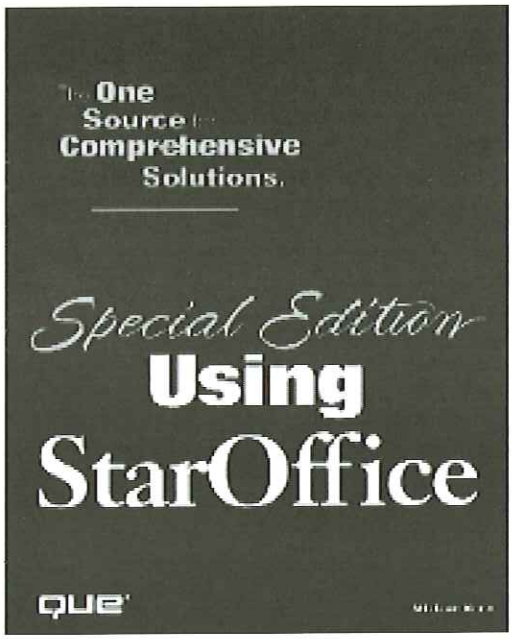
Nye bøger i DKUUG

Vi præsenterer nogle af de nye bøger, du kan købe i DKUUG – som sædvanlig med rabat.

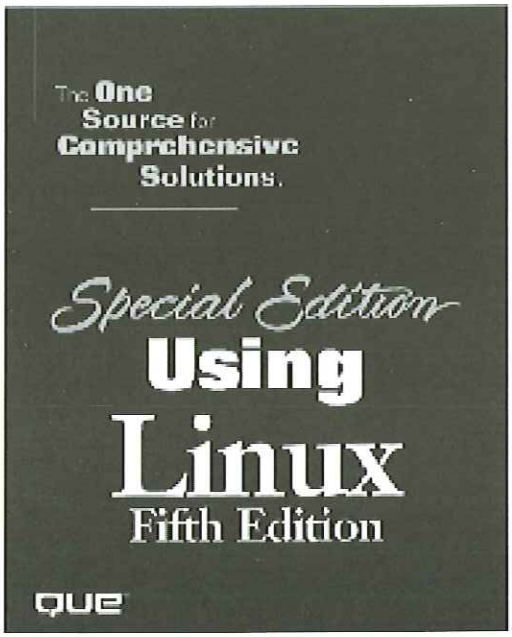
Som en service til medlemmerne tilbyder DKUUG hurtig levering af alle bøger - tekniske som ikke-tekniske, danske som engelske - med 15% rabat.

Har du set dig lun på en bog, så send en mail til boger@dkuug.dk med ISBN-nummer og titel og du vil modtage bogen to til tre dage efter. DKUUG har også bogudstilling i forbindelse med arrangementer og på kontoret i Symbions forhal, Fruebjergvej 3, 2100 København Ø., så kig forbi og se, hvad der er kommet af nyheder. Her kan du se tre af de senest ankomne bøger:

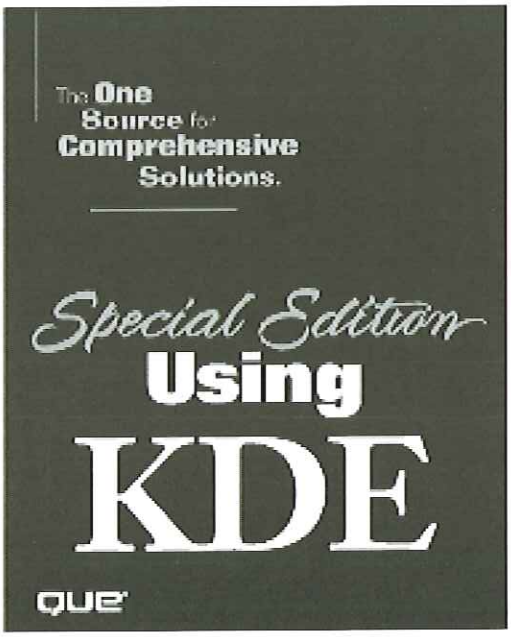
Denne gang er alle bøger fra den populære Special Edition-serie fra forlaget Que:



Special Edition Using StarOffice af Michael Koch, Sarah Murray & Werner Roth. Paperback, 1519 sider. Grundig gennemgang af alle funktioner i StarOffice 5.1. Vejl. udsalgspris kr. 400 -, **pris i DKUUG kr. 360** – (inkl. moms). ISBN 0-7897-1993-2.



Special Edition Using Linux: Fifth Edition af Jack Tackett Jr. & Steven Burnett. Paperback, 917 sider. Meget omfattende guide til Linux med tre CD-ROMs: Caldera OpenLinux 2.3, Red Hat Linux 6.0 og Debian GNU/Linux 2.1. Vejl. udsalgpris kr. 500-, **pris i DKUUG kr. 450-** (inkl. moms). ISBN 0-7897-2180-5



Special Edition Using KDE af Nicholas Wells. Paperback, 857 sider. Med KDE CD-ROM. Gennemgang for den avancerede Linux-bruger, der vil til bunds i KDE. Vejl. udsalgspris: kr. 400-, **pris i DKUUG kr. 360** – (inkl. moms). ISBN 0-7897-2214-3

Millionkrav mod kollegier – måske

Bergsøe Kollegiet

Fire brancheforeninger overvejer millionkrav mod kollegier.

Man kan i øjeblikket nok ikke sige "kollegie" uden at tænke på det erstatningskrav på 57 millioner, der tilsyneladende er undervejs. Brancheforeningerne Multimedieforeningen, BSA (softwarebranchen), Danske Videogram Distributører og IFPI (pladebranchen) har annonceret, at de vil sagsøge fire kollegier for piratkopiering af computerprogrammer, film og musik. Brancheforeningerne vil i første omgang gå efter DTU-kollegierne Kampsax-kollegiet, Professor Ostenfeld Kollegiet, Bergsøe Kollegiet og P.O. Pedersen.

Brancheforeningerne bygger sagen på observationen af, at der bliver kopieret "kolossale" datamængder på kollegierne, hvilket er blevet indberettet af anonyme "konsulenter". Det lyder måske umiddelbart lidt tyndt, og der er da heller ikke tale om en officiel politianmeldelse endnu – snarere en trussel for at få kollegierne i dialog. Brancheforeningerne overvejer også at indlede civile retssager mod enkelte beboere.

Hvad foregår der?

DKUUG-Nyt har bedt forskellige personer med tilknytning til kollegierne udtale sig om sagen:

Jakob Østergaard, medlem af net-gruppen på Prof. Ostenfeld Kollegiet: "IFPI & venner har gennem længere tid kørt skræmmekampagne i medierne mht. piratkopiering af musik i MP3 format. Det

virker på mig som om de er vågnet op og har set at folk ikke køber alle deres CD'er i forretningerne længere, og det skal nu stoppes. Fair nok, de skal jo også tjene deres penge.

Det er et problem for IFPI at man i denne verden med internet (og ytringsfrihed) ikke med loven i hånden kan slå ned på en enkelt person eller virksomhed, og få alle eventuelle ulovligheder bragt til ophør.

Hvad gør man så ? Jo, man skaber så meget postyr som overhovedet muligt, ved at skaffe sig sendetid i TV-nyhederne, og komme med indlæg til aviser m.v. Disse indlæg indeholder IKKE beviser mod noget som helst, men de er skrevet så tilpas vagt, at de insinuerer - for den udenforstående — at der foregår organiseret kriminalitet i meget stor stil på omtalte netværk.

Det eneste IFPI kan gøre i denne sag er at forsøge at insinuere så meget som overhovedet muligt - på en måde så der ikke er for mange der sagsøger dem af den grund - og komme i medierne så meget som muligt. Med andre ord, at skræmme så mange som muligt.

Pas RIGTIGT godt på med hvad der bliver skrevet, hvis der bliver skrevet noget om holdningen til denne sag. Specielt fordi der egentligt ikke er nogen sag, og fordi IFPI (der pt. arbejder på en måde der er på kanten af hvad der virker rimeligt) er de eneste, der tjener noget på omtalen af den fantasi.

Der er INGEN afgørelse i sagen, og det er ikke engang klart (officielt) hvem der bliver anklaget. Læser man i medierne vil man tro at kollegierne bliver anklaget, men læg mærke til at der ikke står noget BESTEMT om det. "

Det er klart at det er i IFPI's interesse at der bliver henvist til sagen som om den eksisterede. Lad være. Hvis problemet med IFPI og kollegienetværk skal nævnes så omtal det med *OMHU*.

Omtal sagen som det den er: Ikke eksisterende. Indtil IFPI enten trækker i land, eller kommer med et konkret søgsmål."

Jacob vil gerne understrege, at han taler helt på egne vegne i denne sag.

Henrik Kressner, EDB-konsulent om piratkopiering på kollegier: "Min holdning er helt klar, det er ulovligt, det er at underminere sin egen fremtid, (de fleste af dem jeg møder er programmører, men problemet er langt mere vidtrækkende) og det er dumt. Derudover er det nemt at knalde folk der gør det. Den præken får alle der møder mig. Jeg tæsker det faktisk ind i hovedet på dem, til de forstår det."

Kenneth Geisshirt, EDB-konsulent: "Mht. piratkopiering er min holdning klar: Det gør man ikke. Jeg bruger ikke kun Open Source forbi det er bedre, jeg gør det også for at slippe for pirater."

DKUUGs holdning

DKUUGs holdning til piratkopiering er helt klar: Det er noget skidt, og det skal stoppes. Fra mange sider har vi fået bekræftet, at der foregår/

Henrik Kresser, EDB-konsulent

har foregået organiseret piratkopiering på mange kollegier – en enkelt kilde påstår, at hans kollegium ligger inde med et diskotek af MP3-titler, der overgår Danmarks Radios. Vi har også fået at vide, at der på flere kollegier er en "piratmafia", der konstant flytter rundt på sine servere. Tilsyneladende nærmer mafiaens aktiviteter sig det kriminelle og inkluderer trusler mod kollegianere, der er kritiske overfor den organiserede piratkopiering. Man kan synes, hvad man vil om den antikverede lov, der forbyder al digital kopiering, men det er ikke desto mindre loven. DKUUG tager kraftigt afstand fra enhver form for piratkopiering – og at den er organiseret, gør kun sagen værre.

Det er så en anden sag, at den aktuelle sag ikke er ret konkret – og indtil videre er den altså slet ikke anlagt. Det er klart, at man på de berørte kollegier gerne vil have lov til at forsvare sig mod eventuelle anklager og have at vide, hvem der bliver anklaget for hvad. Brancheforeningernes skræmme-taktik har indtil videre kun bidraget til at udvide kløften mellem parterne, og man må anstændigvis forlange, at der bliver fremlagt konkrete anklager og beviser.

„IT-viceværterne" – ny FORA-gruppe i DKUUG

Kollegierne er nu så organiserede, at man kan se siden oversat til sønderjysk i Sønderborg.

Der er kommet et nyt medlem i familien: „IT-viceværterne" (arbejdstitel) hed oprindelig Kollegienet, men da fora´et også inkluderer boligforeninger, var et navneskifte på sin plads. IT-viceværterne, der repræsenterer ca. 10.000 bebeoere, mødtes første gang 12. februar i Symbion. Vi har talt med en af hovedmændene, EDB-konsulent Henrik Kressner, der fik ideen efter at have installeret netværk på mange kollegier.

- Hvordan startede IT-viceværterne?
Henrik: Idéen startede vel egentlig da jeg for et par år siden havde nogle konferenceindlæg for DKUUG i forbindelse med Java. Der traf jeg Bo Folkman, og siden hen har ideen udviklet sig.

- Hvad er målet med IT-viceværterne?
- At skabe et forum for IT-ansvarlige på kollegier og i boligforeninger. Et sted hvor de kan møde ligesindede, tilade sig at være nørder, søge hjælp når det brænder på, og i det hele taget få inspiration.

- Hvad er fordelene ved at lave et kollegie/bolignet?
- Det svar er enormt. Som jeg plejer at sige til boligselskaberne, hvis I ikke kan se det, så vent med at installere det til I kan, ellers drukner I i problemer. Men den mest overraskende effekt er faktisk at et net giver bedre socialt sammenhold. Ingen gider sidde og glo på en skærm hele dagen lang, og zappe alt og alle. Nej, de vil hellere zappe ukendte naboer, og så gå ned i baren og prale med deres meritter, som i en god gammel flyverfilm. Det giver forbavsende gode vibrationer. Ikke bare med spil, der er masser af vidt forskellige chat forums, og de forsøges nu at gøre landsdækkende på egne netværk.

Så er der alt omkring den intelligente bolig, som jeg kæmper en sej kamp for at få de etablerede, herunder de store rådgivningsfirmaer, til at indse.

Men måske mest af alt, det er en ny måde at bo på. Må vi bede om at få den LOKALE landsby tilbage, her midt i den globale. (Det er nu rart, den også er global, men vi må ikke glemme den lokale)

- Hvilken oplevelse har du med at installere net på kollegier.
- Det er bare så fedt, pragtfulde mennesker der forstår at stille krav. De har idéer, de har lysten, de har energien til at implementere alt det, min generation har ventet på, siden det blev omtalt af Claus Toksvig og Chr. Rousing under Apolloturene. Så skal man da være godt dum, hvis ikke man vil hjælpe til.

Transmeta afslører strømsvage chips

af Hans Arne Niclasen

Så blev det endelig afsløret, hvad Linus Torvalds har lavet i de sidste tre år.

Det var en dag imødeset med spænding: Efter tre års venten løftede det californiske firma Transmeta sløret for, hvad de laver. Transmeta er især interessant i Linux-samfundet, fordi det siden 1996 har haft Linux-skaberen Linus Torvalds på lønningslisten, og han har indtil ikke kunnet fortælle, hvad han egentlig gik og lavede. Men nu er katten ude af sækken: Transmeta afslørede 19. januar de to første 128-bit chips i produktlinien Crusoe, der er rettet mod det mobile marked. Den ene, TM5400, er Windows-kompatibel og rettet mod bærbare computere. Den leveres med en intern hastighed fra 500 MHz til 700 MHz. Den anden, TM3120, er til Internet-apparater, der kører under en "mobil" version af Linux, udviklet af Linus Torvalds. Transmeta vil selv lancere en såkaldt Web-pad (notesblok), baseret på denne chip. TM3120 er allerede frigivet, mens TM5400 forventes på markedet til sommer.

Der er flere virkelige nyheder i Crusoe-chips´ene: For det første det ringe strømforbrug. En Crusoe-chip forbruger kun en brøkdel af Intels tilsvarende chips. Helt præcist forbruger chips´ene 20 milliwatt strøm i slukket tilstand og 1 watt, når de er i brug. Transmeta har skrevet sin egen BIOS med Power Management på selve chip´en - kaldet „LongRun". Chip´en beregner, hvormeget strøm, der skal bruges og justerer strømmen derefter, hvilket skulle give meget længere batterilevetid. Samtidig kører en Crusoe i brug med en varme på 48 grader Celsius i modsætning til f.eks. Intels nye Pentium III, der opnår en varme på 113 grader celsius, hvilket overfødiggør brugen af køler i Crusoe-apparater, hvilket igen sparer strøm.

For det andet har Crusoe valgt ikke at bruge mere silicium for at opnå mere ydelse. I stedet findes der for første gang software på en chip, hvilket muliggør, at Crusoe kan processere informationer, der er skrevet til x86 – processorer.

Transmeta går efter at få Crusoe-chips i alt fra mobiltelefoner til bærbare computere, men industrien er lidt bekymrede over, at firmaet indtil videre ikke har kunnet præsentere en eneste hardware-producent, der vil understøtte den nye processor. Tilsyneladende tror IBM dog på Transmetas chips, da de fremstiller chipsene for dem.

Linus får tæsk

Afsløringen af Crusoe-chippen var imødeset med stor spænding og selve præsentationen tiltrak da også en hel del medieinteresse. Linus Torvalds var tilsyneladende ikke interesseret i at blive fremhævet som hovedperson, men det blev han (naturligvis) alligevel, og for mange kom dagens højdepunkt, da Linus som en demonstration af, at Crusoe-chippen kan bruges i eksisterende maskiner og software tog sig en omgang Quake mod David Taylor, en af Quakes ophavsmænd. Til stor skuffelse for Linus´ mange fans rundt i verden, fik han godt og grundigt tæsk (i spillet altså) af Dave Taylor, der bagefter kommenterede, at Linus "sucked" (igen i spillet, altså).

Linus afslørede, at hans "Mobile Linux" naturligvis er Open Source og snart vil blive gjort offentligt tilgængelig. Nu er det bare at vente på, om Transmeta får succes med Crusoe-chippen.

LinuxForum 2000

Efter sidste års succes med konferencen ON99, er det nu blevet tid for endnu en DKUUG/SSLUG Linuxkonference. Denne gang er der tale om én dags konference, LinuxForum 2000, der afholdes i samarbejde mellem i Symbion, København lørdag den 4. marts 2000.

Konferencen fokuserer på anvendelsen af åbne teknologier såsom Linux, FreeBSD og Open Source projekter generelt. Konferencen vil i høj grad dreje sig om Linux og FreeBSD som fremtidens styresystemer, men andre Åbne Systemer og teknologier vil også være repræsenteret.

Der vil være følgende talere ved LinuxForum2000:

Matt Welsh:
New challenges to the Linux community

Grundlægger af Linux Documentation Project i 1992. Forfatter til bøgerne "Running Linux" og „Linux Installation and Getting Started Guide" og redaktør af „Linux Journal" og „Linux Magazine". Til daglig er Matt Ph.D.-student i datamatik ved University of California, Berkeley.

Göran Andersson:
Bourne-skalprogrammering

Göran Andersson har arbejdet med UNIX siden 1986 og med Linux siden 1995. Han arbejder til daglig hos Init AB som UNIX-konsulent. Göran er ordfører i SLUG (Stockholm Linux User Group). Göran har arbejdet på Debianudgaven af Linux og har skrevet bogen "Introduktion till GNU/Linux".

Kalle Dalheimer:
KDE - The Next Generation

Kalle er for nylig udvandret fra Tyskland til Sverige, hvor han dybt inde i Värmlands skove er direktør for firmaet Klarälvdalens Datakonsult AB, et firma, der specialiserer sig i cross-platform software udvikling (med fokus på at portere fra Windows til Linux), træning af udviklere og teknisk dokumentation. Kalle var med til at grundlægge KDE-projektet, hvor han arbejder som deltids vedligeholder af biblioteker, Koffice-udvikler og næsten-fuldtids evangelist. Han har skrevet flere O'Reilly-bøger, bl.a. "Programming with Qt" og sammen med Matt Welsh tredje udgave af "Running Linux".

Claus Sørensen:
Kontor-pc med Linux

Claus Sørensen har igennem længere tid fokuseret sin viden om Linux på netop kontor-pc'en, som efter hans opfattelse er det område, hvor Linux har størst potentiale for skoler, private og mindre virksomheder. Desuden er Claus formand for KLID (Kommercielle Linux Interesser i Danmark og har sit eget Linux-konsulentfirma, Plomus.

Ole Tange:
Perl 1-liners

Ole Tange har en fortid som DK-Hostmaster (DNS-admin for dk) og arbejder nu hos Uni-C som sikkerhedskonsulent, hvor han bl.a. holder foredrag om sikkerhed på Internettet. Han har arbejdet med Unix siden 1991, Linux siden 1992 og han slettede sin windows-partition i 1996.

Ulrik Buchholtz:
GIMP - avanceret billedbehandling

Ulrik Buchholtz er 16 år og går på Gl. Hellerup Gymnasium. Han begyndte at bruge Linux i efteråret 1998, og blev hurtigt solgt. Han arbejder idag for Lyngby Uddannelses Centers Biblioteker som hjemmeside- og databaseprogrammør og har brugt sin fritid på at lave billeder og programmer på computeren.

Peter Makholm:
Kryptering for brugere: mail, news og filbeskyttelse

Peter Makholm studerer datalogi på Københavns Universitet. Favoritdistributionen er Debian, som han også aktivt er med til at udvikle. De sidste to gange Peter bootede sin computer i andet end Linux var for at prøve at installere FreeBSD og Solaris.

Thomas Jørgensen:
Make, program til styring af oversættelse

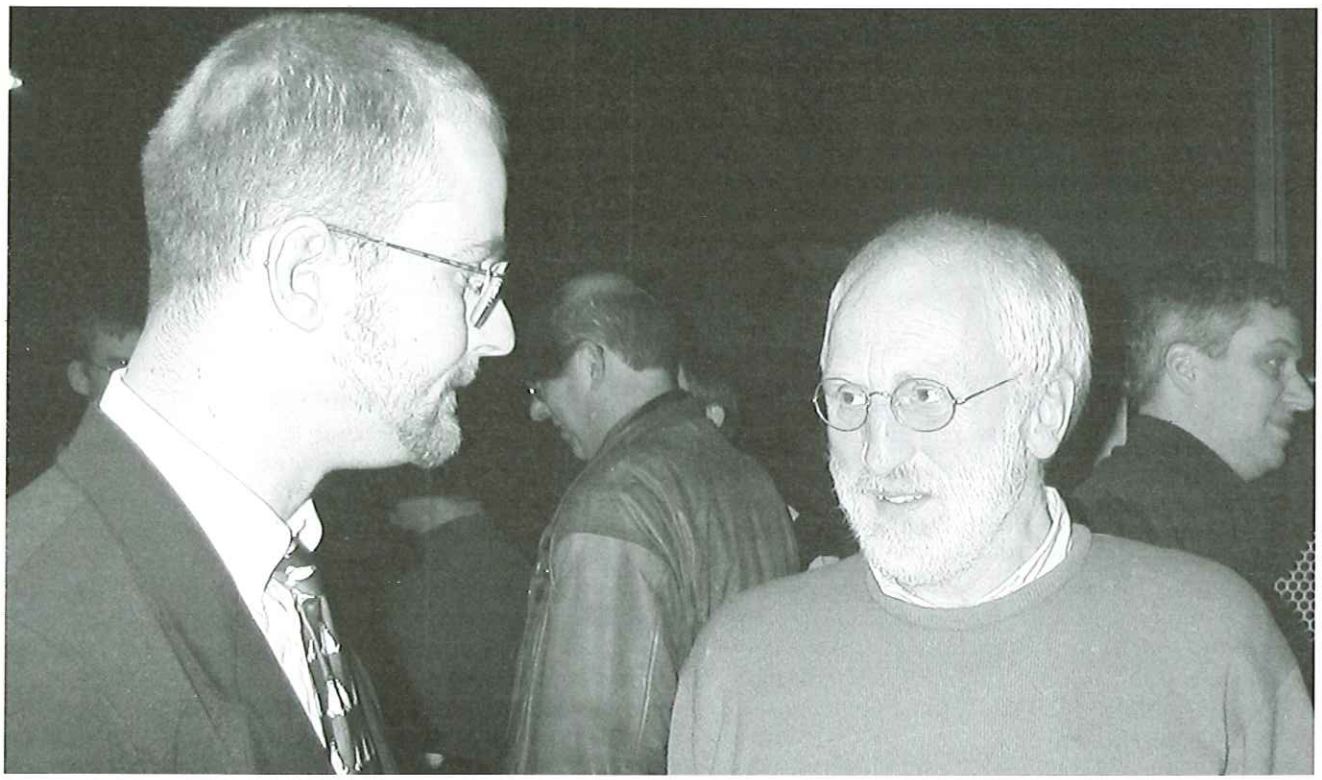
Thomas Jørgensen er egentlig svagstrømsingeniør fra Københavns Teknikum, men har de sidste 7 år udelukkende beskæftiget sig med EDB og er også set studere på DIKU. Han har programmeret i C siden 1989 og brugt Linux siden 1994, hvor „CDROM-drev og mus var ekstraudstyr til en PC." Nu arbejder Thomas hos SuperUsers, hvor han holder kurser i C, Perl, Unix, HTML/CGI/JavaScript og... Linux (selvfølgelig!).

Gene Spafford:
Why Open Source Software Only Seems More Secure

Eugene H. Spafford (Spaf) er professor i datalogi ved Purdue University og en af verdens førende eksperter indenfor datasikkerhed. Spaf har skrevet over 100 artikler, rapporter og bøger om sikkerhed indenfor information, softwareudvikling og etik. Dr. Spafford fungerer regelmæssigt som konsulent i informationssikkerhed og computerforbrydelser for advokater, store firmaer, den amerikanske regering og ordenshåndhævere verden over.

Derudover vil sikkerhedsekspert Henrik Størner fra Neupart & Munkedal fortælle om Linux til hjemme-netværk og Bernino Lind vil fortælle om php - det intelligente web

Læs mere på konferencens hjemmeside, www-linuxforum.dk, men sæt allerede nu kryds i



Knud Erik Hansen (t.h.) i samtale med Ole Tange fra SSLUG under krypteringshøringen i Eksperimentariet.

Open Source – ideén stormer frem

af Hans Arne Niclasen

På det seneste har Open Source-idéen fået fodfæste rundt omkring i verden, også fra mere eller mindre officiel side. Vi har samlet nogle af de seneste nyheder om Open Source.

Open Source i det offentlige Frankrig

I Frankrig arbejder en række senatorer i øjeblikket på et lovforslag, der skal pålægge statslige og kommunale myndigheder at anvende Open Source-software. Loven har en god chance for at blive vedtaget indenfor de næste par måneder. Senatorerne har tidligere offentliggjort flere forslag, der pålægger det offentlige at bruge gratis software, men nu er definitionen blevet tilpasset, så den passer med Open Source software (trofaste læsere vil vide, at Open Source betyder, at kildekoden er tilgængelig, og at

enhver kan ændre, tilpasse og distribuere programmet. At Open Source-programmer ofte er gratis, er en anden sag).

Flere franske ministerier har offentligt støttet Open Source-ideologien, og det franske forsvarsministerium overvejer i øjeblikket at anvende Debian Linux som operativsystem. Det siges også, at premierminister Jospin diskret støtter Open Source-ideen.

I forslaget foreslås det, at der oprettes en statslig tilsynsmyndighed, L´Agence du Logicel Libre, der kan holde øje med og hjælpe til i omstillingen fra det kommercielle software til fri software – en omstilling, der ifølge forslaget skal være gennemført i hele det "offentlige" Frankrig 1. januar 2002.

Kina dropper Microsoft

I Kina har regeringen forbudt brugen af Microsofts nye styresystem Windows 2000 i alle dele af regeringskontorerne. Windows 2000 bliver lanceret på det kinesiske marked indenfor det næste halve år. Beslutningen er gjort i et forsøg på at promovere lokalt udviklet software, skriver den officielle kinesiske avis Yangcheng Evening News. Ifølge avisens kilder sparer regeringen milliarder af dollar ved at droppe Windows.

I stedet vil ministerierne bruge „Red Flag - Linux", en nyt softwareplatform, der er skabt af kinesiske udviklere blandt andet fra den lokale afdeling af Compaq, der har taget udgangspunkt i operativsystemet Linux. Det er traditionen tro svært at få informationer ud af den kinesiske regering men Linux som "offentligt" styresystem i verdens største nation, ses som en stor sejr for Open Source-idéen

SF erklærer krig mod Microsoft

Her i Danmark har SF erklæret krig mod Microsoft's monopol og vil i Folketinget stille forslag om Open Source Software i Danmark – sådan lyder det i hvert fald i en pressemeddelelse fra partiet.

"SF vil i Folketinget stille forslag om, at regeringen tager de nødvendige initiativer, så udbredelsen og anvendelsen af Open Source i den offentlige sektor kommer i gang" – udtaler Knud Erik Hansen, Folketingsmedlem for SF.

"Det er afgørende for SF, at vi omsider har mulighed for at bryde Microsofts de facto monopol, og dermed får mulighed for at opbygge det Europæiske videns- og netværkssamfund på en åben teknologi, der skal give et meget mere frugtbart udviklingsmiljø, og med mulighed for at den store underskov af små og mellemstore danske og europæiske softwarevirksomheder kan få mulighed for at udvikle produkter til styresystemet, uden at de konstant skal slås med Microsoft og deres advokater" – fortsætter Knud Erik Hansen.

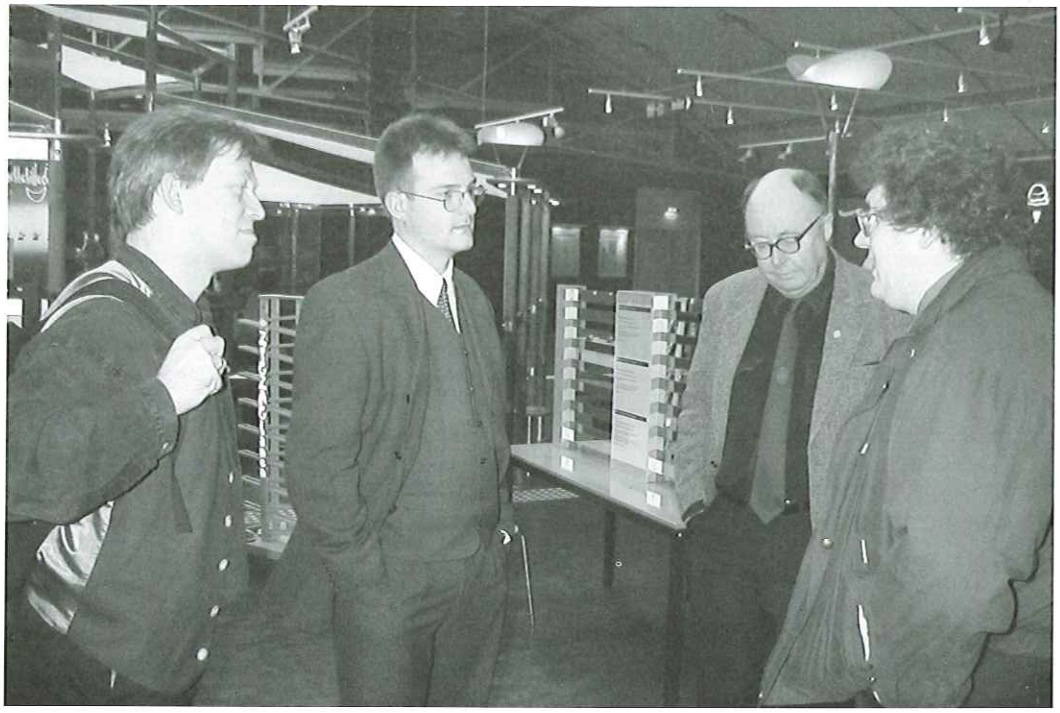
"Det er også afgørende for SF, at det bliver betydeligt billigere for både erhvervslivet og almindelige mennesker at anvende Open Source software – specielt vil virksomheder have stor gavn af det, fordi det bliver meget lettere at tilpasse programmel til deres behov. Virksomheder kan med open source systemer langt lettere skifte leverandører og dermed nyde godt af en reel konkurrence."

SF vil have den offentlige sektor til at trække udviklingen i gang. "Når det er sket, er jeg overbevist om, at den private sektor hurtigt vil følge efter" – udtaler Knud Erik Hansen – derfor er vores forslag en krigserklæring mod Bill Gates og kan blive en langt større trussel for ham end de retsager, der i øjeblikket pågår i USA." SF vurderer, at den danske stat på årsbasis kan spare 500 millioner kr. ved at gå over til fri software.

Reaktioner

SFs forslag har fået en blandet modtagelse i de etablerede medier, men mange har fået dog øjnene op for, at Open Source er noget, man skal tage alvorligt. Selvom mange kommentarer – f.eks. i Politikens computersektion – har gået på, at Bill Gates nok sover roligt på trods af SFs forslag, er mange begyndt at overveje, om det, der opstået i "det anarkistiske nørdmiljø" (citat: Politiken) måske alligevel er en bedre måde at udvikle software på. Naturligvis skal mange vænne sig til ,at man kan tjene penge på noget, der er gratis og offentligt tilgængeligt, men der er jo talrige eksempler på firmare, der tjener penge på Linux og andet Open Source-programmel. Det bliver spændende at følge den videre udvikling indenfor Open Source.

Offentlig høring om kryptering



Verdenener mødes: ved IT-høringen f.v. Werner Koch, Bart Simons (Utimaco), Roger Needham (Microsoft) og Stefek Zaba (HP)

Af Hans Arne Niclasen

IT-sikkerhedsrådet afholdt høring om sikker kommunikation ved hjælp af kryptering – og fortalerne for Åbne Systemer markerede sig.

Debatten om ulovlig overvågning og aflytning – bl.a Echelon - har medført, at forskningsminister Birthe Weis har bedt IT-sikkerhedsrådet undersøge mulighederne for at sikre danskernes kommunikation ved hjælp af kryptering.

IT-sikkerhedsrådet afholdt derfor 17. januar 2000 en høring i Eksperimentariet i Hellerup. Høringen skulle belyse hvilke muligheder, danskerne for at beskytte deres kommunikation på Internettet med sikker kryptering og om der er behov for at udvikle et særligt dansk krypteringsprodukt.

IT-sikkerhedsrådet havde indbudt en række producenter af sikker kryptering til at vidne ved høringen, men havde i første omgang glemt Open Source-samfundet. Det blev der rådet bod på ved SLUUGs og DKUUGs mellemkomst, da det lykkedes at få Forskningsministeriet til at invitere Werner Koch fra Düsseldorf.

Werner Koch – manden bag GnuPG

Werner Koch har udviklet GnuPG, en fri softwareversion af krypteringsprogrammet PGP (Pretty Good Privacy), der bl.a. er underlagt de amerikanske restriktioner på eksport af stærk kryptering og derfor ikke er fri software. Det er Gnu PG, der leveres med fuld kildekode og dermed giver brugeren bedre sikkerhed for, at uvedkommende ikke kigger på ens krypterede post. Den tyske stat har fattet interesse for GnuPG og har fornylig givet 250.000 DM til og videreudvikling og markedsføring af krypteringsprogrammet.

Høringen

IT-høringen blev indledt med en velkomst ved Forskningsministeren. Birthe Weiss fastslog, at regeringen tager diskussionen om privatliv på Internet og e-mail meget alvorligt og hun nævnte også Echelon, som hun tilsyneladende tror på eksisterer. Ministeren slog fast, at Danmark har en krypteringspolitik og at

brevhemmeligheden er en grundlæggende menneskeret. Derfor skal enhver dansker have adgang til fri kryptering. Ministeren måtte desværre gå efter velkomsten og gik dermed glip af den spændende debat.

Så var det tid til producentpanelet, der bestod af følgende:

Neil Hallenden, Baltimore Technologies (Irland)
Anette Byskov, Cryptomathic (Danmark)
Niels Thune Højberg, IBM Danmark (Danmark/USA)
Roger Needham, Microsoft Research Ltd (Cambridge, England)
Albert Huth, iD2 (Sverige)
Stefek Zaba, Hewlett Packart Bristol Lab (UK/USA)
Bernhard van der Feen, Network Associates (USA)
Bart Simons, Utimaco (Tyskland)
Werner Koch - GnuPG/Open Source

Hver producent fik fem minutter af ordstyreren, IT-sikkerhedsrådets formand Mads Bryde Andersen, til at præsentere deres produkter. Stefek Zaba fra HP var første taler og vakte fra starten jubel ved at præsentere HPs krypteringsprodukter med håndskrevne overheads – og så er produkterne tilmed Open Source (sådan da). Werner Koch præsenterede GnuPG og fremhævede fordelene ved Open Source-udvikling – ingen mulighed for "bagdøre", tusindvis af testere o.s.v. Roger Needham, der af fremtoning ledte tankerne hen på en ægte distræt Cambridge-professor, afslørede at kryptering er indbygget i Windows 2000, men ikke hvor stærk kryptering, der er tale om.

Et udspørgerpanel bestående af kommunaldirektør Estrid Oxlund, Holstebro Kommune, konsulent Steffen Stripp, PLS Consult , direktør Jan Carlsen, Institut for datasikkerhed og professor Lars Ramkilde Knudsen, Universitetet i Bergen, stillede nogle korte spørgsmål til panelet, inden der blev mulighed for at stille spørgsmål fra salen – og her var de ca. 15 fremmødte SSLUG-medlemmer hurtigt (meget hurtigt) fremme med spørgsmålet, om hvorvidt firmaerne ville fremlægge kildekoden til deres programmer. Det kunne Networks Asscociates (der markedsfører PGP) og naturligvis GnuPG bekræfte at de gjorde, mens HP var villige til at lade en ekspert se på deres kildekode - den er altså ikke helt offentlig tilgængelig. Baltimore overvejede i øjeblikket at gøre deres produkt offentligt tilgængeligt og resten havde ikke til sinds at offentliggøre deres kildekode, men var villige til at lade deres produkter teste af en uvillig instans.

Panelet: Bagerst f.v. Werner Koch, Anette Byskov (Cryptomatic), Niels Thune Højbjerg (IBM), Albert Huth (iD2), Bernhard v.d. Feen (Network Associates), Stefek Zaba og Roger Needham.

Statslig kryptering er en dårlig ide

Efter en pause var producentpanelet udskiftet med et panel med forskelligartede interesser, der skulle belyse, om der er et behov for, at Danmark udvikler egne krypteringsprodukter.

Dette panel bestod af de fire medlemmer af IT-sikkerhedsrådet Estrid Oxlund, Steffen Stripp, Jan Carlsen og Peter Landrock, direktør for Cryptomathic, samt af MF Kim Behnke, Jens Risgaard fra Dansk Dataforening og Morten Storm Pedersen, Tele Danmark. En repræsentant fra Justitsministeriet skulle også have været tilstede, men dukkede først op senere – og da blandt spørgerne.

Kim Behnke lagde ud med at konstatere, at udviklingen af et krypteringssystem i statsligt regi er en rigtig dårlig ide, for det gælder netop om at udvikle et system, hvor borgerne kan have tillid til, at regeringen eller andre ikke lytter med. Morten Storm Petersen understregede, at netværket i øjeblikket opfattes som usikkert, og at det er her, der i første omgang skal sættes ind – og så skal krypteringsprogrammer være mere brugervenlige. Storm Petersen opfordrede til, at det offentlige går i gang med at reparere på deres infrastruktur og gøre følsomme oplysninger krypterede.

Den efterfølgende debat blev livlig, og fra SSLUG-repræsentanternes side blev der agiteret kraftigt for Open Source-ideén, og det gik især ud over en tilsidst tydeligt irriteret Peter Landrock.

Der kan ikke siges at være en entydig konklusion på høringen. IT-sikkerhedsrådet mødes i begyndelsen af marts for at tage en endelig beslutning om en anbefaling til en dansk sikkerhedspolitik – lad os håbe, det bliver den rigtige.

Om aftenen var Werner Koch endnu engang i ilden ved et velbesøgt ekstramøde i DKUUGs Klub København, hvor han fortalte om udviklingen af GnuPG.

Generalforsamling i DKUUG

Den ordinære ordinære generalforsamling 25. november 1999 blev meget rolig. Læs her, hvad der skete.

19 stemmeberettigede mødte op til generalforsamlingen i Symbion. Formand Myanne Olesen lagde ud med at berette, at Bjørn Johannesen og Peter Lange desværre p.g.a. arbejdspres har trukket sig fra bestyrelsen og takkede dem for deres store indstats gennem årene.

Myanne Olesen fortalte om strategi-arbejdet, der blev iværksat i det tidlige forår -99 for at definere foreningens identitet og mål. Strategiarbejdet har resulteret i følgende "mission statement": DKUUG er en leverandøruafhængig, teknisk IT-forening med fokus på Åbne Systemer. Foreningen vil arbejde for at skabe et netværk med interesse for Åbne Systemer og har som mål at få flere medlemmer, flere ildsjæle og flere interessegrupper. Strategiarbejdet har også resulteret i et forslag om en ny struktur for foreningen. Ifølge forslaget skal DKUUG fremover være en paraplyorganisation med en række interessegrupper under sig.

Formanden kunne fortælle, at kontigentindtægten er faldet en smule p.g.a. et fald i antallet af organisationsmedlemmer, mens antallet af individuelle medlemskaber og studiemedlemskaber er vokset kraftigt. Presseomtalen af DKUUG er også steget betragteligt i det forgangne år.

Udvalgenes resultater

Gitte D´Arcy præsenterede bladudvalget. DKUUG-nyt ændrede lay-out og format i februar –99, hvilket har resulteret i et mere læsevenligt blad, der har tiltrukket flere annoncører.

Myanne Olesen måtte igen på talerstolen, da FORA-udvalget skulle præsenteres. I årets løb har DKUUG fået nye FORA-grupper som medlemmer, så listen i øjeblikket ser sådan ud:

- DSDM (Dynamic Systems Development Method)
- SSLUG (SkåneSjælland Linux User Group)
- FLUG (Fyns Linux User Group)
- AALUG (Århus Linux User Group)
- KLID (Kommercielle Linux Interesser i Danmark)
- XML-gruppen
- SILD (Sammenslutningen af IT-ladies i Danmark)
- Kollegienet (som i mellemtiden har skiftet navn til IT-viceværterne)

Interessegrupperne samles nu under den nye paraply , hvor DKUUG vil hjælpe med samarbejde og oprettelse af nye interessegrupper. Der vil hurtigst muligt blive oprettet deciderede interessegrupper for UNIX og systemprogrammering.

Ulf Nielsen berettede fra klubudvalget for Jacob Bække, der dagen før var blevet far til en datter (redaktionen ønsker tillykke). Klubmøderne er i høj grad gået over til at blive arrangeret af interessegrupperne, og der kommer i gennemsnit ca. 100 til hvert møde, hvilket er en fordobling i forhold til sidste år. Af nye tiltag kan nævnes Netcaféen, der har åbent efter hvert klubmøde i København og er blevet et populært mødested for DKUUGs medlemmer. Udflytningen af klubmøder til Symbion og samarbejdet med SSLUG, FLUG og AALUG har været succesfyldt. I fremtiden vil klubudvalget arbejde med sponsorering, hvilket skulle give mulighed for dyre talere.

Myanne Olesen måtte også holde for ved præsentationen af marketing- og MedlemsMøde-udvalgene. Med baggrund i strategiarbejdet arbejdes der med et nyt navn og logo, hvilket vil blive fremlagt på en generalforsamling.

Kristen Nielsen berettede fra Netforum, der har ansvaret for opsætning og drift af DKUUGs netaktiviteter. I 1999 har Netforum opsat en firewall, opgraderet alle servere og udskiftet RAID-diskene i ftp-serverne, som der er god trafik på. I det kommende år vil Netforum udvide ftp-kapaciteten, automatisere flere services, yde bedre IT-støtte til sagsbehandlingen i sekretariatet og etablere Login-servicen, som DKUUG har overtaget fra Tele Danmark.

Svend Thygesen præsenterede standardudvalget. Svend sammenlignede udvalgets mål med de opnåede resultater: Standard havde som mål at opretholde aktivitetsniveauet, men indsatsen blev reduceret i det forgangne år. Testpunktet har fået støtte til videreudvikling. Udvalget ville synliggøre standardiseringsarbejdet, og det lykkedes, bl.a. gennem presseomtale af ISO-mødet i september, som DKUUG

DKUUG's bestyrelse efter generalforsamlingen: F.v. Gitte D'Arcy, Ulf Nielsen, Jan Kristiansen, Kristen Nielsen, Myanne Olesen, Keld Simonsen (siddende).

Peter Holm, Jacob Bække og Svend Thygesen var fraværende ved fotograferingen.

var vært for. Udvalget vil fremover arbejde på at få flere medlemmer med i standardiserings-arbejdet, vil arbejde for større synlighed og vil udvide samarbejdet med Dansk Standard. I øvrigt er DKUUG blevet autoriseret af ISO som registrant af det Kulturelle Register.

Valg til formand og udvalg

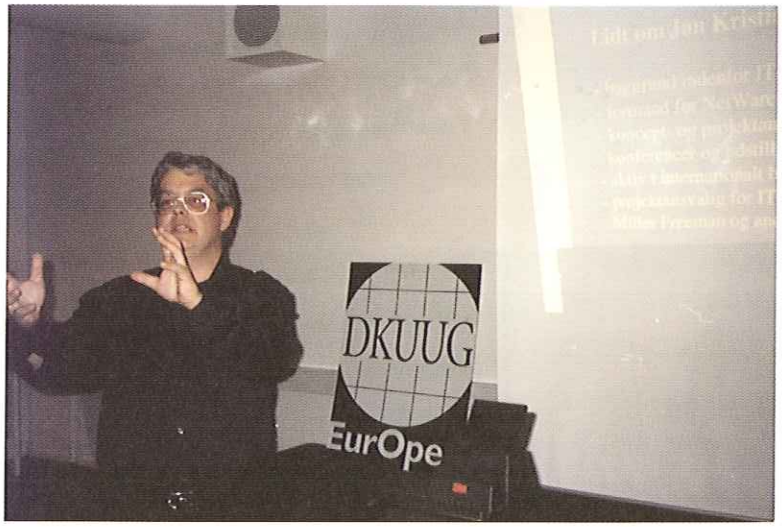
Myanne Olesen blev genvalgt som formand uden modkandidater. Der var genvalg til Kristen Nielsen, Peter L. Holm og Jacob Bække. Ny i bestyrelsen er Jan Kristiansen, der præsenterede sig selv. Jan er 53 år og til daglig leder af kursusudbyderen SuperUsers´ nystartede afdeling i Århus, Kampehøjgaard. Derudover er Jan formand for Netware Bruger Gruppen Danmark (NBD). Vi præsenterer Jan mere indgående i næste nummer af DKUUG-Nyt.

Kontingent

En kontigentstigning med virkning fra 1. januar 2000 blev vedtaget. Priserne ser nu således ud:

Stormedlemskab:	9600 - kr. (ex. moms)
Organisationsmedlemskab:	3500 - kr. (ex.moms)
Individuelt medlemsskab:	600 - kr. (ex. moms)
Studiemedlemskab:	110- kr. (ex. moms)

Alt i alt var generalforsamlingen meget rolig og efter godt tre timer kunne dirigent Michael Svendsen takke forsamlingen for god ro og orden.

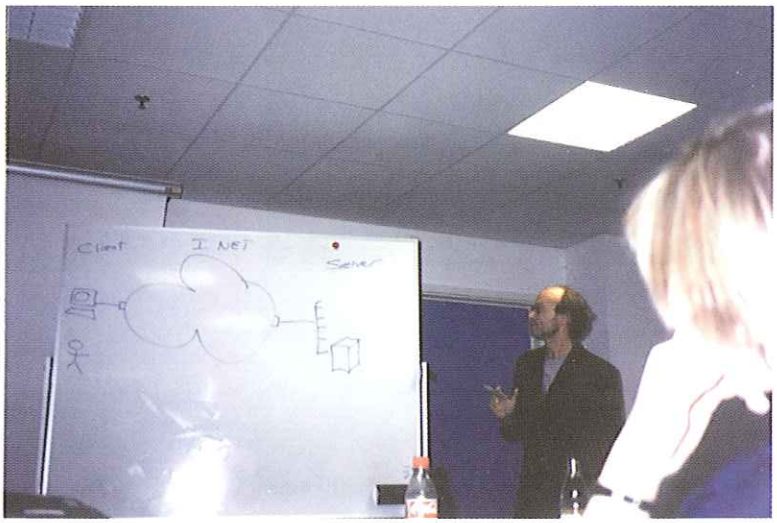


DKUUG's nye bestyrelses-medlem, Jan Kristiansen

Arrangementer i DKUUG

af Hans Arne Niclasen

Se her, hvad der er sket i DKUUG siden sidste nummer.

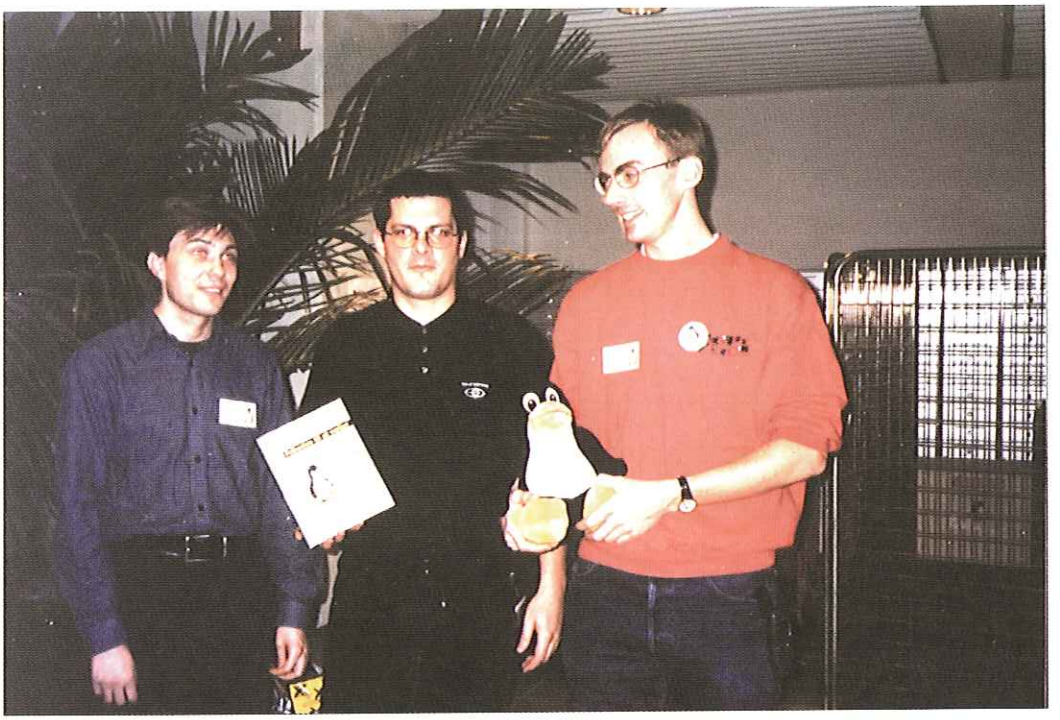


Brian Eberhardt giver sit bud på fremtiden -

Årsmøde i SILD

IT-kvindegruppen SILD holdt deres første årsmøde 1. december 1999. Brian Eberhardt holdt først et meget spændende foredrag om fremtidens Internet, inden SILD konstituerede sig. Initiativtageren Hanne Schmidt blev valgt til styresild og der blev nedsat en styregruppe med 7 medlemmer. 19. januar 2000 holdt SILD sit første møde, hvor BEA fortalte om e-commerce.

- Til stor interesse for SILD'ene



De stolte forfattere til „Linux - Friheden til at vælge".
F.v. Kenneth Geisshirt, Snebjørn Andersen, Tux og Peter Toft

Ny udgave af Linux -Friheden til at vælge

9. december lagde DKUUG hus til præsentationen af bogen "Linux - Friheden til at vælge" af Peter Toft, Kenneth Geisshirt og Snebjørn Andersen, der nu er kommet som "rigtig" bog på Forlaget Globe.

SSLUG hyggemøde og Installfest

14. december holdt SSLUG hyggemøde og Installfest, og det lykkedes at trække 100 Linux-entutiaster til Symbion i den værste snestorm i mands minde. Som det ses på billedet, dukkede julemanden også op, men han har selvfølgelig også en kane at komme frem med.

Julemanden var også til Install-fest

Afsløring af medlem nummer 2000

21. december 1999 fik DKUUG sit medlem nummer 2000, og det blev med en lille højtidelighed på kontoret. Det blev Telia Mobile, der løb med den eftertragtede titel og det flotte diplom.

Bo Folkmann overrækker Katrine Holm det synlige bevis på, at Telia Mobile er DKUUG-medlem nummer 2000.

Bo Folkmann fyldte 50 år

DKUUGs direktør Bo Folkmann troede han kunne slippe for festligholdelse af sin 50-års fødselsdag ved at fylde år 31. december 1999. Men så let slipper man ikke her i foreningen: Ved et sindrigt komplot (der bl.a. involverede Bos kone Mona), lykkedes det at lokke Bo forbi kontoret 30. december – og der ventede en overraskelse, som det ses på billedet. Godt 40 stk. familie, venner og bekendte ventede på at tage fusen på Bo, hvilket lykkedes til fulde. DKUUG-Nyt ønsker endnu engang tillykke til Bo og held og lykke med de næste 50 år.

Og her bliver overraskelsen fuldbyrdet

Her går det op for Bo Folkmann, hvad der foregår.

Præsentation af Novell Netware 5.1

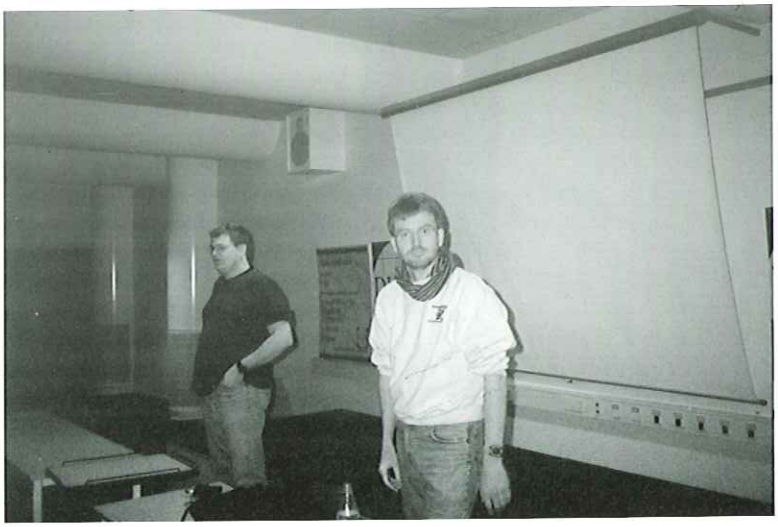
20. januar 2000 lagde DKUUG hus til, da det nyeste FORA-medlem, Netware Brugergruppen Danmark (NBD) præsenterede Novell Netware 5.1. Arrangementet blev med 230 deltagere et af de største tilløbsstykker i foreningens historie.

230 deltagere til NBD-gruppens præsentation af Netware 5.1

Da FreeBSD-gruppens ledelse er de til enhver tid fremmødte, må dette være ledelsen 25. januar 2000.

F.v. Anton Berezin, Michael Larsen, Flemming Jacobsen, Jon T. Erichsen og Phil Regnauld

Poul-Henning Kamp (t.v.) ser lidt skræmt ud ved mødet med DKUUG's Klub København - helt så slemt var det nu ikke.



FreeBSD i Klub København

Poul-Henning Kamp holdt foredrag om FreeBSD i klub København og de ca. 50 fremmødte fik sig god og hjertelig diskussion, der bl.a. indeholdt en del drillerier mellem Linux- og FreeBSD-lejrene (nogle læsere husker sikkert en artikel i DKUUG-Nyt sidste år, hvor Poul-Henning sammenlignede Linux med en tunet Opel Ascona og FreeBSD med en stor lastbil – i øvrigt den hidtil eneste artikel, der har fået et medlem til at melde sig ud). Ved samme lejlighed holdt DKUUG i øvrigt møde med FreeBSD-gruppen om muligheden for at få gruppen ind som FORA-medlem.

Siden sidst

Siden med nyt fra DKUUG og resten af verden.

AOL køber ind

I de seneste måneder har internetportalen og -udbyderen America Online købt stort ind og er godt på vej til at blive enerådende på levering af underholdning på Internettet. Først blev Netscape købt og i begyndelsen af januar blev det annonceret at AOL har købt film- og TV-giganten Time Warner for den nette sum af 1285 milliarder kroner. Warner-koncernen beskæftiger sig udover filmproduktion med TV via ejerskabet af tv-kanaler som CNN, TNT og TBS og har også et pladeselskab – mere om det lige om lidt. Mediegiganten kommer til at hedde AOL Time Warner, og selvom om der tales om en fusion, er der reelt tale om en AOL-overtagelse af Time Warner, der har en gæld på 128 milliarder kroner. I begyndelsen af februar blev det annonceret, at AOL Time Warner også har købt det engelske pladeselskab EMI, der nu fusioneres med Warner Music Group for at skabe verdens største pladeselskab – EMI Warner Music Group - med kunstnere som Madonna, Eric Clapton, Alanis Morisette, Spice Girls og The Rolling Stones. Allerede nu har AOLs kunder adgang til Time Warner´s film- og TV-udbud, og inden længe vil musik fra EMI Warner Group blive distribueret gennem AOLs web-portal.

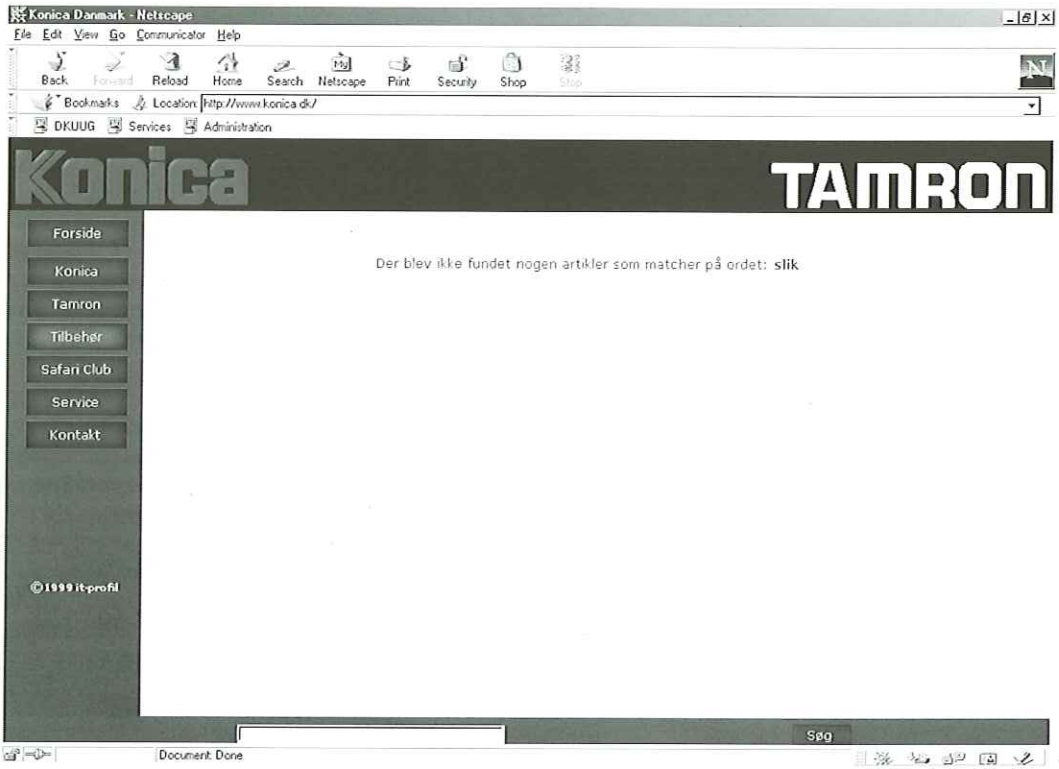
Det forventes i branchen, at vi i fremtiden vil opleve flere fusioner mellem Internetbranchen og underholdningsbranchen, mens de to verdener smelter sammen. Rygter har indtil videre kædet Microsoft sammen med teleselskabet AT&T, Yahoo, filmselskabet Viacom samt tv-kanalen CBS, men ifølge den forhenværende Bill Gates er Microsoft ikke interesseret i at fusionere med nogen som helst.

Månedens hjemmesidebøffer

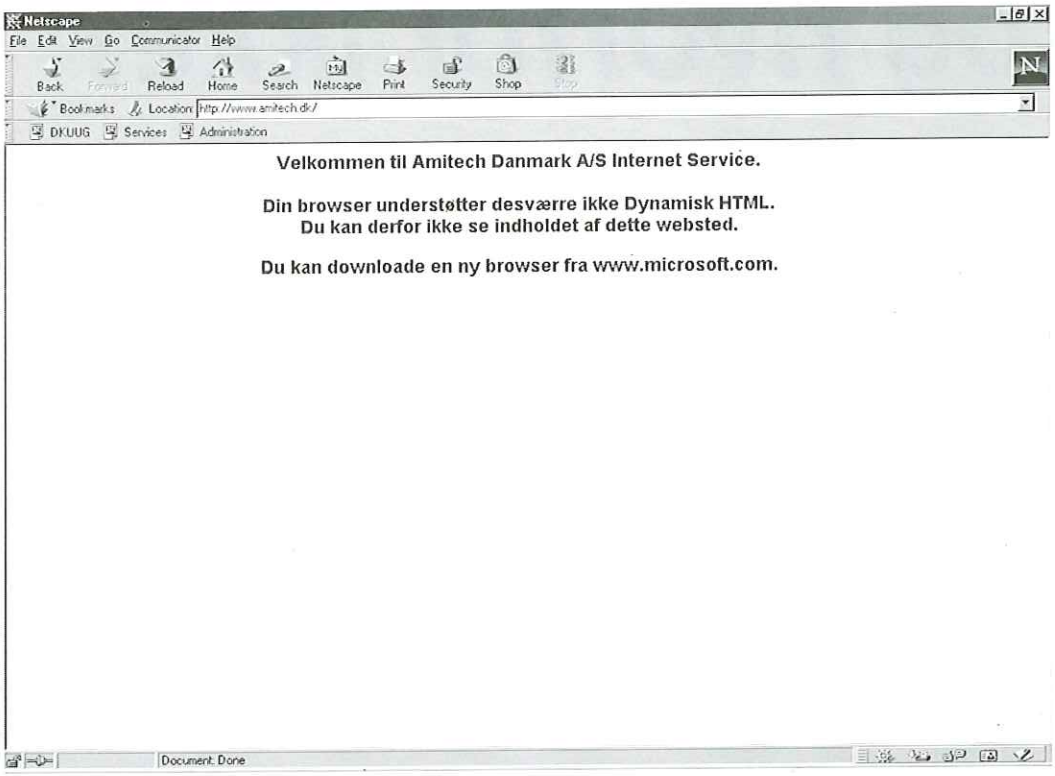
I denne måned synes vi vil grine af hele tre bøffer – mærkeligt nok alle fra anerkendte firmaers hjemmesider. Den første bøf blev godtnok fundet af en ComputerWorld-læser, men vi synes, den var så morsom, at vi ikke kan lade være med at bringe den videre.

Det drejer sig om fotofirmaet Konicas hjemmeside. Hvis man vil se, hvad tilbehør man kan få til Konica-kameraer, får man denne besked: „Der blev ikke fundet nogen artikler som matcher ordet: slik".

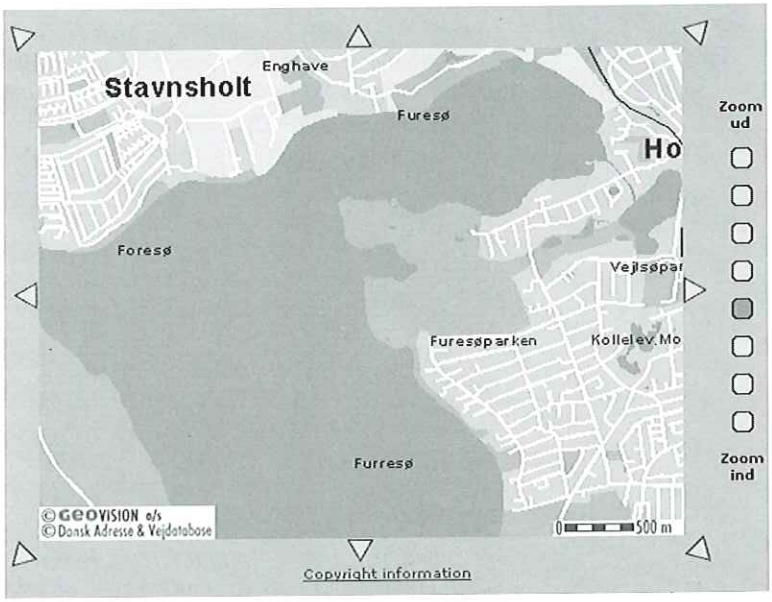
– og så kan vi selvfølgelig godt more os over, at den stadig står der, selvom det er over en måned siden, Computerworld bragte "afsløringen".



Den næste bøf er lidt mere alvorlig: Computerkæden Amitech tillader ikke, at man bruger en Netscape-browser til at se deres hjemmeside med; men man kan downloade en ny browser på www.microsoft.com. Det er måske ikke altfor smart at afskære godt halvdelen af sine potentielle kunder fra at se ens gode tilbud (men Amitech meddeler dog, at de arbejder på sagen).



Sidst, men ikke mindst fandt redaktøren ud af, at han boede i nærheden af hele tre søer, da han på Nettet søgte efter et fadølsanlæg til sin fødselsdagfest. Der var både Foresøen, Furesøen og Furresøen. Det er jo hele tre ting på én gang.



Root access - hvem, hvordan og hvorfor ikke?

af Hanne Munkholm
<hanne@aub.dk>

og Peter Toft
<pto@sslug.dk>

Dette er den tredje artikel i en serie på seks om sikkerhed på Linux.

Når en bruger for første gang skal til at anvende Linux (eller en anden UNIX), kan det måske være svært at forstå, hvorfor man ikke skal være logget ind som systemadministrator - dvs. brugeren root - hele tiden. Dette vil vi starte denne artikel med at diskutere. Derefter vil vi se på fornuftig håndtering af root-rettigheder.

Der er flere sikkerhedsaspekter forbundet med root-adgang. Ud over risikoen for selv at komme til at ødelægge noget på sit system, er der spørgsmålet om hvilke personer ud over systemadministratoren, der skal have root privilegier - om nogen. I den forbindelse vil vi også se på nogle af de elementære forholdsregler, man bør tage for at forhindre, at uautoriserede personer får root adgang.

Desuden vil vi se på valg af passwords. Det er meget vigtigt - specielt for root-kontoen - at der vælges passwords, der ikke kan gættes. Som det sidste i artiklen ser vi på SUDO og suid programmer, dvs. programmer, der kører med rettigheder, som om de var startet af root. Dette kan naturligvis være et sikkerhedsmæssigt problem. Disse lokale problemer bliver til netværksproblemer i det øjeblik, nogen trænger ind på systemet via netværket. Er en cracker inde som almindelig bruger, er det endnu begrænset, hvor meget skade han kan gøre. Det er nok desværre sandsynligt, at crackeren vil gå efter at få root-rettigheder for at have fuld kontrol over din computer. Det ville også være slemt, hvis nogen fra salgsafdelingen fik fat i dit root password...
Fra http://www.userfriendly.org/static

Hvem er root?

På et Linuxsystem er der som regel et antal brugere med forskellige rettigheder. Linux er grundlæggende et fler-bruger system. Hvis man f.eks. bruger Linux i en virksomhed, eller på en skole, er der forskel på, hvad folk skal have lov til at gøre på maskinen. Hvor nogle brugere kun kan hente deres email fra maskinen, kan andre betroede brugere have lov til at logge ind på maskinen og køre programmer. De forskellige brugere har et brugernavn og et password, som de logger ind på systemet med. Ud fra bruger-ID nummeret (fås ud fra brugernavnet) afgør systemet, hvilke handlinger man har lov til at udføre. Passwordet sikrer, at man er den man giver sig ud for at være. Ingen af de „almindelige" brugere kan ændre systemfiler, konfigurere ny hardware eller re-installere software. Derfor har Linux brugeren root, som kan alt dette. Er man root, så har man total kontrol over maskinen. At være root kan du blive ved at logge ind med brugernavnet root, og det dertil hørende password. Brugerkontoen root er en system-administratorkonto, som du også kan skifte til og fra ved brug af su kommandoen. Det skal nævnes, at det er bruger-ID 0, som giver root-rettigheder, egentlig ikke alene navnet root. Hvis du derfor finder flere brugere med bruger-ID 0 (nul), så skal du være meget opmærksom på, hvad der er sket.

Hvis du er systemadministrator for en Linux-maskine og kender root passwordet, er det stadig vigtigt, at du har en almindelig bruger konto, som du bruger til daglig. Man bør kun være root, når det er nødvendigt, for at udføre opgaver, hvor root-rettigheder er nødvendige. Lad os illustrere hvorfor.

Antag som første eksempel, at du arbejder i et lokale, hvortil andre har adgang, og at du altid logger ind som root. Du skal i løbet af dagen forlade din maskine et antal gange f.eks. til frokost eller møder. Hvis du bare en gang glemmer at sætte en password-beskyttet screensaver på eller logge helt ud, kan enhver, som kommer forbi dit kontor ødelægge hele din maskine. F.eks. ved at skrive rm -rf / som vil slette alle filer på din harddisk uden at spørge, om du mener det - og der er ingen fortrydelses-mulighed. Eksemplet er naturligvis grelt og ren sabotage, men det er faktisk sket, at andre lige skulle rette noget på et tidspunkt, hvor system-administratoren lige var ude, og med root-login forvoldte stor skade, fordi vedkommende overvurderede sine evner som UNIX-administrator.

Andre uheldige hændelser sker ved, at en root glemmer at logge ud, og andre ser dette. For at

drille skiver de så rm -rf / men uden at trykke retur - dvs. ordren er ikke udført endnu. Hvis den rigtige root så kommer tilbage og ved et uheld trykker retur, er alt tabt, og han har selv udført handlingen. Det, som var en sjov spøg, blev pludselig til et sort uheld. Desværre er uheld, som disse set før.

Lad os som det næste eksempel se på de uheld, man selv kan komme til at lave, når man er logget ind som root. Den hyppigste grund til fejl og ulykker er nok slåfejl eller rettere sløseri. På en Linuxmaskine vil du normalt altid få udført den ordre, du skriver, og du må selv garantere for fornuften i dette. Linux har den fordel, at du som almindelig bruger ikke kan slette systemfiler, såsom den meget vigtige fil / etc/passwd, der indeholder information om brugerne og deres passwords. Prøver du, som almindelig bruger at slette password-filen, vil blot blot få en besked med „Permission denied" - og det skal du faktisk være glad for. Sker det samme, imens du er root, vil du få lov til at slette filen. Styrer maskinen emails for 500 brugere, så går der sikkert mellem 10 og 20 sekunder før at din telefon er rødglødende af sure folk, som ikke længere kan hente emails eller logge ind på maskinen.

Selvom man bare har sin Linuxmaskine derhjemme, og der ikke er andre, der bruger den, er det stadig vigtigt at have mindst én almindelig konto ud over root-kontoen.

Når du skal lave systemarbejde, så kan følgende fremgangsmåde være anvendelig: Tag en speciel rød kasket på hovedet, som tegn på at du nu vil være root :-) Skift nu til root arbejde ved at skrive su - root. Bemærk at nogle gange udelades minustegnet. Det kommer vi tilbage til. Og før du skriver den mindste ordre, så placer begge hænder under din bagdel. I den tilstand tænker du dig så grundigt om, før du skriver og udfører ordrer - for du kan ALT som root. Det lyder nok lidt komisk, men der er alvor i noget af det. Skil dit normale arbejde på maskinen, såsom at læse din egne emails og programmere, fra root arbejdet.

Vær kun root, når det er nødvendigt og brug root-kontoen med stor varsomhed. Sørg bl.a. for at videresende emails til root til en almindelig brugerkonto (din egen), idet du ikke bør læse emails, når du er logget ind som root. Hvis du hører til dem, der tror, at de sagtens kan administrere at være root hele tiden, så kan vi kun sige, at du ikke er den første. Det er noget man typisk hører fra begyndere, der endnu ikke har oplevet, hvor let det er som root at ødelægge meget med en lillebitte forkert kommando. Hvis du vil være root hele tiden, så kræver det stor disciplin. Du bør overveje, om du vil udsætte dig selv for de risici, det indebærer at være root hele tiden.

Vi vil gerne sige det en gang for meget, så det er helt klart: En god administrator giver altid så få rettigheder som muligt til brugerne og tilsvarende til sig selv. Kun når det er nødvendigt, skifter systemadministratoren fra sin egen personlige konto til root kontoen, og man låner ikke sit root password ud. I praksis vil man mange steder synes, at denne meget restriktive måde at administrere sikkerhed er unødigt streng og ofte fører til alt for langsomme ændringer af systemet, men det er den afvejning man altid skal lave mellem kontrol, sikkerhed og fleksibel brug af et computersystem.

su root

Så hvad er forskellen på su root og su - root? Minus-tegnet betyder at root brugerens environment (miljø-variable) bliver brugt. Hvis minus-tegnet udelades, beholder root de miljø-variable, som brugeren der skrev su kommandoen havde. Dette kan være et sikkerhedsaspekt. En brugers miljø-variable indeholder bl.a. hans personlige sti til de programmer, han vil køre, gemt i variablen PATH. Forrest i en brugers PATH kan man ofte finde „.", som betyder „det aktuelle katalog". Det betyder, at når man skriver en kommando, vil maskinen først lede efter programmet i det aktuelle katalog. Det kan være meget praktisk, men som root er det farligt. Vi antager, at en bruger har skrevet et program og kaldt det ls, og lagt det i sit hjemmekatalog. Root står tilfældigvis i denne brugers hjemmekatalog, og skriver ls. Hvis root har „." forrest i sin PATH, hvad sker der så? I stedet for at ls kommandoen bliver kørt, bliver brugerens eget program kørt - som root! Root bør ikke have „." i sin egen PATH - og slet ikke forrest. Dette er bare et eksempel. Brugeren kan også have aliaser i sine opstartsfiler, så kommandoer ikke gør det, man forventer, og der kan ske uheld - selvom man som regel bruge „su" fra sin egen bruger konto, hvor man kender opsætningen. Desuden har root ofte / sbin og måske /usr/sbin i sin PATH, hvor der ligger en række systemkommandoer. Det er en god ide altid at bruge minus-tegnet.

Uddeling af root rettigheder

Som systemadministrator vil du komme ud for, at nogle brugere har behov for at kunne lave noget „specielt" systemarbejde, og derfor mener de skal have root-passwordet. Det kunne f.eks. være selv at kunne genstarte en webserver, måske stoppe/genstarte maskinen eller dræbe processer efter programmer, som ikke fungerer. Disse ting kræver at root passwordet anvendes på tidspunkter, som ikke kan forudsiges. Du kan bevare root-passwordet på få hænder og alligevel give nogle brugere de tilstrækkelige systemrettigheder ved at installere programmet „sudo".

Programmet sudo følger ikke med alle Linux distributioner, men kan downloades fra http://www.courtesan.com/sudo. Programmet er nemt at oversætte og installere - gør følgende som root:

```
[root@sherwood robin]# tar xvzf
cu-sudo.v1.5.9p2.tar.gz
[root@sherwood robin]# cd cu-
sudo.v1.5.9p2
[root@sherwood sudo.v1.5.9p2]# ./
configure; make; make install
[root@sherwood sudo.v1.5.9p2]#
exit
```

Derefter skal du lære at konfigurere sudo rigtigt. Dette afgør, hvilke programmer bestemte personer kan tilgå. Du bør også følge med i hvilke sikkerhedsfejl, der bliver fundet i sudo (følg med på deres hjemmeside). Der er på sudo-hjemmesiden en kortfattet eksempelfil. Læs desuden man-sider for sudo, sudoers og visudo.

Konfigurationen startes som root ved at skrive

```
[root@sherwood robin]# /usr/local/
sbin/visudo
```

Nu kommer editoren vi frem med den konfigurationsfil, du skal udfylde. Som et eksempel lader vi brugeren robin kunne genstarte NFS-serveren. Find linien med

```
root    ALL=(ALL) ALL
```

Under denne tilføjer du, at brugeren robin på maskinen sherwood må køre kommandoen /etc/rc.d/init.d/nfs restart

```
robin     sherwood=/etc/rc.d/
init.d/nfs restart
```

Gem filen og prøv nu som brugeren robin at genstarte nfs.

Det eneste trick er, at du, som almindelig bruger, skal skrive sudo foran den kommando, du skal kunne køre med root-rettigheder. Efter en lille formaning om at passe på skal robin som almindelig bruger skrive sit eget passsword. Derefter udføres kommandoen, som om det var root, der gjorde det. Man skal skrive sit password som en sikkerhedsforanstaltning, der beskytter imod, at andre brugere kan udnytte ens sudo rettigheder. Hvis du f.eks. er gået til frokost uden at logge ud, så kan kollegaen ikke gå over og lave sudo kommandoer fra din maskine, da han stadig ikke kender dit password.

```
[robin@ sherwood]$ sudo /etc/rc.d/
init.d/sendmail restart

We trust you have received the usual
lecture from the local System
Administrator. It usually boils down
to these two things:

        #1) Respect the privacy of
others.
        #2) Think before you type.

Password:
Shutting down sendmail:
[  OK  ]
Starting sendmail:
[  OK  ]
```

Eksemplet er fra Red Hat 6.0, men kan være taget med en vilkårlig Linuxdistribution.

super er et andet program, som kan meget af det samme som sudo, og som kan downloades fra ftp://ftp.ucolick.org/pub/users/will. Umiddelbart har super flere muligheder, men det er sværere at anvende end sudo.

Endelig skal det siges, at programmet sudo også er smart, selvom du har spredt root password på flere hænder, idet det tvinger brugeren til at være lidt forsigtig med root-kontoen. Som afslutning vil vi dog påpege, at hvis du tildeler personer rettigheder via sudo, så bør det ikke være ene generelt blankocheck til at kunne køre alt som root. Istedet bør du anføre hver af de services, der skal kunne startes og stoppes via sudo. En god grund til dette er, at du så ikke havner i en situation, hvor dine basale binære programmer eller bibioteker er bliver udskiftet pga. misforståelser eller destruktiv handling. Hvis en person virkelig skal være root ofte, så er det måske klogere, at personen også har root-password og et tilsvarende ansvar.

Valg af password

Det er vigtigt at hemmeligholde sine passwords - især sit root password. På en Linuxmaskine logger man ind med et bruger-id såsom robin og et tilhørende password. Vi vil se på, hvorfor det er vigtigt, at du beskytter dit password, og hvordan du kan beskytte det. Vi vil se nærmere på, hvad der sker med dit password på Linuxmaskinen, og på nogle af de værktøjer, du kan bruge til at højne sikkerheden omkring passwords.

Skriv ikke dit password, hvor andre kan se det

Styrer du en Linuxmaskine med et antal brugere, der har hver sin login-konto, så er det vigtigt, at de alle forstår, at de hver især er ansvarlige for deres password. Hvis de skriver det på en lap papir og sætter den på opslagstavlen eller på skærmen, er de med til at bryde sikkerheden. Man kan grine af dette, men det er langt mere udbredt, end man skulle tro. Sagen er, at en vilkårlig anden person, som kender din kombination af login-navn og password, kan logge ind som dig og arbejde som dig, misbruge, ødelægge eller spionere i dit navn. Det skal selvfølgelig undgås.

Hvordan vælger man passwords ?

Ud over, at password ikke må skrives, hvor andre kan se det, så er det ikke lige meget, hvordan du

vælger dit password og specielt ikke dit root password.

Desuden bør man skifte password med passende mellemrum. Passwords kan knækkes ved en kombination af gode gæt og rå beregningskraft. Før vi ser på dette, så lad os se på, hvordan dit password er gemt på på din Linuxmaskine.

Dit password og information om dit login-navn og gruppe gemmes i filen /etc/passwd. Hvis du ikke anvender shadow passwords (hvad det er kommer vi ind på senere), så kan en linie i passwd-filen ligne følgende:

```
robin:A1$HNlr2zxs$A2mawluybzv8kf4Hpzz0:501:501::/
home/robin:/bin/bash
```

De første to felter er dit login-navn og dit krypterede password. Når du ændrer password (med kommandoen passwd), så vil Linuxmaskinen kryptere dit password til noget meget ukendeligt og gemme dette i /etc/passwd. Ideen bag dette er, at man har en algoritme, som hurtigt kan generere noget unikt krypteret tekst ud fra en anden tekst såsom dit password, men at det i praksis er umuligt at gå den anden vej. Det vil sige at der ikke findes en metode, hvor man finde det originale password ud fra det krypterede password. Som et lille matematisk eksempel kan vi nævne, at man nemt kan finde y hvis man kender x, ud fra y = x^3+2*x^2-3*x+2, mens det er langt mere besværligt at finde x ud fra y - i dette eksempel skal man løse en tredie grads ligning. De metoder, man anvender til at kryptere passwords, er meget smartere end bare en trediegradsligning. Metoderne er udviklet, således at man garanterer, at der kun er et password, som svarer til det krypterede password.

Fra den mere muntre afdeling kan vi lige igen vise en stribe fra http://www.userfriendly.org/static

DES kryptering af passwords

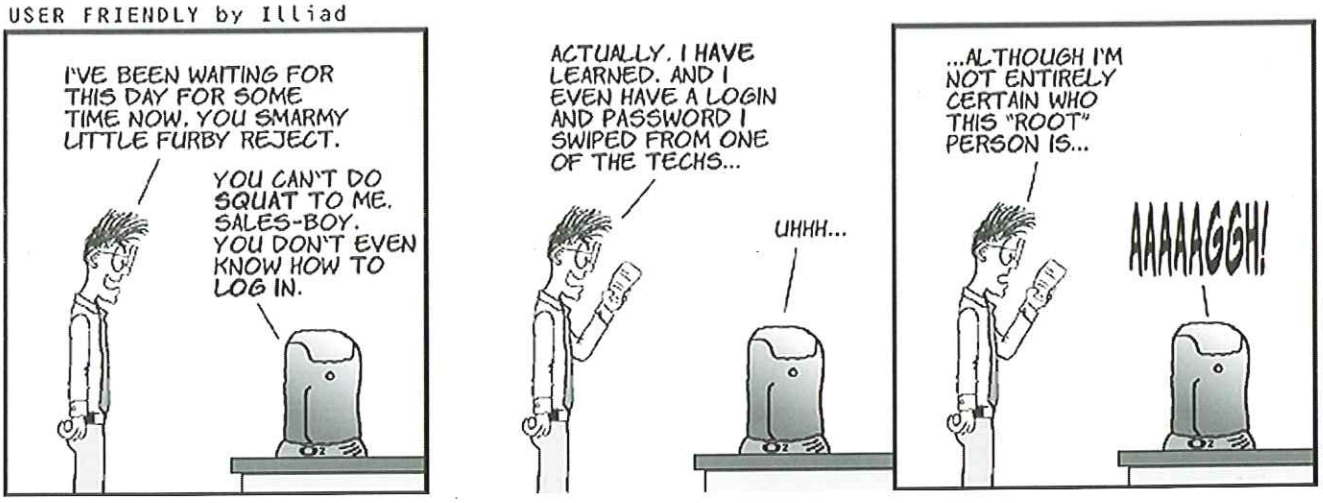
På de fleste UNIX systemer har det i mange år været standard, at et password måtte være op til otte tegn langt, og ud fra dette blev der gemt 13 krypterede tegn i din password-fil. På Linux har man længe anvendt crypt, som benytter sig af DES (Data Encryption Standard). Læs mere om DES på http://csrc.ncsl.nist.gov/cryptval/des/des.txt.

Funktionen crypt bruger det indtastede password som krypteringsnøgle. Den tekst, der krypteres, er blot en række nuller. Men det er ikke hele passwordet, der bruges som DES-nøgle, den sidste bit i hvert tegn smides væk. Desuden sættes 2 tilfældige tegn ind, det såkaldte „salt", der blot er beregnet til at gøre det sværere at rekonstruere passwordet. Se i øvrigt man crypt.

MD5

I gamle dage, hvor man ikke havde så store computere, var crypt en god løsning til passwords, da den er nærmest umulig at bryde på kort tid. Men i dag har man rå computerkraft nok til, at man ikke behøver at bryde krypteringen. Man kan i stedet sætte sine computere til at prøve sig frem fra en ende af. Derfor er der i dag brug for længere passwords, som er sværere at bryde.

Linux Red Hat 6.0 har en langt mere veludviklet håndtering af passwords end tidligere UNIX systemer, hvis man har valgt at kryptere med MD5 checksums. Man kan nu med MD5 vælge passwords, der har mere end otte tegn, og uanset længden af det man taster ind, gemmes



der altid 34 krypterede tegn i password-filen. Det er langt sværere at knække de lange passwords.

Det, vi ønsker med vores avancerede kryptering, er, at der kun er en måde, hvorpå du kan få det ukrypterede password ud fra det krypterede - ved at indtaste det korrekte password. Er du cracker, må du prøve at gætte på passwordet, kryptere alle disse passwords og sammenligne det krypterede gæt med det rigtige krypterede password. Er de to krypterede passwords ens, så er gættet og det rigtige ukrypterede password ens - du kender nu passwordet og kan logge ind på systemet som den pågældende bruger. Derfor bør man vælge et password, der er svært at gætte. Ydermere kan vi igen anbefale, at du bruger shadow passwords, for så har man ikke adgang til det krypterede password.

Jeg knækker dit password

Der findes programmer, som kan bruges til at knække passwords effektivt. Man kan måske mene, at det er med til at svække sikkerhed generelt, at der ligger programmer frit tilgængeligt på Internet, som gør det nemt at cracke passwords. Vi mener, at det er for enkelt at tænke sådan. Enhver kan i princippet skrive et program til at knække passwords, og derfor bør man måske selv lade sit password komme igennem sådan et program. Hvis det ikke er knækket indenfor en måned, er det ikke så ringe... Men så er det alligevel på tide at skifte det ud. Et udbredt program til at knække passwords er John the Ripper, der kan findes på http://www.false.com/security/john/. Man kan finde programmer, som er en del hurtigere til blindt at knække passwords fra en ende af, men John the Ripper har nogle spændende aspekter. Nedenfor er vist, hvordan programmet knækker passwords for brugeren robin i med tre forskellige passwords, hhv. „a", „ab" og „qsw". Udskriften stammer fra en 300 MHz PII, og det viser, at et bogstav knækkes på få sekunder, mens to og tre tilfældige bogstaver kan knækkes på 5 hhv. 8 minutter. Generelt så bliver det meget langsommere at knække et passwords for hver gang at der kommer et tegn mere i passwordet. Derfor bør man altid vælge passwords med mere end syv tegn.

```
  Loaded 1 password (FreeBSD MD5
[32/32])
  a                (robin)
  guesses: 1  time: 0:00:00:06 100%
(2)  c/s: 746  trying: a

  Loaded 1 password (FreeBSD MD5
[32/32])
  ab               (robin)
  guesses: 1  time: 0:00:05:12 (3)
c/s: 665  trying: ab

  Loaded 1 password (FreeBSD MD5
[32/32])
  qsw              (robin)
  guesses: 1  time: 0:00:08:08 (3)
c/s: 669  trying: qsw
```

John the Ripper er lidt langsom til de „tilfældige" passwords ovenfor, fordi det er programmeret ud fra, hvordan mange brugere i praksis vælger password. Man vælger ofte kærestens navn, måske koblet med en fødselsdag, et sted man er glad for, eller andre ting man kan huske. Det er ikke klogt, fordi det er for nemt at gætte, hvilket følgende viser. Først har vi ladet brugeren robin have password „abc" som står i alle ordbøger. Det koster kun 4 sekunder, før det er fundet. Dernæst er vist, at fem bogstaver som i ordet „apple" findes på 3 sekunder, og endelig gentagelsen „appleapple" med 10 bogstaver som kun tager 19 sekunder at knække - skræmmende, ikke sandt? Ordbøger findes til alle sprog, så vælg altid passwords som ikke står i en ordbog - bland tal ind i ord og lav et underligt system, andre ikke har en chance for at gætte. Brug f.eks. forbogstaver fra en sætning eller en sang, og flet specialtegn og numre med ind. Vær dog lidt varsom med specialtegn i passwords - specialtegnenes placering på tastaturet kan variere alt efter hvilket land, tastaturet er sat op til. Man kan f.eks. komme ud for et dansk tastatur, som er sat op som et amerikansk, hvor det kan det være ret svært at finde specialtegnene. Jo længere password du vælger des bedre - og altid på mere end syv tegn. Root passwordet skal helst være endnu længere og vælges med særlig omhu. I øvrigt bør du med jævne mellemrum ændre password, men sørg for at dette sker enten på selve maskinen eller via en krypteret adgang til maskinen såsom ssh (secure shell).

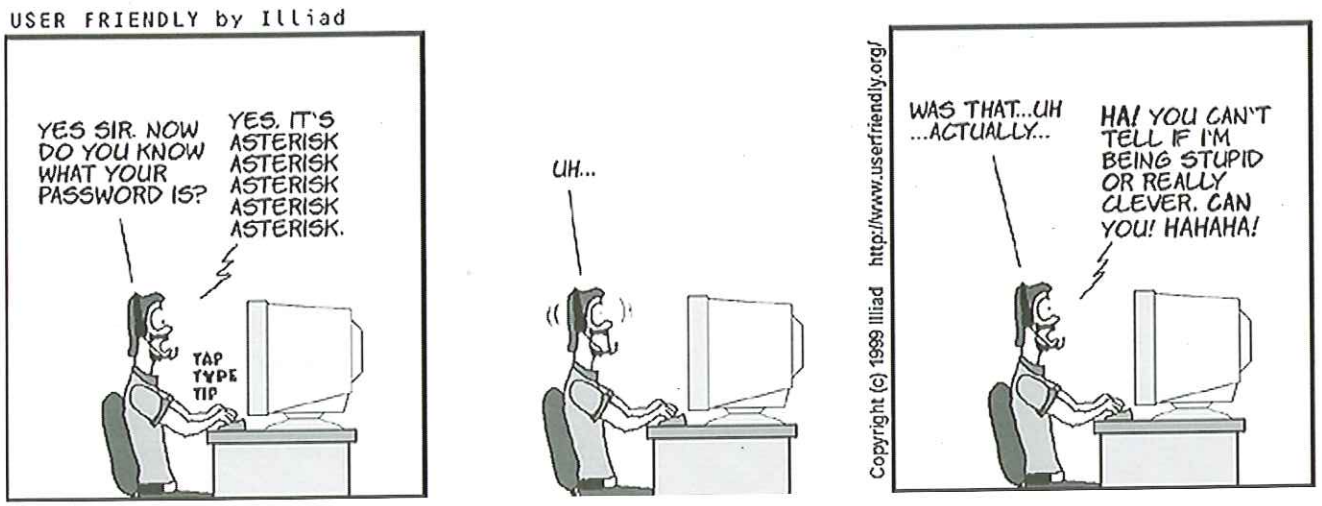
```
  Loaded 1 password (FreeBSD MD5
[32/32])
  abc              (robin)
  guesses: 1  time: 0:00:00:04 100%
(2)  c/s: 837  trying: abc

  Loaded 1 password (FreeBSD MD5
[32/32])
  apple            (robin)
  guesses: 1  time: 0:00:00:03 100%
(2)  c/s: 891  trying: apple

  Loaded 1 password (FreeBSD MD5
[32/32])
  appleapple       (robin)
  guesses: 1  time: 0:00:00:19 100%
(2)  c/s: 710  trying: appleapple
```

Shadow files

Den almindelige password-fil, /etc/passwd, kan læses af alle. Dette er nødvendigt, da en del programmer bruger filen til at koble en brugers bruger-id (tredie felt i password-filen) med det



tilhørende brugernavn. At alle kan læse filen betyder imidlertid også, at alle kan se dit krypterede password. Derfra kan man cracke dit password, og som vi har beskrevet, så kan det gøres hurtigt, hvis du har valgt et svagt password. Med flere Linux distributioner bl.a. Red Hat 6.0 bliver du ved installationen spurgt, om du vil anvende shadow passwords, hvilket du bør svare ja til. Når du har installeret dette, så vil du se, at der står et x i /etc/passwd, hvor dit krypterede password før ville have stået:

```
robin:x:501:501::/home/robin:/bin/bash
```

Dit krypterede password er nu flyttet til /etc/shadow, som kun kan læses af root - dvs., ingen almindelig bruger på maskinen nu kan læse dit krypterede password. Hvis du har installeret Linux, men ikke har shadow passwords slået til, kan det gøres med kommandoen /usr/sbin/pwconv, som skal køres som root. Den laver shadow filen ud fra password filen og tilsvarende laves en shadow gruppe-fil /etc/gshadow ud fra /etc/group med programmet /usr/sbin/grpconv. For at dette virker, skal dine Linuxprogrammer være oversat til at kunne håndtere dette - tidligere var dette ikke altid tilfældet. Læs manualsiden for pwconv for detaljer.

I det ovenstående, hvor vi skriver, at alle kan læse password-filen, går vi ud fra, at det er brugere med lokal adgang. Hvordan får en cracker udefra adgang til min password-fil, så han kan se mit krypterede password? Ofte er det CGI-scripts på en web-server, som pga. simple programmeringsfejl eller pga. fejl i de anvendte programmeringssprog kan lokkes til at vise de krypterede passwords fra password-filen. Dygtige crackere finder fra tid til anden nye metoder til at gøre dette. Normalt findes tilsvarende rettelser til disse huller - hold derfor altid din maskine opdateret.

SUID root programmer

SUID betyder, at et program kører „som sin ejer", og ikke „som" den bruger, der udfører det. Dvs. at det kører med ejerens rettigheder. Et program, som robin ejer, og som er SUID, har f.eks. ret til at skrive i robins hjemmekatalog, selvom det er en anden bruger, der eksekverer det. Et SGID program er det samme bare med gruppe rettigheder i stedet.

Hvorfor er det farligt? SUID er specielt farligt, når det er et SUID-program som root ejer. Så længe programmet opfører sig pænt, er det ikke noget problem. Men hvis der er fejl eller sikkerhedshuller i programmet, kan det være en trussel mod sikkerheden. Man kan forestille sig, at et program har et sikkerhedshul, som gør det muligt for en almindelig bruger at gå ind og overskrive noget af programmets hukommelse, imens det kører, og få det til at gøre noget andet, end det skal. Så har denne bruger faktisk root adgang til systemet. Man har set eksempler på dette med efterfølgende sikkerhedsopdateringer til følge.

