DKUUG-Nyt

Nr. 58 — marts 1993

ISO-9000 Tema

Alle taler om det, men hvad er det egentlig?

Søren T. Lyngsø er glade for deres klassificering — deres kvalitetsstyringschef fortæller hvorfor

UNIX-sikkerhed

Vi har en rapport fra Rik Farrows sikkerheds-workshop

X til PCere

Beskrivelse af en 32-bit implementation af X til PCere.

Indhold

ISO 9000: Modeflip eller praktisk værktøj?

Niels Svenningsen. DKUUG-Nyt

John Brix, du har lige udgivet en bog om ISO 9000 og kvalitetsstyring. Hvad betyder disse modeord?

ISO 9000-serien er en betegnelse for nogle internationale standarder, som indeholder praktiske råd om kvalitetsstyring. Og kvalitetsstyring vil blot sige, at man arbejder efter nogle fælles retningslinier, så produkterne bliver af ensartet kvalitet.

Der er flere standarder i serien end lige ISO 9000?

Serien omfatter tre standarder med formelle krav til godkendt kvalitetsstyring, som hedder ISO 9001, 9002 og 9003. De er næsten ens i opbygningen, de retter sig bare imod forskellige virksomhedstyper. Og med numre omkring disse tre kravstandarder findes der så en hel stribe vejledninger og tolkninger.

Hvorfor skal man dog standardisere?

For at gøre livet nemmere. Tænk et virvar, vi ville have, hvis forskellige landes el-apparater ikke var standardiserede, hvis de ikke kunne bruges i samme stikkontakter, brugte samme spænding. Vi er ikke nået langt nok, men det kommer. Også i edb-verdenen.

Der går en bølge af kvalitetsstyring hen over Europa for tiden, er det hele ikke bare eet stort modehysteri?

Joh, det er det nok man-

ge steder. Nye metoder har det med at danne mode, kvalitetsstyring er ingen undtagelse. Men når man bruger kvalitetsstyring - eller kvalitetssikring, som jeg foretrækker at kalde det - fornuftigt, indebærer det mange fordele for alle de berørte parter.

Hvad mener du med fornuftigt?

På en måde, så ISO-standardens krav omsættes til arbejdsregler, der gør det nemmere at være medarbejdere. De fleste virksomheder har en masse skrevne og navnlig uskrevne regler, som alle ansatte forventes at arbejde efter. Problemet er bare, at der ikke er klarhed om, hvordan reglerne skal forstås. Der er sjældent åben uenighed, man tror simpelthen, at man er enige — og trækker alligevel i hver sin retning. Et fornuftigt og ubureaukratisk kvalitetssystem afskaffer den usikkerhed.

Hvilke fordele giver det medarbejderne?

Først og fremmest giver det større arbejdsglæde, for det er kun de færreste af os, som er ligeglade med kvaliteten af det arbejde, vi udfører. Vi vil næsten allesammen gerne kunne være tilfredse med de resultater, vi skaber. Det, vi laver, skal kunne bruges af andre, uanset om vi programmerer eller sylter jordbær. Og hvis firmaet har et praktisk kvalitetssystem, bliver det hele simpelthen nemmere. Syltning og al anden madlavning lykkes nu bedst, når man har en kogebog med gode råd og opskrifter inden for rækkevidde.

Det lyder stift, bliver systemet ikke en spændetrøje?

Kun, hvis systemet ikke levner plads til den sunde fornuft. Lad os blive lidt ved kogebogen. Det er kun meget få kokke, som er slave af den. De fleste tyr til den en gang imellem, når de kommer i tvivl eller skal prøve noget nyt.

Det siges, at kvalitetsstyring giver en masse papirarbejde?

Det koster en del papirarbejde at fremstille et kvalitetsstyringssystem, men når systemet er indført, stiller ISO-standarderne meget få krav til skriverier. Desværre er der mange kvalitetsansvarlige, som benytter lejligheden til at indføre en sand papirkrig i firmaet. Og måske er ikke alle konsulenter tilstrækkelig opmærksomme på, hvor lidt man kan klare sig med.

Du siger i din bog, at kvalitetsstyring ligefrem kan føre til forenkling?

Ja, det kan det da bestemt, men det kræver omtanke fra starten. Hvis dem, der fremstiller systemet, hele tiden spørger sig selv og hinanden: Hvad skal der til, og kan det gøres enklere? " så bliver systemet enkelt, praktisk og overskueligt. Når kogebogen er nem at bruge, bliver arbejdet nemt. Og resultaterne gode!

Hvilke fordele har firmaerne så af kvalitetsstyring?

Stort set de samme fordele som medarbejderne. Når det bliver nemmere at fremstille gode produkter,

bliver det også billigere. Når medarbejderne kommer glade ind ad døren om morgenen, stiger produktiviteten. Og når virksomhedens tilfredse ansatte fremstiller gode og billige produkter, stiger afsætningen. Det er bare synd, at medarbejdernes trivsel ikke er i kurs i disse år. Medarbejdernes usikkerhed og utryghed koster virksomhederne meget mere, end de fleste ledere tør gøre sig klart.

Du har snakket meget om kogekunst. