DKUUG-N

Nr. 103 — maj 1998

Kryptering

DKUUG-Nyt belyser emnet kryptering fra flere forskellige vinkler:

- Kryptering for dummies
- Implementation af kryptering i FreeBSD
- Hewlett-Packard's VerSecure
- Optakt til kursus med Bruce Sneier

Manden bag forsiden

Hvem er det egentlig der laver DKUUG-Nyts karakteristiske forsider? Vi bringer et portræt af Erik Werner

Indhold

Kryptering for fuld udblæsning

Når du sidder og læser disse linier, sidder du med nøglen til en masse viden om kryptering. Uden at DU behøver en nøgle til at afkode denne viden. Vi har leveret denne viden som "en åben bog", og du er mere end velkommen til at lade andre læse indholdet, når du selv engang er færdig.

Det er selvfølgelig med fuld overlæg.

Der er imidlertid situationer, hvor du ikke ønsker, at andre end lige én bestemt modtager skal læse det, du sender elektronisk til en anden. Derfor kommer kryptering ind i billedet som en vigtig parameter. Lige som al anden udvikling indenfor IT-verdenen, så går udviklingen indenfor kryptering også meget stærk.

I dag tager det kun millisekunder at bryde en 40 bit kryptering. Der skal mindst en 128 bit kryptering til, førend det begynder at ligne noget. Men der er jo lige et "men", hvis man ser det fra

myndighed
med at det
afkode en
ver det ogs
myndighed
med over s
er det forbu
portere en
længere en
flere steder
den arbejd
nøgle på 1
sigende sk
gange så m
kraft for at

En af de
som har ta
amerikansk
dette områ
Bruce Schn
des DKUU
med UniFo
USA at få
Danmark f
dages kurs
her i maj m
chance, da
meget efter
land og der
grænse sin

René Esper

BEA Systems

Nu 1 år i Danma

BEA Systems Inc er anerkendt som verdens
middleware til transaktionskritiske distribuere
globale organisation består af 800 medarbejdere
mere end 20 lande. I samarbejde med vore part
rådgivning til mere end 1.000 kundevirksomhede
kunderne maksimalt udbytte af deres investeringe

Vi har nu virket i Danmark i 1 år og vores kun
andet SAS Data, DSB Data, Post Danmark,
Alta Copenhagen og DEFU Data.

Tak for opbakningen og

LØSNINGSEKSEMPLER:

En bank ønskede at tilbyde sine kunder Internet-adgang til mainframe-baserede data uden omskrivning af applikationer. Samtidigt udviklede man nye applikationer baseret på Windows NT, og disse applikationer skulle have adgang til eksisterende proprietære database-data.
Løsningen: BEA TUXEDO, Connect, Jolt.

En europæisk offentlig administration rådede over hundreder af forskellige UNIX servere og adskillige mainframes, som det var nødvendigt at integrere for at give organisationens mere end 20.000 medarbejdere adgang til centrale applikationer og data.
Løsningen: BEA TUXEDO.

En førende bank har valgt et objektorienteret udviklingsværktøj som et middel til at reducere udviklingstiden for nye kunderettede ydelser. Banken har behov for at sikre sammenhængende kommunikation og administration.
Løsningen: BEA ObjectBroker.

DKUUG
IT-FORENING

BEA

THE ENTERPRISE MIDDL

BEA Systems Danmark
Emdrupvej 28 C
2100 København Ø
Telefon 39270208
e-mail: info@beasys.dk

www.beasys.dk/www.beasys.co

Kryptografi for dumn

Af Flemming Jacobsen

Kryptografiske algoritmer findes i to hovedvarianter: symmetriske og asymmetriske, også kaldet private-key og public-key algoritmer.

Symmetriske algoritmer er de bedst kendte. Her benytter afsender og modtager den samme nøgle til at kode og afkode med. Den nok bedst kendte symmetriske algoritme er DES.

Asymmetriske algoritmer har to nøgler. Disse kaldes oftest den private og den offentlige nøgle. Hvad der er kodet med den privat nøgle, kan kun afkodes med den offentlige nøgle og omvendt. Den bedst kendte asymmetriske algoritme er RSA.

Den største forskel på symmetriske og asymmetriske algoritmer er den hastighed, hvormed de kan kode og afkode meddelelser og de muligheder, de giver udover kryptering.

Symmetriske algoritmer er langt de hurtigste (software implementeringer af DES er 100 gange hurtigere end RSA), tilgengæld giver de kun mulighed for, at afsender og modtager kan kommunikere uden, at andre kan læse indholdet af meddelelserne, samt at modtageren er sikker på, at meddelelsen er

afsendt af
talt med. N
af nøgler e
med symm
mer. Hvis
kommunik
kræver det
ker måde b
nøgler.

Asymme
giver, ud o
ligheder so
goritmer, m
le signatur
væsentligt
stribution.

To parte
haft muligh
nøgler i he
kommunik
to parter s
den deres
Eftersom d
er beregnet
distributio
get, at udv
aflyttet. Ku
mulighed f
nøgler, der
muligt at k

kerheden.

Brug af en asymmetrisk algoritme er meget lig brugen af en symmetrisk algoritme. Afsenderen (kaldet A) koder meddelelsen med modtagerens (kaldet M) offentlige nøgle. M afkoder meddelelsen med sin private nøgle (M afkoder altid med sin private nøgle, uanset hvem der modtages meddelelser fra).

I modsætning til når en symmetrisk algoritme benyttes, så har M ingen garanti for, at det nu også var A, der afsendte meddelelsen (i princippet har alle adgang til M's offentlige nøgle). Dette problem løses ved, at A laver en digital signatur på meddelelsen inden afsendelsen.

Digitale signaturer laves som regel ved, at der beregnes en checksum for den meddelelse, der skal signeres. Afsenderen koder checksummen med sin hemmelige nøgle. Modtageren verificerer, at checksummen kan afkodes med A's offentlige nøgle, og at den er den samme som checksummen for den meddelelse, der blev modtaget. Er dette tilfældet, så ved M at checksummen er blevet kodet med A's hemmelige nøgle (der kun kendes af A), hvorfor det kun er A, der har kunnet signere meddelelsen.

Problemet med den meget langsomme kodning/afkodning, når asymmetriske algoritmer benyttes, løses som regel ved at kode meddelelsen med en symmetrisk algoritme og en (for hver meddelelse) tilfældigt valgt nøgle. Denne nøgle kodes så med den asymmetriske algoritme, og resultatet sendes med som en del af meddelelsen. På denne måde opnås hastighed svarende til en symmetrisk algoritme samtidigt med, at alle fordelene ved de asymmetriske algoritmer bevares.

Sikkerheden holder naturligvis kun, hvis algoritmen ikke er blevet brudt, og hvis nøglen ikke er blevet gættet. Hvordan sikrer man sig rimeligt mode dette?

For det første skal man sikre sig at der er brugt en stærk/sikke
Dette er van
man umidde
For den ikke
ligner outpu
algoritme til
put fra en sv
Begge dele e
tilfældigt/m
ende data. F
onelle er der
forskel - ogs
ikke vides, h
me der er br
algoritme fin
tede genveje,
man ikke be
nøglen for at
lelsen, eller
let bestemm
kodede medd
sikre algorit
således, at d
lighed, der e
krypteringen
nøglen. Der
diskussion a
algoritmer o
og svaghede
mer, der ikke
goritme, der
i [1], bør ikk
øst - specielt
geren nægte
hvilken algo

nyttet (se [2]).

Man kan kun undgå, at nøglen bliver gættet (dvs. fundet ved systematisk at prøve alle muligheder) ved at gøre antallet af mulige nøgler tilstrækkeligt stort. Det store spørgsmål er: Hvad er "tilstrækkeligt stort" ? Dette afhænger af, hvad man ønsker beskyttet, og hvor længe man ønsker det beskyttet. Hvis vi antager, at meddelelsen ønskes beskyttet i min. 20 år, og at andre vil have stor økonomisk eller politisk gevinst af at afkode meddelelsen, kan vi se på hvor lang en nøgle minimum skal være. [1] diskuterer dette, og når frem til at for symmetriske algoritmer er 40 bit nærmest latterligt lidt mens 112-128 bit er rimeligt. For asymmetriske algoritmer er 1024 bit i underkanten, 2047 bit er et mere realistisk bud.

Konkurrencer på nettet har vist, at en lille gruppe kan gætte en 40 bit nøgle på en uges tid ved at benytte den overskydende CPU kraft i de computere, gruppen har adgang til. Mere dedikerede forsøg har fundet 40 bit nøgler på nogle timer, blot ved at benytte et par hundrede workstations.

Forordet til [1] starter med: "There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop a major government from reading your files". 40 bit nøgler hører til den første type...

Desværre er det svært at finde kommercielle programmer, hvor nøglen i den symmetriske algoritme er tilstrækkelig lang. Dette skyldes, at USA stadig sidestiller eksport af kryptografisk software med eksport af våben. Det er så godt som umuligt at få en generel eksporttilladelse, hvis den effektive længde af nøglerne er over 40 bit.

Alle de kryptografiprogrammer og postsystemer med indbygget kryptering, der er udviklet i USA, og som kan købes af almindelige mennesker i resten af verden, benytter derfor 40 bit nøgler.

Det bedste kryptografi

program, c
nyttet, og
en fornufti
PGP. PGP
des til stor
systemer.
hentes hos
grammer t
har indbyg
af PGP, sål
afkodning
turer ikke
tra af brug

Et ande
mercielle p
den benytt
ikke er sik
behandlere
mer med e
hed for at
ment. Desv
for langt st
se, at man
programme
ware eller
kan finde
mentet på
geren er så
end hvis de
tet krypter
nu tror, at
sikret, men
er, at alle ,
læse indho

Netscap

eksportversionen også begrænset til at benytte 40 bit nøgler. Hos [4] kan man dog hente et patch, der får den til at benytte 128 bit nøgler. Dette er endnu et eksempel på, hvor absurd USAs eksportlovgivning på kryptografi området er.

Selvom der benyttes en stærk algoritme med en tilstrækkelig lang nøgle er sikkerheden ikke nødvendigvis i orden.

Hvis nogen formår at stjæle en kopi af en hemmelig nøgle, så er vedkommende i stand til at lytte med. Dette er især et problem, hvis tyveriet er foregået ubemærket. Skulle tyveriet være blevet bemærket, så vil et nøgleskift ikke forhindre tyven i at afkode tidligere meddelelser.

Selvom et dokument er sikkert krypteret, så kan det stadig slettes. Derfor er almindelige sikkerhedsprocedurer lige så vigtige som før.

Betroede personer kan stadig læse fortrolige dokumenter. Bestikkelse og afpresning er stadig en nem måde at få kopier af dokumenter og nøgler.

Sløset omgang med dokumenter, og almindelig glemsomhed kan stadig føre til at udenforstående får adgang til hemmeligheder. Dette er især muligt, hvis ikke alle kender/anerkender firmaets politik om brug af kryptografi.

Selvom indholdet af en meddelelse er krypteret, så er det sommetider muligt for andre at bruge det, at der / er/ blevet sendt en meddelelse. F.eks. kunne krypterede meddelelser mellem to, der mistænkes for at have et forhold antyde, at der er hold i mistanken.

Hvis nogen ønsker at læse yderligere om teorier og principper bag den moderne anvendelse af kryptografi, kan [1] kun anbefales. Den fungerer både som en interessant introduktion til emnet samt som den for øjeblikket mest definitive reference på området. Bogen er både underholdende og (i betragtning af emnet) meget let læst. Indholdet i bogen kan opdeles i: Introduktion til kryptografi, krypto-

grafiske prot
de kan bruge
grafiske tekn
der, diskussi
velse af forsk
mer, brug af
den virkelige

Noter

[1] Schneier,
Applied Cry
Second Edi
Wiley & Son
0-471-1170
[2] Curtin, M
Warning Si
tion Softwa
http://www
net/people/
snake-oil-fa
[3] The Inter
Home Page
http://www
[4] Farrell Mc
Systems Pty
http://www

Sådan bruges krypto

Bruce Schneier står i spidsen for fortroppen, når det gælder hed. DKUUG har fået ham til København, hvor han vil hold kursus om kryptering.

Kurset med titlen "Introduction and Advanced Cryptography" afholdes i Symbion den 25.-26. maj. Det henvender sig til dem, der vil forstå kryptografi: hvad det gør og hvordan det virker. Bruce Schneier vil fokusere på teknologien bag kryptering, hvorfor der ikke forudsættes nogen stærk baggrund i matematik hos deltagerne for at få et stort udbytte af kurset.

Fra omsætning af kode til digital signatur til elektronisk handle til sikker afstemning - kryptering er blevet den teknologi, der sætter os i stand til at tage de eksisterende forretninger og sociale interaktioner og flytte disse til computer netværket. Men meget af krypteringen er dårlig og problemet med dårlig kryptering er, at det ligner en god kryptering. De fleste kan da heller ikke se forskel.

Sikkerheden er som en kæde - den er ikke stærkere end det svageste led.

Kurset vil omhandle kryptering som det bruges i hverdagen: algoritmerne, protokollerne og implementationerne. Bruce Schneier vil på kurset understrege "hvad" og "hvordan" mere end "hvorfor". Folk der opbygger - eller bruger - kryptering har ifølge Bruce Schneier brug for at forstå, hvad kryptering kan gøre og ikke kan gøre - kryptering er nemlig ikke altid det universalmiddel, som det oftest præsenteres som.

Følgende emner vil blive behandlet:

- Fundamentalt kryptografi
- Symmetrisk kryptografi: DES, triple-DES, IDEA, Blowfish, RC2, RC4, RC5 og AES
- Public-k
  Omsætn
  tal signa
  Hellman,
- Hash fun
  lelsens æ
  MD4, MI
  MAC, HM
- Random
  tion
- Protokoll
  ling, ægt
  deling, n
  certifikat
  tanter
- Hvad kry
  for dig
- Hvad kry
  gør for di
- Kryptogra
  netværk
- Redskabe
  kryptogra
- Threat M
- E-Mail sil
  MIME

- Trust Management: X.509, SDSI, SPKI
- IP Sikkerhed
- World Wide Web sikkerhed
- Elektronisk Handel:: Cybercash, Digicash, First Virtual, SET

Bruce Schneier understreger, at han som "enlig" instruktør ikke kan lære deltagerne at blive kryptografer. Men efter at have gennemgået dette kursus, så vil deltagerne blive intelligente forbrugere af kryptografi, der vil forstå kryptografiens byggestene, hvordan disse byggestene sættes sammen for at danne et kryptografisk system, og endelig hvilke begrænsninger denne teknik har.

Lidt om Bruce Schneier

Bruce Schneier er direktør for Counterpane Systems - et konsulentfirma med speciale i kryptografi- og computersikkerhed. Bruce Schneier er forfatter til en række bøger, hvor den bedst kendte nok er "Applied Cryptography" (John Wiley & Sons, 1994 & 1996). Den anden udgave af denne bog er allerede blevet solgt i over 80.000 eksemplarer verden over. Den er oversat til fire forskellige sprog. Han har desuden skrevet dusinvis af artikler om kryptografi til de alle de store magasiner om IT-teknologi.

Bruce Schneier har desuden designet den populære "Blowfish encyrption algorithm", som nu efter fire år stadig ikke er blevet brudt.

Praktiske oplysninger

Kurset afholdes som nævnt den 25.-26. maj i Symbion, Fruebjergvej 3, 2100 København Ø. Prisen er kr. 6.000 for medlemmer af DKUUG, mens ikke-medlemmer må betale kr. 8.500. Priserne er ekskl. moms.

Tilmelding skal ske til DKUUG's sekretariat, tlf. 39 17 99 44, fax 39 20 89 48 eller e-mail sek@dkuug.dk senest den 20 maj 1998.

❑

Den V Verde

En teknike kunde det putte hans ind i dreve Kunden ba "blive i røre nikeren ku lægge røret gå til den a relset for at værelset.

En anden I de for at sig kunne få si faxe noget 40 minutte uden held, keren, at ku faxe et styk holde det fo og trykke p

Danmark importerer s kryptering fra USA

Hewlett-Packard har fra den amerikanske regering opnået t Danmark for første gang må importere produkter til stærk k bit) fra USA. Danmark er blandt de 5 første lande i verden, denne tilladelse.

HP's nye teknologi til kryptering, VerSecure™, giver danske virksomheder og forbrugere nye unikke muligheder for at udveksle data sikkert på Internettet. Eksempelvis kan danske borgere nu kommunikere sikkert med det offentlige og sende personlige data over Internettet uden at bekymre sig om, at informationerne kan blive aflyttet eller opsnappet undervejs.

Den manglende sikkerhed på Internettet er hidtil blevet opfattet som den største barriere for en udbredt, kommerciel anvendelse af Internettet. Men HP's VerSecure teknologi giver mulighed for uhyre sikker kommunikation og kan f.eks. anvendes til sikker elektronisk dataoverførsel, overenskomst- og politiske forhandlinger via Internettet, militære oplysninger, finansielle transaktioner, udveksling af sensitive sociale oplysninger, EDI, digitale signature, medicinske- og lovmæssige informationer samt afsendelse af private beskeder via e-mail.

- Tilladelsen til at importere VerSecure teknologien betyder, at den elektroniske verdens muligheder nu kan udnyttes fuldt ud også i Danmark, siger administrerende direktør, Jørgen Bardenfleth, Hewlett-Packard Danmark.

HP's Ve
ringsteknc
fået tilslut
nationale
re inklusiv
Motorola,
og Trustec
stems.

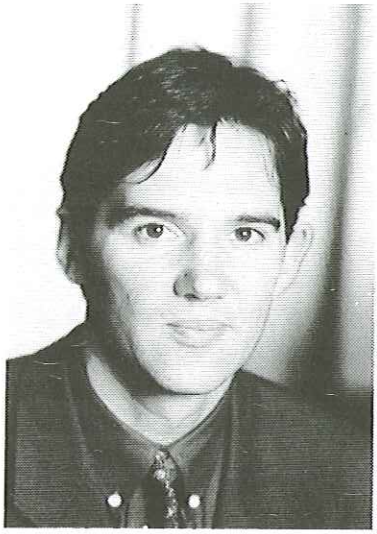
Danmar
med Int

Danske vi
ligheder fo
sikkert på
lang tid va
amerikane
at eksport
inkluderer
Det er ænd
delsen af H

Danmark er sammen med Tyskland, Frankrig, England og Australien de første lande, der har fået mulighed for at importere VerSecure baserede produkter.

- HP's danske kunder har længe udtrykt et stort behov for stærk kryptering så de bedre kunne udnytte mulighederne i E-business. Efter vi for første gang blev opmærksomme på VerSecure, har vi i HP Danmark presset hårdt på for at få VerSecure til Danmark hurtigst muligt. Da Danmark samtidigt betragtes som et IT-foregangsland, kom vi med i første bølge, siger Internet programchef Henrik Hvid Jensen, Hewlett-Packard Danmark.

- Det er glædeligt, at de amerikanske myndigheder nu har erkendt, at man også udenfor USA har brug for stærk kryptering i forbindelse med brug af amerikanske IT-produkter i overensstemmelse med en national politik og ikke kun en amerikansk. Det er en fjer i hatten til både Hewlett-Packard og Danmark, at vi



Internet programchef Henrik Hvid Jensen, Hewlett-Packard Danmark.

er med blandt de allerførste lande, som får adgang til dette, siger professor Peter Landrock, Ph.D. og administrerende direktør i Cryptomathic.

VerSecure er designet til at give den fleksibilitet, som adresserer disse bekymringer, idet teknologien tilbyder en arkitektur, som kan tilpasses ændringer i en nations krypteringspolitik. Hvis man i Danmark på et tidspunkt vælger at indføre restriktioner omkring brug af kryptering, kan disse ændringer aktiveres ved blot

at kopiere ny
VerSecure ko
via Internett
måtte man fo
fattende re-p
af software s
re denne elle
skifte hardwa

Detaljeret
om HP's VerS
gi findes på H
VerSecure hj
adressen: ww
versecure

Historien om en password scra

Af Poul-Henning Kamp
<phk@FreeBSD.org>,
The FreeBSD Core team.

Poul-Henning har hærget den danske UNIX branche i mere end elleve år. Han arbejder som freelance konsulent med eget firma og har slet ikke tid nok til FreeBSD nu om dage.

Egentlig skylder jeg læserne en fortsættelse af "FreeBSD, The Inside Story X/N" men jeg kan faktisk ikke huske, hvad nummer vi er kommet til...

Denne klumme er foranlediget af temaet for dette nummer: Kryptering.

Gode dyr var rådne

For nogle år siden, i 1994 faktisk, stod FreeBSD projektet med et problem: Vi kunne ikke distribuere den "sædvanlige" DES baserede password scrambler fordi sourcen naturligvis ville indeholde en fuld DES implementering, og sådan noget må man jo ikke eksportere fra USA. "Almindelige" UNIX leverandører havde det nemmere, de distribuerede ikke sourcen og derfor kunne de få en ITAR licens idet man ikke kunne få fingre i den indlejrede DES rutine.

Gode dyr var rådne, som man siger, vi havde en rudimentær scramble routine, men den var klappet sammen i hast, for i det mindste at undgå at skrive password i klartekst i /etc/passwd, men den var utroligt dårlig, og havde hvis jeg husker ret det meste af en invers algoritme.

Vi havde ganske vist en fuldt funktionsdygtig og kompatibel implementering liggende klar til download fra Sydafrika, men det ville jo ikke hjælpe dem, der ikke havde InterNet adgang, og slet ikke dem der købte en CDROM.

Nød lærer nøgen...

Således frustreret satte jeg mig ned og begyndte at rode med det, og resultatet forelå den 7. nov
ny passwo
ret på MD5

Forud fo
mange tim
følgelig hav
kode samm
ternational
Code Cont
men det vil
pe os. Sikl
get man fu
kræver om
udemærke
ikke har hv
den eller e
bide skeer
nelle på de
der var jo h
til at opfin
og den var
gang mere.

Algoritm

I stedet bes
at basere k
de eksister
MD5. MD5
terings algo
det er en "h
det vil sige,
antal bytes

en "signatur" ud. Der er ingen kendt metode til at komme fra signaturen til input andet end at prøve sig frem fra ende til anden.

Det er omtrent perfekt til password beskyttelse. Man gemmer signaturen, hvis det password som brugeren taster ind giver samme signatur, som den man har gemt, kendte hun det rigtige password.

Dette var også princippet i den traditionelle DES baserede passwordscrambler, men der brugte man en DES som hash algoritme ved bl.a. at køre de samme data igennem mange gange. For at gøre det lidt sværere har man tilføjet et "salt" på 12 bit, som modificerer nogle parametre i algoritmen, det øger med en faktor 4096, den tid et brute-force angreb vil tage.

Desværre er de 12 + 56 bits ikke ret meget med moderne cpu-kraft. (http://www.distributed.net) og hvad der er endnu værre, det er så lille et udfaldsrum, at man kan forudberegne en ordbog.

FreeBSD

Tag f.eks
DLT bånd.
GB ukompr
det modsva
word+salt=h
oner, og ma
sammenlign
de per seku
bliver noget
man anven
mering.

Til samm
der kun 2^2
nummerpla
det normale
mat.

Det var v
riøst proble
crackere, hv
til de scram
words, ville
og forsøge s
force eller d
greb. Cliff S
f.eks. om et
"The Cucko

Valget af
ret på mang
blandt copy
port lovgivn
der var nogl
egenskaber
opfyldt også
met skulle v
sentlig størr

le være svært eller umuligt at optimere algoritmen både i HW og SW. Alle disse ting pegede på MD5, se f.eks. RFC1810 vedr. hastigheden.

Antallet af "salt" bits blev øget til 48 og selve det scramblede hash fra MD5 er på 128 bits. På den måde blev udfaldsrummet 2^108 gange større end for den traditionelle DES metode. Selve rutinen jeg skrev, blev også skrevet på en sådan måde, at man ikke kunne forkorte, parallelisere eller optimere den. Den tog dengang 34msec på en P5/60 maskine, hvilket var et par størrelsesordener mere end den DES baserede kode tog.

Det er altid en tvivlsom affære at iterere en krypto algoritme, idet man nemt kan komme til at forstørre eventuelle svagheder i den grundlæggende algoritme, men jeg vurderede, at det var værd at tage chancen for forlænge den tid, det tager at gennemføre algoritmen.

For det første bedømte jeg det som meget tvivlsomt om nogen ville bruge den fornødne tid og energi på at finde

"THE BEER-WARE LICENSE" (Revis

<phk@FreeBSD.org> wrote this file.
As long as you retain this notice you can d
want with this stuff. If we meet some day,
stuff is worth it, you can buy me a beer in

Poul-Henning Kamp

en sådan systematisk svaghed, men sekundært, når/hvis vi får nys om noget sådant, så kan vi jo bare lave en ny algoritme, det såkaldte "Krypto-Kleenex" princip.

Passwords bør jo principielt ikke leve lang tid (Hvornår skiftede DU dit password sidst ???), så der er ikke nogen stor katastrofe i at introducere en ny algoritme hvert andet eller tredje år, sålænge den nye kode kan genkende de gamle passwords også.

Den sidste hurdle der var at passere, var at repræsentere de 176 bits som ascii, så de kunne gemmes i /etc/{passwd | shadow} filerne. Der valgte jeg at anvende samme base-64 encodning som den traditionelle DES algoritme, men satte "1" foran til at markere at det var en anden algoritme og et "$" mellem

salt og has
at man ogs
ducere nye
tiden.

Resultat

Et færdigh
kan derme
ud:

1iRE
SG/VMx8

Det var
traditionel
words, me
er det kun
grammer,
mer med d
dem kunn
nogle char
re.

Koden
http://
cgi/cvsweb
bcrypt/cry

og er be
erware" lic

Dermed var historien egentlig forbi for FreeBSDs vedkommende. Siden FreeBSD 2.0 har vi brugt denne algoritme som default, hvis ikke folk valgte at installere den separate "DES" distribution fra Sydafrika.

Jeg har naturligvis holdt antennerne ude for at høre om min kode holdt vand, og forskellige kontakter ude omkring har forwarded mig godbidder. Der er selvfølgelig blevet knækket passwords med bruteforce og dictionary attacks. Hvis folks password er tåbelige, kan ingen hash-algoritme beskytte dem. Men jeg har ikke hørt om nogen angreb baseret på forudberegnede dictionary filer. Det er et stort fremskridt, fordi de betyder, at angriberen hver gang skal starte forfra med at tygge sin ordliste igennem, det forsinker tingene en hel del.

Jeg har også modtaget nogle snippets fra IRC sessioner, hvor nogle elendige småkriminelle eksistenser siger ting som "Don't waste your time on FreeBSD systems takes too bloddy much time :-(" Vi takker for de gode anmeldelser :-)

Så en dejlig dag i starten af 1997 opdagede jeg i en cisco-konfiguration pludselig en linie, der sagde:

enable secret 5 1ay44$Gsx7oyYljljOcPBZJqFHA0

JasåJaveljaMONikke...

En diskret email af sted til en FreeBSD gut der sidder med fingrene dybt nede i Ciscos kildetekst: "kan du ikke lige checke... ?" svaret var: "Jo, jo, den er god nok!"

Jeg er blevet lovet, at jeg vil få en bajer af cisco hvis jeg stikker hovedet forbi en dag...

❑

Den V
Verde

En forbitre
til Dell Con
support, fo
kunne få ta
Dell compu
forsikret sig
rent faktisk
kontakten,
ren hvad de
trykkede på
pen. Hende
trykker og
dalen, men
Fodpedalen
musen til c

Compag ov
kommando
Key" til "Pre
på grund af
tal telefono
spørger, hv
er.

Lynindlæring med Int

Alle sejl var sat til, da Intellix A/S præsenterede deres videnl gram, KnowMan ved et gå-hjem-møde i marts måned.

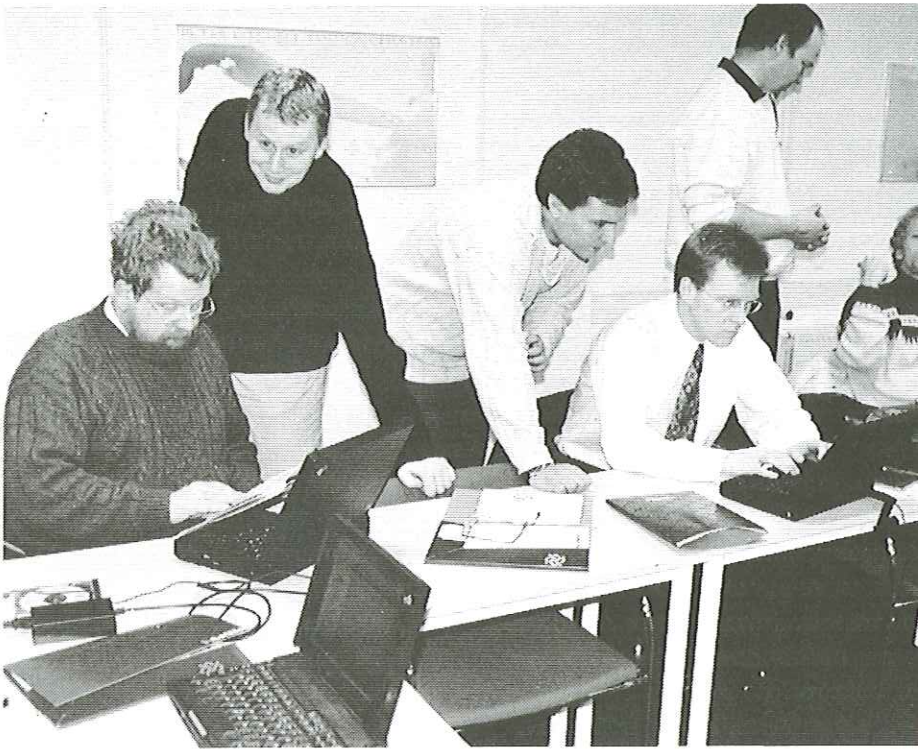
Af René Espersen

I over tre timer guidede direktør Christian Liisberg og stort opbud af ansatte fra Intellix de 18 deltagere, som alle havde taget deres bærbare PC'ere med. Så kunne de hele tiden selv "lege" med de mange facetter i KnowMan-programmet.

Allerede inden deltagerne mødte op, havde DKUUG-sekretariatet travlt med at finde forlængerledninger nok til at kunne levere strøm til de mange PC'ere. Selvom Symbion er et stort sted, så måtte hjælpen hentes mange steder fra, men til sidst lykkedes det, og det blev en aften udover det sædvanlige.

Deltagerne i gå-hjem-mødet lærte at bygge deres eget ekspertsystem i programmet, der kombinerer neurale netværk og avancerede statistiske metoder. Programmet "kortlægger" den menneskelige viden dvs. der puttes data ind, og via simple svar-funktioner bliver ens eget ekspertsystem bedre og bedre, jo flere data d et ekspert-s get, så kan finde frem t Hvad der - Liisberg - n

Christian Liisberg fra Intellix havde deltager hjem-møde i sin hule hånd.



Der blev arbejdet intenst under DKUUGs gå-hjem-møde med Intellix, og som de
næsten en hjælpende konsulent til hver deltager.

menneske 2 1/2 år at lære kan nu læres på seks uger. Dermed er indlæringstiden faldet - der er tale om en lynindlæring.

Deltagerne på gå-hjem-mødet prøvede at kortlægge deres eget følelsesliv med programmet dvs. give programmet svar på, om de vil have det pragtfuldt eller rædselsfuldt i forskellige situationer. Det kom der mange sjove og fantasifulde løsningsmodeller ud af.

De mange konsulenter fra Intellix var hurtige på pletten til at hjælpe delta-

gerne i enhv
når det gjald
nesserne i p
var lærerigt
gere og for I
lenter, så all
et stort udby

Et par gode kursustilb

DKUUG har fået et par stærke personligheder til at gæste D maj måned for at dele ud af deres viden.

Som nævnt i sidste nummer af DKUUG-Nyt, så kommer Nordens førende CORBA-ekspert, Pekka Kähkipuro fra Finland den 19. maj for at afholde et én-dags kursus om CORBA programmering. Ugen efter handler det om kryptering, når specialisten i kryptografi, Bruce Schneier fra USA afholder et to-dages intensivt kursus med titlen "Introduction and Advanced Cryptografphy". Det sker den 25.-26. maj. Begge kurser afholdes på Symbion i København.

Sidstnævnte kursus henvender sig til dem, der vil forstå kryptografi: hvad det går ud på, og hvordan det virker. Bruce Schneier vil koncentrere kurset om teknikken bag kryptografering, men der forudsættes ikke nogen stærk baggrund i matematik for at få et stort udbytte af kurset. Faktisk kan både begyndere og erfarne få et stort udbytte af dette kursus.

Fra omsætning af kode til digital signatur over elektronisk handel til sikker afstemning - kryptering er blevet den teknologi, der sætter os i stand til at tage de eksisterende forretninger og sociale konstruktioner og flytte disse til det globale netværk. Men meget af krypteringen er dårlig, og problemet med dårlig kryptering er, at det ligner en god kryptering. De fleste kan da heller ikke se forskel. Sikkerheden er som en kæde - den er ikke stærkere end det svageste led.

Kurset vil omhandle kryptering, som det bruges i virkelighedens verden: algoritmerne, protokollerne og implementationerne. Bruce Schneier vil på kurset understrege "hvad" og "hvordan" mere end "h opbygger - e kryptering h Schneier br hvad krypte ikke kan gø nemlig ikke salmiddel, s præsenteres

Bruce Sc streger, at e tør ikke kar blive en kryp at have gen kursus, så v ve intelligen kryptografi, kryptografie hvordan dis sættes sam et kryptogra endelig hvilk denne tekni

Lidt om B

Bruce Schn for Counterp

konsulentfirma med speciale i kryptografi- og computersikkerhed. Bruce Schneier er forfatter til en række bøger, hvor den bedst kendte nok er "Applied Cryptography". Allerede er den anden udgave af denne bog blevet solgt i over 80.000 eksemplarer over hele verden. Den er oversat til fire forskellige sprog. Han har desuden skrevet dusinvis af artikler om kryptografi til de alle de store magasiner om IT-teknologi.

Bruce Schneier har desuden designet den populære Blowfish encyrption algorithm, som nu efter fire år stadig ikke er blevet brudt.

Pris og tilmelding

Prisen for medlemmer af DKUUG er 6.000 kr. ekskl. moms. For ikke-medlemmer er prisen 8.500 eksl. moms. Yderligere oplysninger og tilmelding skal ske til DKUUG's sekretariat, tlf. 39 17 99 44, fax 39 20 89 48 eller email: sek@dkuug.dk.

CORBA 2

I samarbejde med BEA Systems Danmark og Tieturi Oy fra Finland tilbydes DKUUG's medlemmer et éndags kursus med Nordens førende CORBA-ekspert, Pekka Kähkipuro fra Finland, som vil give en introduktion til CORBA 2 programmering.

Kurset afholdes tirsdag den 19. maj i Symbion i København.

Efter endt kursus vil deltagerne have en god, grundlæggende viden om, hvorledes man anvender en objektbroker fra C og C++. Herudover får man en god forståelse for CORBA-arkitekturen og de funktioner, som de forskellige dele af arkitekturen tilbyder.

Målgruppen for dette kursus er systemudviklere og projektledere med forståelse for objektorienterede teknikker og programmering i C og C++. Kurset afholdes på engelsk.

Pris og til

Prisen er 2.5
lemmer af D
prisen er 3.5
ikke-medlem
ding og yderl
ger kan fås h
kretariat på
fax 39 20 89
sek@dkuug.

Tegner fatter ikke en lyd af de

Igennem en lang årrække har en flot tegning prydet forsiden Nyt. Tegneren bag hedder Erik Werner, men hvem er mande

Af René Espersen

Han har ingen teknisk sans overhovedet; er formentlig den dansker, der går oftest i teatret, og når han skal lave noget for DKUUG, så må han have "førerhund" med! For han fatter ikke en lyd af det hele.

Det lyder umiddelbart ikke som den perfekte medarbejder i DKUUG, men faktisk er han én af nøglepersonerne. For hvem ville undvære de oftest meget humoristiske tegninger, som har præget forsiderne af nærværende blad igennem en længere årrække.

Navnet er Erik Werner, og han er - som man nu nok har regnet ud - bladtegner. Egentlig vil han helst have, at titlen er "Teatertegner", for det er faktisk i det virke, som han bruger langt det meste af sin tid. Faktisk gik Erik Werner på pension lige før jul, men det stopper ham ikke fra at sætte streger på et stykke papir - til stor glæde for læsere af både Berlingske Tidende og DKUUG-Nyt.

Hvordan og hvorledes det lige blev Erik Werner, der skulle leverer alskens sjove tegninger til en forening, hvis emneområder han ikke fatter en meter af, kan han faktisk ikke huske.

- Der var nogle, der sagde, at det vil være en fordel, at jeg ikke ved noget om det. Jeg er således nødt til at have en "førerhund" med hver gang. Men det har været meget hyggeligt, understreger Erik Werner.

Førerhunden er bladets redaktør, der med nogle ganske få ord beskriver for Erik Werner, hvad bladets tema er - og få dage efter dumper så tegningen ind af døren.

Blækspru

Hans karri
20-årig, hv
redaktør af
så nogle af
ninger. Der
som kom m
udgave. De
da det som
dre og man
som får lov
dette "pæne

Men det
for en mang
som bladteg
ville han ha
der, men de
til noget. De
fald være n
sker, og det
baggrunden
at blive teat

- Det er
form for teg
per for at bl
der det fra

Der ligge

DKUUG-Nyt's tegner, Erik Werner, i et selvportræt.

udvalg af hans tegninger på Teatermuseet - cirka 4.000 tegninger ligger dér, men selvom Erik Werner nu er gået ind i pensionsalderen, så er han langt fra færdig med at sidde i teatrenes halvmørke og tegne.

- Jeg har to pladser på første række, hvor jeg så sidder og laver små "notater". Der er ikke lys nok til at lave en færdig tegning, så det er vigtigt at finde sjælen hos skuespillerne, siger Erik Werner, hvis tegninger alene skal kunne være en slags minianmeldelse. Han understreger, at han tegner sådan, som han nu engang oplever skuespillerne på scenen.

Han mener, at der er to former for at tegne; enten som en billedhugger (hvor tegneren kigger på former-

ne) eller so
tegneren m
sig om lys

- Det ga
det karakt
sonen - ud
en karikatu

Samtidi
Erik Werne
oplagt, kor
lille smule
skal i gang
Det lyder r

modsigende, men det gælder også om ikke at falde ind i en rutine, hvor der bare slås nogle streger "lige som sidste gang".

Ved siden af tegneriet, så modellerer Erik Werner også - således kan man bl.a. se tre bronzeskulpturer på det Kgl. Teater, som han har udført. Han er medlem af Kunstnersammenslutningen Grønningen, så det bliver også til udstillinger i mere gængs forstand.

DKUUG's tegner erkender, at han har været heldig, idet han allerede to år efter han fik et par af sine tegninger i "Blæksprutten" blev fastansat på Weekendavisen, men arbejdet bredte sig hurtigt til både Berlingske Tidende og B.T.

Verdensmester

Det blev dog til et år i ufrivillig "frihed", men efter en snak med daværende chefredaktør Niels Nørlund blev Erik Werner fastansat endnu engang. Faktisk er teatertegneren noget helt enestående. Det findes stort set ikke i nogle andre lande end i Danmark. Traditionen er dog lang, idet teatertegninger netop i år har 100 års jubilæum.

Hvert år afholdes der "verdensmesterskab" i tegning, hvor der er forskellige kategorier. Ikke mindre end tre gange er Erik Werner blevet verdensmester - men i dag er den pågældende kategori røget helt ud af konkurrencen.

Tegningerne har næsten som alt andet her i livet haft sine bølgedale, og i denne tid vinder de igen større indpas. Efter Erik Werner's mening måske i lige rigelig målestok, idet mange tegninger blæses op i kæmpeformater - mere for at fylde siden ud end hensyntagen til, at det er en illustration.

Selvom Erik Werner ikke har nogen teknisk sans overhovedet, så var han faktisk den første, der tegnede med "mus" i TV. Egentlig var det med en pind, hvor fjernsynskiggeren så kunne følge tegningen tilblivelse samtidig med en transmission fra Folketinget. Anden gang det med en rigtig - elektronisk - mus.