Lad os nu se på hvilke programmer, der på en normal Linux maskine er SUID programmer.

```
[robin@sherwood robin]$ su - root
[root@sherwood root]$ find / -perm +4000
```

Sådan finder du alle SUID programmer. Men det er kun SUID root programmer, som vi vil være bange for i dag. Hvis andre brugere selv laver SUID programmer så lad os antage, at de ved, hvad de laver og selv tager eventuelle konsekvenser. Vi går nu efter de programmer, hvor root er ejeren og som er SUID. Så vi tager parametrene „-user root" med til find komman-

doen:

```
[robin@sherwood robin]$ su - root
Password:
[root@sherwood robin]# find / -
perm +4000 -user root
/bin/ping
/bin/mount
/bin/umount
/bin/su
/bin/login
/sbin/dump
/sbin/restore
/sbin/pwdb_chkpwd
/sbin/cardctl
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/at
/usr/bin/dos
/usr/bin/chage
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/passwd
/usr/bin/suidperl
/usr/bin/procmail
/usr/bin/screen
/usr/bin/nwsfind
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/zgv
/usr/bin/gpasswd
/usr/bin/sperl5.00405
/usr/X11R6/bin/xterm
/usr/X11R6/bin/XConsole
/usr/X11R6/bin/nxterm
/usr/X11R6/bin/xscreensaver
/usr/X11R6/bin/Xwrapper
/usr/lib/news/bin/startinnfeed
/usr/local/bin/ssh1
/usr/sbin/usernetctl
/usr/sbin/inndstart
/usr/sbin/sendmail
/usr/sbin/traceroute
/usr/libexec/pt_chown
find: /proc/1144/fd: Permission
denied
find: /proc/1145/fd: Permission
denied
find: /proc/6286/fd/4: No such
file or directory
/opt/kde/bin/kvt
/opt/kde/bin/kppp
```

Outputtet er de SUID root programmer, der findes på systemet. Der er også et par fejl fra find nede fra /proc kataloget. Det skal du ikke tage dig af, /proc er et interface til den kørende kerne, og der ligger ikke almindelige filer (f.eks. SUID root programmer) der. Det er mange programmer at passe på, måske er der et sikkerhedshul i nogle af dem. Har du brug for alle disse programmer? Er der mon nogle af dem, der kan køre uden SUID root eller helt fjernes? Check programmernes man page, check om andre programmer er afhængige af SUID-programmet, som det f.eks. er tilfældet med /bin/su. Det kan ofte undersøges med systemets pakkemanager. Er der sikkerhedsopdateringer til nogle af programmerne, du burde installere? Kan du overskue at følge med sikkerhedsopdateringer for alle disse programmer? Konklusionen er, at du aldrig skal installere flere programmer, end der skal bruges.

SGID - set group ID - er også farligt, hvis gruppen er root. Det er ikke så almindeligt at anvende SGID

```
[root@sherwood robin]# find / -
perm +2000 -group root
/sbin/netreport
/usr/sbin/sendmail
find: /proc/1144/fd: Permission
denied
find: /proc/1145/fd: Permission
denied
find: /proc/6296/fd/4: No such
file or directory
```

Der var ikke så mange, men dem skal man også være opmærksom på.

Lad os som et eksperiment prøve at lade /bin/ping være ejet af robin i stedet for root, og lad os se om den stadig virker:

```
[root@sherwood robin]# ls -l /bin/
ping
-rwsr-xr-x 1 root root 14116 Jun
18 1998 /bin/ping
[root@sherwood robin]# chown robin
/bin/ping
[root@sherwood robin]# ls -l /bin/
ping
-rwsr-xr-x 1 robin root 14116 Jun
18 1998 /bin/ping
[root@sherwood robin]# ping
10.10.10.3
ping: ping must run as root
[root@sherwood robin]#
Ups, det kunne man ikke. Vi må
hellere skifte tilbage:
[root@sherwood robin]# chown root
/bin/ping
```

Programmet ping er svært at undvære og er nødt til at køre som SUID root. Du kan i øvrigt se, at det er SUID ved det „s" som kommer frem, når du kører ls -al på filen. Programmet /usr/bin/passwd er svært at undvære, og det er nødt til at køre som root for at kunne ændre i /etc/passwd filen. Et program som kppp kunne derimod afinstalleres, hvis du ikke bruger det. Kppp er et KDE program, der bruges til at koble sig til

Internet via modem. Tilsvarende kan du afinstallere /sbin/cardctl, hvis du ikke har PCMCIA kort i din maskine. Anvender du en RPM baseret Linuxdistribution såsom Mandrake, SuSE eller Red Hat, kan du have glæde af at finde ud af fra hvilken pakke, et givent SUID program kommer fra.

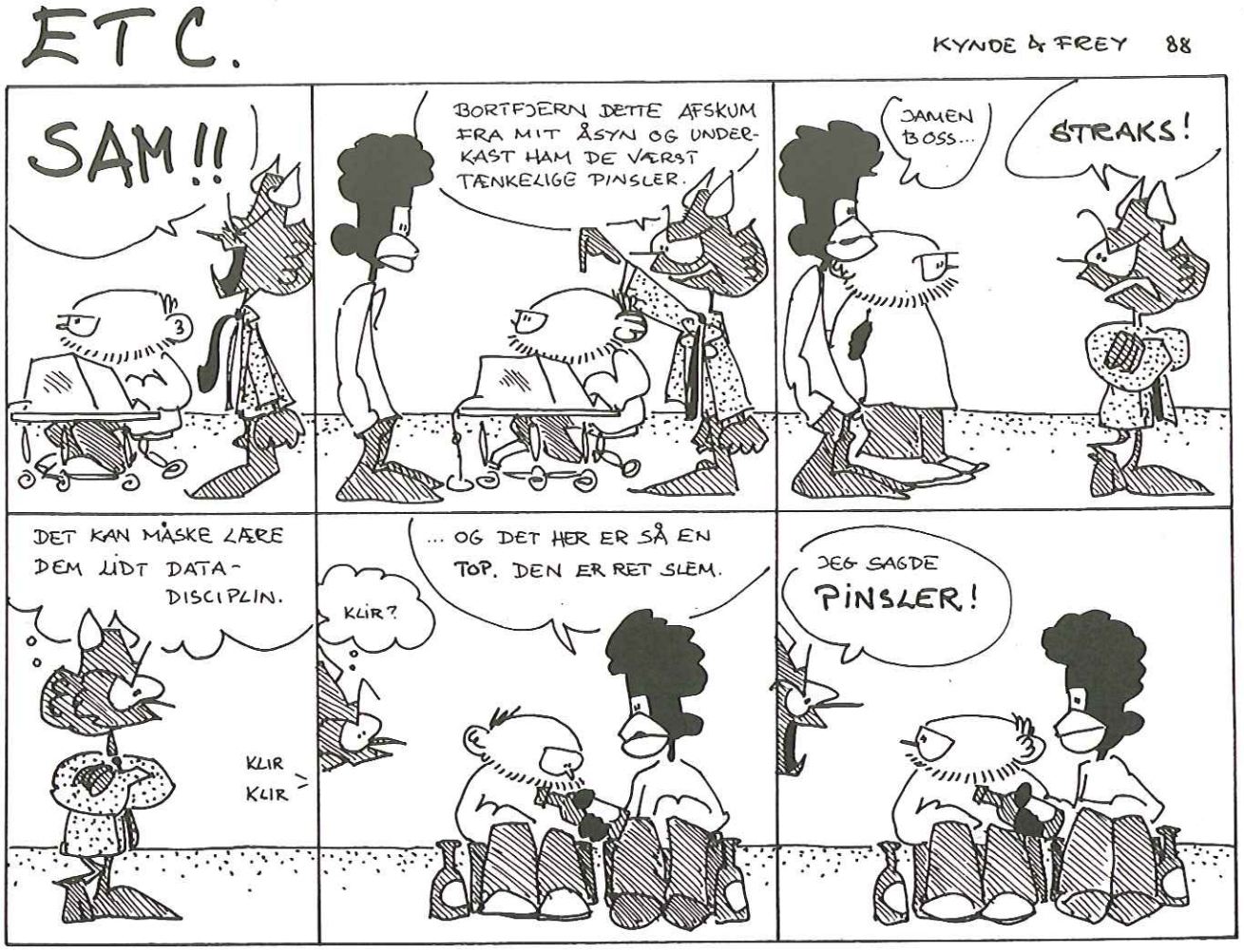
```
[root@sherwood root]# rpm -qf /
sbin/cardctl
  kernel-pcmcia-cs-2.2.5-15
```

Så kan du checke hvilke filer, pakken indeholder. Når du frem til, at pakken ikke bruges, så afinstaller den:

```
[root@sherwood root]# rpm -ql
kernel-pcmcia-cs-2.2.5-15
  ...klip mange linier
  [root@sherwood root]# rpm -e
kernel-pcmcia-cs-2.2.5-15
```

SUID root programmer er en alvorlig sikkerhedsrisiko, og man bør i hvert fald ikke lave SUID root programmer selv for at løse en given opgave. Der er ting man ikke har fundet smartere løsninger på endnu, men de fleste ting kan gøres uden. I Linux har man som en sikkerhedsforanstaltning overfor SUID root programmer indbygget, at et script (tekstfil med kommandoer) ikke kan køres som SUID root.

Hele artikelserien om netværkssikkerhed som kan findes på http://www.sslug.dk/artikler/Linux_sikkerhed



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

Deadline:
Deadline for næste nummer nr. 121 er fredag d. 25. februar 2000

Medlem af Dansk Fagpresse

DKUUG-Nyt
ISSN 1395-1440

Aktivitetskalender

Februar:

7. KLID
Gå-Hjem-Møde m. Bjarne Stroustrup

8-11: NordU2000

8.: Klub Odense: Richard M. Stallman

Marts:

4. Linuxforum 2000

Maj:

2. Internationale SANE-konference

Se www.dkuug.dk for nærmere oplysninger

Afholdte arrangementer i 2000

Januar:

11. Hyggemøde på Niels Bohr Instituttet

11. Møde i Klub Odense:
Oracle giver øl

17. Klub København:
GnuPG med Werner Koch

18. NBD:
Netware 5.1 lancering Århus

19. *SILD:*
E-commerce m. BEA

20. NBD: Netware 5.1 lancering Kbh.

25. Klub København:
FreeBSD m. Klub København

25. Klub Århus:
Hyggemøde

Pers hjørne

Katastroferne, der udeblev

Så fik vi da endelig Nytårsaften overstået og kunne se, hvor mange – eller rettere sagt hvor få – problemer, der egentligt opstod. Hvor må det være pinligt for de mange konsulentfirmaer, der havde malet fanden på væggen i årevis. Og hvor er jeg glad for, at jeg hele tiden har anbefalet at slå koldt vand i blodet.

Hvad skete der så? IDC fulgte gennem Projekt Magellan udviklingen hele nytårsnat og dagene efter over hele verden, og indberetninger af problemer var ganske få. Et omstillingsbord ved Scotland Yard gik ned. En pumpestation i Tyrkiet fik fejl, der dog hurtigt blev rettet igen. På Hawaii gik fjernsynsforbindelsen til hovedlandet ned. Nogle spillemaskiner holdt op med at fungere. Enkelte kortvarige strømafbrud.

Det interessante er imidlertid, at der INGEN korrelation er imellem investeringerne i Y2K løsning og problemerne nytårsnat. Det ved IDC, fordi vi har analyseret disse investeringer i årevis. Sagt på en anden måde: Lande med meget lave Y2K investeringer havde ikke specielt mange problemer i forhold til lande med meget store Y2K investeringer.

Dette var blandt andet baggrunden for IDC's analyser, der viser, at vi i Danmark har anvendt 25-30% for meget på Y2K problemerne – eller omsat i penge omkring kr. 5 mia. for meget. En udtalelser, der er blevet mødt med megen kritik – specielt naturligvis fra de firmaer, der har levet af at løse problemerne for folk. Hvad kunne man ellers forvente.

Hvad har modargumenterne været? Ja, lad mig lige nævne et par stykker:

- "Jamen, pengene har været givet godt ud, for vi har fået fx nyt software og fået chekket vores systemer". Svar: Ja, det er jo derfor vi siger, at 70-75% af pengene har været givet godt ud – det er de sidste 25-30% vi hævder ikke er givet godt ud.
- "Jamen, hvis vi ikke havde gjort så meget, havde vi haft store problemer". Ikke korrekt, idet vores analyse netop viser, at lande med lavere investeringer ikke havde væsentligt flere problemer.
- "Jamen, det er jo en forsikring – ingen kunne jo vide hvor slemt det ville blive". Korrekt, men det er jo en risikovurdering. IDC har hele tiden hævdet, at man har "overforsikret" fordi man har vurderet risikoen langt højere end den reelt har været. Vi lever jo blandt andet af at komme med sådanne risikovurderinger.

Det skal tilføjes, at omkring 1/3 af overforbruget på Y2K er blevet anvendt selve nytårsnat på at have et stort beredskab, folk på arbejde eller vagt og diverse nødplaner og nødforsyning på plads. Det er altså langt fra hele overforbruget, der relaterer sig til problemløsninger på konkrete systemer.

På et andet punkt fik jeg også ret. Dommedagsprofeter tager nemlig pr. definition aldrig fejl – de finder altid et godt argument for, hvorfor deres profeti ikke gik i opfyldelse, og for Y2K forudsagde jeg, at konsulenter ville stå frem og påstå, at årsagen til de manglende katastrofer nytårsnat var deres rådgivning om at få løst problemerne.

Og det er netop, hvad der er sket. Uden at de har skygge af dokumentation for, at hvis man i Danmark ikke havde anvendt næsten 20 mia. kr. på Y2K, men noget mindre, så ville landet være gået i stå nytårsnat.

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.

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

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".