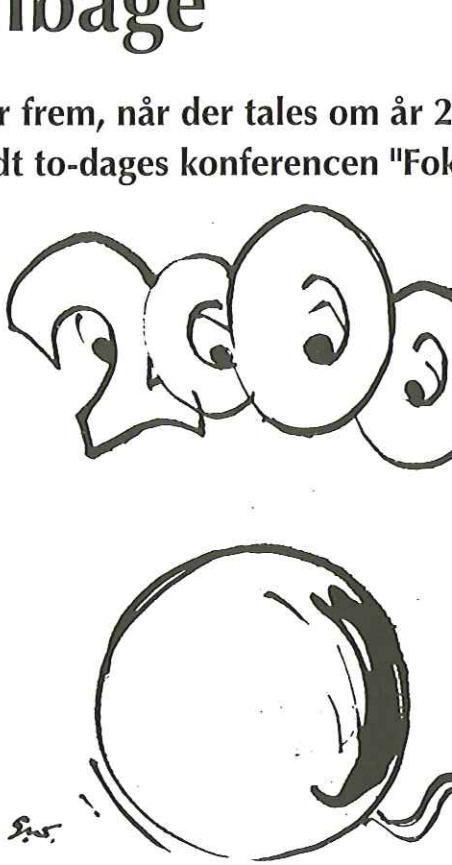
- Man kan
der har lavet t
der mangler li
Det er svært a
med. Det er sv
men kan ikke
sidste ting me
ner på en skæ
Erik Werner.

På redaktio
ikke dy os for
Werner ville v
Internettet! O
han har lavet
til Kulturmini
meside "Kultu
selv bl.a. på h
www.kum.dk/
kap09.html, h
gere kulturmi
den, den endn
turminister Ni
sen, og depart
Henning Rohd
ret.

Forhåbentl
Nyt's læsere m
over kunne gl
Erik Werners
her og i den d
ger...

Tiden med rationeringsma kan komme tilbage

De værste forudsigelser kommer frem, når der tales om år 2 met. Således også da IDG afholdt to-dages konferencen "Fol for en måneds tid siden.



Af René Espersen

Ingen strøm, intet vand, ingen telefon, ingen varme - og hvad der så deraf følger, er nogle af de skræk-scenarier, som trækkes frem. Alle er dog enige om, at så slemt bliver det ikke, men ingen vil på den anden side garantere, at det ikke bliver sådan.

Hvad skal man så tro? Den, der ligger inde med det rigtige svar, vil kunne tjene en formue ved at gå til bookmakerne og satse sine sparepenge - hvis da ikke bookmakeren noterer kundernes indsatser på sin ikke-år 2000 sikrede computer eller han har sat pengene ind i en mindre bank, der havde overset en eller flere dato-fejl, som lagde hele deres system ned ved overgangen til det nye århundrede. Det kan selvfølgelig også gå galt hos det offentlige, hv
får en eller
ydelse herf
"udbetaling
oneringsma
tersysteme

det ene eller andet sted i systemet.

Det er ikke for sjovt, at Claus Toftlund, projektleder for År 2000 fra medicinalvirksomheden H. Lundbeck afslørede, at de her i januar måned 1998 havde købt en splinterny PC'er hos Compaq/Digital, som ikke var År 2000 Parat. Og som han selv sagde, så er det mærker, hvor man ellers forventer tingene er i orden.

Problemerne er over alt, og det er umuligt for en virksomhed af en vis størrelse at tjekke alt, specielt hvis man har produktion af den ene eller anden art. Specielt svært kan det være at tjekke de indlejrede systemer. Og flere virksomheder lagde da heller ikke skjul på under ovennævnte konference, at de var nødt til at stole på de garantier, som leverandørerne gav dem. Dog gælder en mundtlig garanti ikke. Få garantien på skrift, så har du dit på det tørre - forhåbentligt.

Som det også blev nævnt af Jens Kolind i sidste nummer af DKUUG-Nyt, så gælder det under alle omstændigheder at udarbejde en beredskabsplan i tilfælde af, at noget går galt. De større virksomheder vil have nogle på vagt nytårsaften næste år. At det bliver dyrt for virksomheden lægger ingen skjul på, men hellere det, end at det hele eventuelt bryder sammen. For Lundbeck er det således vigtigt, at deres mange forsøgsdyr ikke kommer til at lide overlast, hvis der eventuelt opstår strømsvigt. Og her hjælper det jo f.eks. ikke, at man opretter en telefonkæde, hvis telefonerne nu ikke virker. Der skal tænkes utraditionelt for at kunne tage højde for det, der kan ske.

En anden god idé, der kom frem på konferencen var, at man nedsatte erfagrupper, hvor virksomhederne så kunne diskutere, hvad de gjorde for at imødekomme År 2000 problemet. Det behøver nødvendigvis ikke være branchebestemt, men kan lige så godt være for virksomheder, der ligger i det samme område. For hvis strømmen og telefonien forsvinder, så gør den det højst sandsynligt også hos

En hudløs
M. Mogensen
A/S fortalte o
2000 bliver ta
heden. Hos G
de man først i
hvor et indlæ
de, at der for
fokus på prob
først på det ti
man i Grundf
der kunne væ
kymring.

Der blev af
ressourcer til
samtidig har
heden erkend
nødt til at ned
systemudvikli

Grundfos
skulle bruge
mandeår på a
teste for År 20
men erkendte
de ikke kunn
kelt gruppe m
udelukkende
sig med dette.
sige alle ansa
arbejdet, dog
projektgruppe
står for den o
ring.

En ting ha

Grundfos dog ikke forudset, nemlig at nøglepersonen eller -personerne ville forlade Grundfos, inden alt var klappet og klart.

Der var hidtil ikke givet År 2000-medarbejderne nogle specielle fordele - eller stillet sådanne i udsigt. Men da nøglepersonen så sagde sit job op, erkendte man hos Grundfos, at de nu stod med et konkret problem - og at det godt kunne være, at man var nødt til at etablere en beredskabsplan, hvis andre skulle finde på det samme.

Fra Bankdata fortalte Lars Olsen, at de har givet deres medarbejdere en År2000-"gulerod" - 180 medarbejdere har fået en komplet multimedie PC'er, scanner m.v. leveret til privaten. Og har de pågældende haft et vist antal overarbejdstimer samt stadig er i virksomheden den 1. januar 1999, så PC'eren deres egen.

Klistermærker

Både hos Lundbeck og Bankdata har de mærket alt deres udstyr, så de på en meget synlig måde kan se, om det pågældende udstyr er blevet testet igennem og fundet År 2000 Parat.

Hos Lundbeck er der tre kategorier: "Ja - År2000 Parat", "Nej - År2000 Parat" og "Undersøges År2000 Parat", mens de hos Bankdata kun opererer med "Virker" eller "Virker ikke"-mærkater. Begge anbefalede varmt denne måde at synliggøre løsningen af problemet på.

Er problemerne så så store, som det lyder til? Hos Bankdata regnede man med at skulle igennem 18-20.000 stykker kildekode, men efter en gennemgang steg tallet til 39.000! De har afsat 50 mandeår til opgaven, beregnet ud fra, at det i snit tager 45 minutter at kigge ét program igennem, fem timer at rette ét program med fejl, og at det tager en time og 45 minutter at teste programmet. Alt sammen ud fra en antagelse af, at fejlprocenten ligger mellem 15 og 20!

Hos Grundfos har man allerede testet et helt fa-

briksanlæg
sted gik sy
og det ene
fandt, var
ne. De sto
blev ikke t
ikke umid
de enkelte
den frem p

Dirigen
rencen var
mark, jour
terWorld, o
bl.a., at ha
email fra é
ste stålvæ
fortælle om
oplevelser
År 2000-p
så enkelt s
viste sig at
tofunktion
måleren ha
dato-funkt
aflæsninge
ellers ville
muligt at a
Da virkson
frem til eft
gerede" pH
dvs. i displ
den senest
1999! Et s
sempel på,
de systeme

ning.

- Vi går ud til leverandørerne for at få en garanti. Vi har således måtte antage en holdning: Hvis vi får en garanti fra store soft-/hardware firmer, vil vi heller ikke teste standardløsninger, sagde Henrik M. Mogensen fra Grundfos.

Da man i Grundfos havde uddelegeret arbejdet, så var man i starten ude for, at den samme leverandør blev kontaktet af 6-7 forskellige fra virksomheden. Henrik Mogensen erkendte, at det selvfølgelig er kritisabelt, hvorfor det i dag kun er projektgruppen, der kontakter eventuelle leverandører.

Ingen forsikring

Er det muligt at forsikre sig imod en erstatningspligt forårsaget af År 2000? Det var ét af spørgsmålene, som direktør Claus Jakobsen fra Codan A/S skulle svare på i sit indlæg.

Svaret er kort og kontant et "Nej" - i hvert fald når det gælder erhvervskunder. Og i forsikringsverdenen kigger man ikke alene på den 1. januar 2000 som den eneste kritiske dato. Ifølge Claus Jakobsen er der ikke én men hele 24 kritiske datoer i løbet af de kommende hundrede år bl.a. den 9.9.1999, 28.-29. februar 2000 og 1. marts 2000 - de sidste 2-3 datoer handler om, at det i år 2000 er skudår!

Forsikringsbranchen har indført undtagelsesbestemmelser for alle de 24 kritiske datoer. I USA, der jo som bekendt er advokaternes paradis, forventes det, at de retssager, som vil opstå i kølvandet på år 2000 problemet, vil komme til at koste tre gange så meget som at få løst selve År 2000-problemet.

Er der så hjælp at hente hos ens leverandør? Advokat Karin Absalonsen understregede, at det er en god idé at kigge ens kontrakter igennem - ifølge standardkontrakterne K18 og K33 skal leverandøren opfylde alle kontraktens krav dvs. ét års garanti og 7 år vedligeholdelsesgaranti. Spørgsmålet er samtidig, om man har lovlig adgang til kildekoden til de programmer, man har og

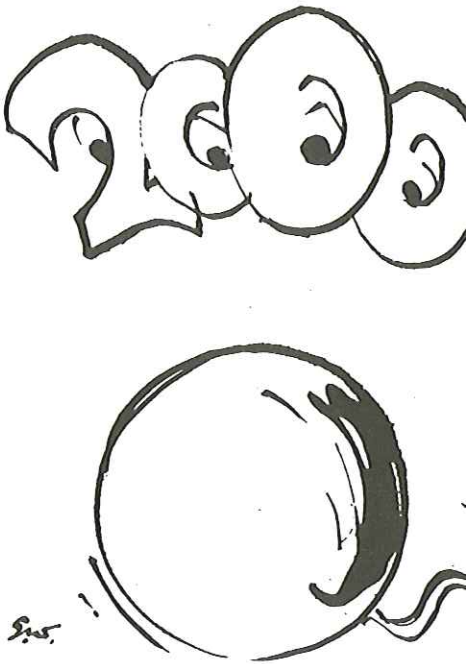
dermed lovlig
rette i progra
talen faldt på
dering til ny v
leverandøren
betaling, hvis
ny funktioner
men År 2000
funktionalitet

Karin Absa
derede, at ans
ning af År 200
ligger hos virk
delse, at muli
gøre leverand
beror på konk
og endelig, at
grund er til pa
der skal hand

De ansvarlige vil ikke stille op ti

År 2000 Forum afholder den første af tre konferencer om Å merne i det offentlige. Der skulle have været tale om høring ansvarlige ville ikke stille op!

Af René Espersen



Mai Buch, formand for År 2000 Forum, er dybt foruroliget over, hvor lidt tjek der i det offentlige er på eventuelle År 2000 problemer. Tre planlagte høringer er ændret til konferencer, idet de ansvarlige indenfor de pågældende områder ikke ville deltage, hvis der skulle gives nogle garantier.

Den 4. maj afholdes den første konference i Landstingssalen på Christiansborg, hvor det er sundhedssektoren, der sættes fokus på. Situationen på netop dette område er så graverende ifølge Mai Buch, idet Forum ikke har kunnet få nogle konkrete svar fra de ansvarlige, om man vil nå at teste alt udstyr i sundhedssektoren. Mai Buch har nu bedt sundhedsministeren tage affære.

I juni måned bliver der en konference om den trafikale infrastruktur; tog, fly, veje m.v., mens der i august måned vil blive sat fokus på forsynings el, gas og

År 200 daværend ster Jytte i dag sidd

sker i det - uden penge og kompetence, men med det mål at sætte fokus på År 2000 problemerne, koordinere de forskellige initiativer på området samt vurdere de samfundsøkonomiske konsekvenser af problemet.

I spidsen for År 2000 Forum sidder som nævnt økonomidirektør Mai Buch fra Det Kongelige Teater. Forum er bredt sammensat af organisationer og brancheforeninger. Det bakkes op af År 2000 sekretariatet, der har fået 12 millioner kroner over tre år til at skabe opmærksomhed om År 2000-problemet og opbygge viden om problemerne i forbindelse hermed.

År 2000 Forum lavede i starten en undersøgelse hos danske virksomheder for at få et indblik i, hvor stor bevidstheden var om problemet. 81 pct. havde hørt om det, og kun 6 pct. svarede, at de ikke havde hørt om det. Men nok så vigtigt - 84 pct. havde ikke afsat én eneste krone til finde, rette og teste for År 2000 problemer.

Mai Buch fortalte på IDG's konference i sidste måned om, hvor langt man er nået på Det Kongelige Teater. Her har man bl.a. også rettet henvendelse til Københavns Elforsyning og Tele Danmark, men ingen af de to har hidtil kunnet give et ordentlig svar, hvilket selvfølgelig er dybt bekymrende. Ikke alene for Det Kongelige Teater, men alle i der er afhængige af el og telefoni.

Endvidere har halvdelen af Det Kongelige Teaters leverandører kun ville give en mundtlig garanti for, at deres produkter er år 2000 sikker. Hvilket jo heller ikke er særlig betryggende. På teatret opererer man selvfølgelig med forskellige nødplaner, så der i det mindste vil kunne spilles forestillinger de første par uger i år 2000, hvis ellers er der strøm, varme, transportmidler osv. til rådighed.

❑

Den Vi
Verden

En kunde h
for at klage
statur ikke
Han havde
rent ved at
med vand o
ter at lade t
vandet i en
havde han f
ne og vaske

En forvirret
IBM, da han
mer med at
kumenter. H
keren, at co
fortalt ham "
printer". Kun
søgt at dreje
computeren,
se printeren,
ren kunne st
printeren.

Officielt referat

- fra den ordinære generalforsamling i DKUUG, torsdag den 1997 i Symbion.

Af advokat
Michael H. Svendsen
Qvist • Stanbrook:

Til dirigent blev valgt advokat Michael H. Svendsen, der konstaterede, at generalforsamlingen var indvarslet og indkaldt med det i vedtægterne fastsatte varsel, men at de forslag, der skulle behandles på generalforsamlingen, ikke var udsendt med det i vedtægterne fastsatte varsel på mindst 2 uger. Samtlige de mødende accepterede dog, at generalforsamlingen var lovligt indvarslet og dermed beslutningsdygtig.

Bestyrelsen og de enkelte udvalgsformænd aflagde beretning om aktiviteterne i det forløbne år. Særligt blev de nye medarbejdere præsenteret, direktør Bo Folkmann, bogholder og sekretær Hanne Schmidt samt den nye redaktør for DKUUG-Nyt René Espersen, som tiltræder pr. 1. januar 1998. Foreningen har planer om yderligere at ansætte en netpasser. Ansættelse vil formentlig finde sted pr. 1. januar eller straks i begyndelsen af det nye år.

Endvidere blev det nye sekretariat særligt omtalt og den opstramning i forretningsgangen, som nu er foretaget.

Bestyrelsen kunne berette, at der efter langvarige forhandlinger er skabt ro om foreningens skatteforhold.

Der blev afgivet særlige indlæg for de enkelte udvalg, Kim Biel-Nielsen, Myanne Olesen, Kristen Nielsen, Sven Thygesen og Gitte D'Arcy.

Beretningerne blev taget til efterretning.

Årsregns

Benny Mic
gik regnsk
og der var
veksle spø

Regnsk
udviser et
967.955, b
godkendt.

Valg af bestyrels

Efter præs
daterne bl
sen valgt s

Valg af r til besty

Der skulle
vælges 7 n
Efter præs
daterne bl
som nye m
styrelsen:

Sven Th

Nielsen, Myanne Olesen, Gitte D'Arcy, Jacob Bække, Bjørn Johannesen og Peter Holm.

Bestyrelsen har herefter følgende sammensætning:

Kim Biel-Nielsen, formand
Peter Lange
Benny Michelsen
Sven Thygesen
Kristen Nielsen
Myanne Olesen
Gitte D'Arcy
Jacob Bække
Bjørn Johannesen
Peter Holm

Valg af revisor

Som foreningsvalgt revisor blev genvalgt Bo Holst-Christensen.

Som revisorsuppleant blev genvalgt Lene Abild.

Indkomne forslag

Hr. Keld Jørn Simonsen har i overensstemmelse med vedtægterne fremsendt forslag til behandling på generalforsamlingen. De to forslag vedrører refusion af visse udgifter i forbindelse med en tidligere generalforsamling samt visse udlæg i forbindelse med hr. Simonsens rejseaktiviteter.

Generalforsamlingen udtrykte almindelige forståelse for, at bestyrelsen ikke havde bevilget disse udbetalinger til hr. Keld Simonsen, men besluttede desuagtet at honorere de af Keld Simonsen fremsatte krav om refusion, idet Keld Simonsen samtidig tilkendegav, at han herefter ikke har yderligere krav over for foreningen.

Budget og kontingent for 1998

Hr. Benny Michelsen gennemgik hovedpunkterne i foreningens budget for 1998. Med en enkelt korrektion, nemlig en forhøjelse af udgiftsbudgettet med kr. 10.000 for klubudvalg, blev budgettet godkendt af generalforsamlingen. Budgettet indebærer, at stormedlemmer for 1998 betaler kontingent på kr. 9.000 med tillæg af moms, organisationsmedlemmer betaler kr. 3.250 med tillæg af moms, mens individuelle medlemmer betaler kr. 560 med tillæg af moms.

Eventuelt

Et enkelt me
de til bestyre
gjorde sig me
at afgive en b
på den ordin
samling, hvo
medlemmern
samlet.

Hr. Benny
lagde til drøft
den for at lad
som ansvarli
gen af et udv
som på joint
skulle kunne
kapital til råd
dre og mellen
somheder. Et
udtrykte sig l
tanken om, a
skulle bruge
som risiko-ve
frem for at br
som indtægts
opfylde foren
formålsparag

Generalfor
vet.

Som dirige
Michael H

Linux 98

- Konference om Linux på hjemmefronten

DKUUG afholder i samarbejde med SSLUG - Skåne/Sjælland Linux User Group - en konference om Linux. Konferencen afholdes lørdag den 16. maj 1998 kl 10-18 på Symbion, Fruebjergvej 3, 2100 København Ø.

Linux stormer frem som operativsystem, især på netværksområdet som web-server og firewall, men også som arbejdsstation og til hjemmebrug. Denne konference vil sætte fokus på, hvordan man får Linux til at fungere godt på hjemme-PC'en. Konferencen kommer ind på mange aspekter af Linux, såsom:

- Den bagved liggende filosofi med gratisprogrammel og fri kildetekst
- Hvordan man får fat på det og installerer det
- Hvordan laver man sin egen system-kerne
- Hvordan man nemt administrerer det med dotfile generat
- Brug af komand
- Program tråde, o nistratio
- Hvordan op på In server, p
- Hvordan netværk win95 o
- Nogle or pakker
- Grafiske window
- Ting ma bedre at og svens
- Hjemme tal-knus ger man comput

I forbinde cen laves Linux-sys res gratis og der vil

at installere forskellige Linux-distributioner, samt få hjælp til Linux-problemer.

Aktiviteter

Udover det tekniske program vil der være en del andre aktiviteter om eftermiddagen:

- Installation af Linux - på din medbragte computer. Der planlægges at være en række forskellige distributioner tilgængelige, bl.a. RedHat, S.u.S.E, Debian og Slackware.
- Praktisk Perl programmering tutorial ved Ole P. Tange
- Planche om CVS - til administration af kildetekst ved Peter Toft
- Planche om programmering med tråde (threads) ved Ole Vilmann
- Planche om firewall ved Kristian Vilmann
- Planche om MPI ved Jacob Østergaard

Der vil også være mulighed for hjælp med praktiske Linux problemer. Se endvidere det detaljerede program på http://www.dkuug.dk/keld/konf2.htm

Målgruppe

Konferencen henvender sig til hjemmebrugere af Linux, både avancerede brugere og også brugere der lige er begyndt med Linux. Andre teknisk interesserede i Linux som folk der påtænker at bruge Linux kan også få et godt udbytte af dagen.

Pris og tilmelding

I sædvanlig Linuxånd er der mange som giver en hånd med gratis, og derfor er det gratis at deltage. Af hensyn til plads og mad er tilmelding dog nødvendig. Der kan bestilles snitter/smørrebrød til kostpris, ca. 12 kr. stykket, og vand til ca. 4 kr. pr flaske. Tilmelding og bestilling skal ske til DKUUGs sekretariat, email sek@dkuug.dk. Der vil være mulighed for at få installeret Linux på din egen maskine på konferencedagen.

Hvis du medbringer en maskine, se så venligst tilmeldingsblanketten på DKUUGs websider

http://www.dkuug.dk.

Den V
Verde

En IBM-ku
mer med at
software og
hjælp. "Jeg
diskette ind
fortalte kur

"Da den
anden disk
ind, så hav
blemer med
sagde, at de
skulle indsæ
jeg ikke få d

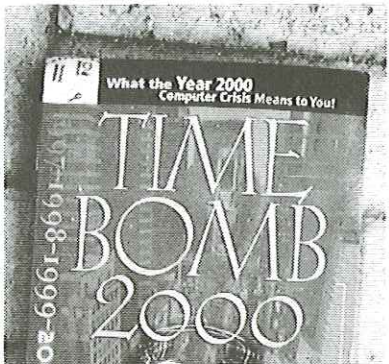
Kunden
ikke, at "In
2" betød, at
ne diskette

Boganmeldelse:

Tag dine forholdsregl

Time Bomb 2000
Edward Yourdon & Jennifer Yourdon
ISBN 0-13-095284-2
Normalpris:
kr. 184,00 ekskl. moms
DKUUG-pris:
kr. 165,60 ekskl. moms

Af René Espersen



År 2000-problemet er uoverskueligt, men man kan tage nogle forholdsregler.

Det må være konklusionen på bogen "Time Bomb 2000", som er skrevet af Edward Yourdon og Jennifer Yourdon. Det er en amerikansk bog med stort A, som opstiller forskellige scenarier for, hvad der kan ske, når der på kalenderbladet står 1. januar 2000.

Det skal siges med det samme, at der her ikke er tale om nogen egentlig teknisk bog, hvor man får løsningen på, hvordan man løser dato-problemet i alverdens programmer. Dette er mere en overlevelseshåndbog, der giver nogle gode råd til, hvilke forholdsregler man skal (bør) tage. Alt efter, hvor mange nerver man nu engang har, og hvor me-

get tiltro m
2000 prob
løst rundt
fundet.

Igenner
nemgås, h
År 2000-p
finansverd
hjemme-P
sektoren,
tionen, su
undervisn
statslige i
indlejrede

Samtid
deres bud
holdsregle
tage, hvis
områder b
men i hen
én måned,

I de fles
vil et nedb
nok kunn
ste, mens
værre ud,
varer en m
der bliver
få fat i føde

Derfor opfordres læseren til at hamstre forskellige mere eller mindre livsnødvendige ting såsom fødevarer, vand, medicin, kontanter m.v. - i hvert fald så man kan klare sig en måned.

Et andet råd er, at man skal undgå at blive indlagt i dagene omkring nytåret 1999/2000. Det kan jo unægtelig svært at styre selv - men det var måske værd at overveje ikke at blive gravid i foråret 1999!

Nogle af læserne vil være klar over, at der kan blive problemer allerede før nytåret. Således skal man nok tænke en ekstra gang om, inden man begiver sig ud på en rejse den 22. august 1999.

Netop denne dag vil GPS satellitternes "tidsmåler" nå et vendepunkt. Tiden bliver her målt i sekunder, timer, dage og uger. Da hukommelsen kun er på 12 bit, så vil denne blive fyldt netop den 22. august næste år og skifte til 0! Spørgsmålet er, hvad det kommer til at betyde, men i værste fald vil de cirka 10 millioner skibe og fly, der navigerer efter disse satellitter få udregnet forkerte positioner, hvilket kan få katastrofale følger.

I USA sørger den offentlige myndighed (SSA) for at udbetale folkepension til millioner af amerikanere hver eneste måned. SSA regnede med, at de skulle igennem og rette 30 millioner liner af kode. Et arbejde der forventes at være afsluttet i slutningen af 1999. Det er jo meget godt, men SSA startede altså også i 1991. Og det er unægtelig mange år før andre overhovedet vidste, at der kunne være problemer.

I bogen kan man også læse om en anden "pudsighed" (der er rent faktisk flere af den slags, end man går og tror!). Hos mange banker åbner døren til bankboksen kun på bestemte tidspunkter, naturligt nok på hverdage på et bestemt klokkeslæt. I de fleste tilfælde er den pågældende chip med datofunktionen indlejret godt og grundigt af sikkerhedsmæssige hensyn, og for at komme til denne skal halvdelen af banken rives ned. Det, der kan ske, er, at chip'en den 1. januar tror, a
januar 1900.
mandag, vil
boksen åbne
ret uheldigt,
2000 jo er en

Forfatter
at skulle ned
år eller mere
usandsynligt
nok i mellem
dre veje til at
udført de påg
Men meget k
sammen, hvi
én eller flere

De to ame
tere indrømm
le af scenarie
noget domme
men at man
må vurdere,
selv tror det g
det vil komm
ens dagligdag

Bogen ska
læse, hvis ma
komme i godt
den anden si
hvis man øns
sig godt, hvis
galt i år 200

Per´s hjørne

Kryptering - barnedrømmen levet ud

Af Per Andersen

De fleste af os - i hvert fald den halvdel af racen, jeg tilhører - kan huske, hvordan vi som børn var fascinerede af kode-skrift, så vi hemmeligt kunne kommunikere med hinanden. Man oversatte fx bogstaverne til tal og udførte en bestemt funktion på disse, som kun modtageren kendte. Bagefter var vi lige så tændte på at bryde de andres hemmelige kode, og vi anvendte mere eller mindre logiske måder at gøre dette på (jeg fandt det nu nemmere at banke oplysningerne ud af de andre snotunger).

Visse ingeniører har ikke helt kunne lægge denne idé fra barndommen fra sig, og de får derfor meget tid til at gå med at udtænke avancerede måder at kryptere data på, så ingen kan læse dem. Særlig avanceret er DES, der har en 56-bit kodelængde,

hvilket sk
ville tage
at finde d

Andre
følgelig de
dring, og
tænke en
koden på
netværk a
stationer
tigt!) over
hver arbe
at bryde l
des, og di
det sikker
(det skal
jeg ikke s
imod inge
sagtens fi
ske nørde
også, fx ø

Det fik
eksperter
måtte ma
koder me
længde. S
lig ikke k
før de 20.
ner havde

10.000 år. Jamen, siger du nu, arbejdsstationernes kapacitet vokser jo kraftigt! Jo, er det ikke noget med en fordobling ca. hvert år (nu er det faktisk kun for hver 18 måneder, men lad os bare overdrive). Det vil sige, at om 5 år vil de 20.000 arbejdsstationer "kun" skulle arbejde i 300 år for at bryde koden (og til den tid, vil de jo nok være forældede, ikke sandt!).

Nu håber jeg sandelig, at der lå noget meget værdifuldt bag ved denne 56-bit DES kode, for værdien af 20.000 arbejdsstationer i 150 dage er rundt regnet 300 mio. kr. plus mandtid. Så med mindre kriminalitet pludselig er blevet en velgørenhedsforretning, så vil det ikke rigtigt være attraktivt at ofre 300 mio. kr. for at få adgang til fx en stribe dankortnumre.

Det kan chefer og andre så tænke over, når de beder sekretæren kode indholdet på deres disk, så medarbejderne fx ikke kan snige sig til at finde ud af, hvad kollegerne tjener i løn. Og sekretæren så finder ud af, at det er en oplagt mulighed for hende til at få mere i løn: Hun beder diskret chefen om mere i posen, eller også kommer hun "desværre" til at glemme hvilken kode, der er anvendt for at kode alle virksomhedens livsvigtige oplysninger!

Gennem en virtuel markedsanalyse (også kaldet et gæt) har jeg fundet ud af, at der mistes langt flere penge på ovenstående "anvendelse af kryptering" end gennem kriminel "brydning af kryptering". Så måske var det en idé at tænke sig lidt om, inden man kaster sig ud i det helt store krypterings-orgie.

Der er nu mange, der går amok med sikkerhed. Det har udbyderne af sikkerheds-software også fundet ud af, og der er ombrydninger i denne industri som sjældent set før. Alle ruster sig til, at hr. Jensen skal have indført sikkerhed over hele linien. Amerikanske virksomheder inden for edb-sikkerhed opkøber hinanden for et godt ord - eller rettere sagt dollars. Der er handlet sikkerhedsfirmaer for 12 mia. kr. på bare 6 måneder! McAfee har slået sig sammen med Networ rity Dynami naSoft og Cy gorithmic fo nogle få.

Men mis ikke, der er for krypterin standard. Jo komme i tar sempler, sås ton skal udv ger med sin gerne eller r skal forbere uden at Glir kikker hend (ingen sex-v

For nu at de 20.000 a som jeg helt svært ved at er det hele j enkelt: Et sp kerhed er et hvor meget ner vil have investerer jo 100.000 kr. hjem for at reoanlæg til sagt på en a skal jo være for tyven at cer på at bry

Det er altså ikke et spørgsmål om, hvorvidt koden kan brydes eller ej (det kan den altid). Det er derimod et spørgsmål om værdien af det, man ønsker at beskytte kontra, hvor besværligt det vil være at bryde koden. Men længe leve ingeniørerne, der både har opfundet arbejdsstationerne, og bagefter har kunnet finde på noget at holde jordens bestand af arbejdsstationer beskæftigede med.

❑

Den VirkeligeVerden

Fra formanden har redaktionen modtaget følgende lille historie, som kan give stof til eftertanke, når emnet falder på kommunikation:

Har du nogensinde undret sig over, hvordan frontruden på flyvemaskiner testes mod sammenstød med flyvende fugle. Ifølge "California Poultry Industry Federation", så afskydes døde kyllinger mod ruden.

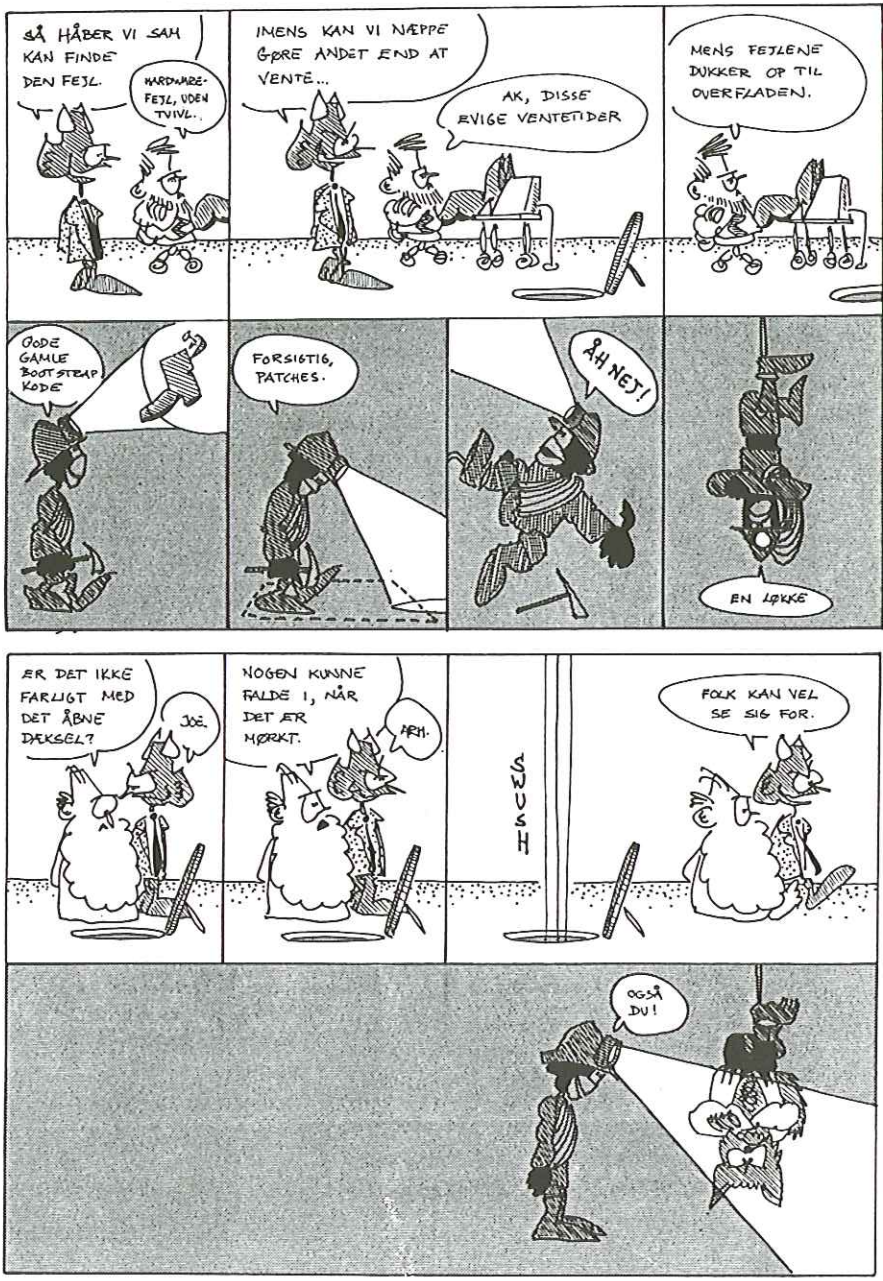
Åbenbart har det amerikanske luftfartsvæsen en speciel "kyllinge-kanon", som skyder med kyllinger som ammunition. Tanken er, at hvis frontruden ikke går i stykker, når den døde kylling rammer denne, så vil ruden sikkert også holde til en kollision med en levende fugl.

Da eksperterne fra British Rail hørte om "kyllingekanonen" spurgte de, om de ikke kunne teste frontruden på de nye høj hastigheds tog på ovennævnte måde. Som sagt så gjort, men da de ladte kanonen med en kylling og afskød d
knustes ru
røg lige iger
stol, ødelag
panelet og
i kabinens
rigtigt proje

Englænd
forbavset o
amerikansk
sen, hvad d
galt. Luftfa
rede med fø
sætning: "H
at bruge op

ETC.

KYNDE & FREY 87



Aktivitetskalender 1998

Maj

06. Seminar
- Handel på Internettet

16. Konference
- Linux

19. Gå-hjem-møde
- Unicenter TNG

19. Kursus
- CORBA programmering
- Pekka Kähkipuro

25.-26. Kursus
- "Introduction and Advanced Cryptography"
- Bruce Schneier

25. Klub Århus

26. Klub København

28. Klub Sønderborg

Juni

02. Gå-hjem-møde
- WinFrame

10. Seminar IT
- Perspektiver og muligheder

17.-18. Kursus
- Advance C++
- Rex Jaeschke

19. Kursus
- Java
- Rex Jaeschke

22. Klub Århus

25. Klub Sønderborg

26. Klub København

Juli

Ingen planlagte aktiviteter

Nye medlemmer

Følgende er nye medlemmer i DKUUG:

Østbirk Bygningsindustri er blevet nyt organisationsmedlem.

Tele2 A/S er blevet nyt stormedlem.

Thomas Jørgensen, Annemette Ibsen fra Netch, Poul Henning Kamp, Theis Passer fra TC Computing og Peter Jelver fra Tempest er nye individuelle medlemmer.

Alle bydes hjertelig velkommen i DKUUG.

DKUUG-Nyt er mec

Udgiver:
Dansk UNIX-syster
Fruebjergvej 3
2100 København Ø
Tlf. 39 17 99 44
Fax 39 20 89 48

Email: sek@dkuug.

Sekretariatet er åb
Mandag-fredag kl.

Direktør:
Bo Folkmann

Redaktion:
René Espersen (ans
Gitte D'Arcy
Søren Oskar Jense
Bjørn Johannesen
Jacob Bække
Keld Simonsen
Kim Biel-Nielsen
Peter Holm
Bo Folkmann

Tryk:
Palino Print

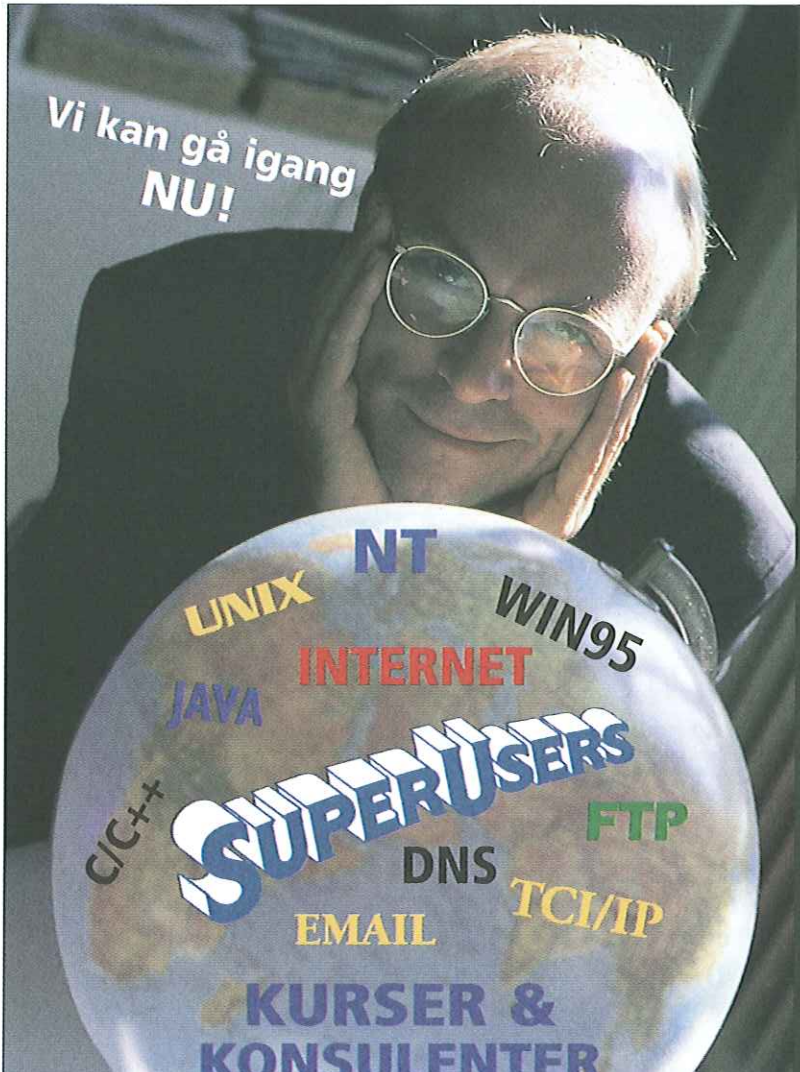
Papir: Cyclus
Annoncer:
DKUUG Sekretaria

Artikler m.v. i DKU
digvis i overensster
eller DKUUG's best
tertryk i uddrag me

Deadline:
Deadline for næste
dag den 15. maj 19

Medlem af Dansk F

DKUUG-Nyt
ISSN 1395-1440



Ring og rekvirer vores
216 siders katalog

U

20 UNIX-kur
hed for afvik
forskellige U
samt konsule
indenfor drif

Microsoft Au
Technical Ed
(ATEC) med
konsulentop
Windows 95
MS BackOffi

Int

Vi var med d
startede i Da
80'erne. Stor
internet appl
teknologier o

C/C++, H

Sprog som al
UNIX-verden
millioner af
erfaring.

Super
Karle
Karle
3400
Tlf: 48

EMail: super
URL: http://w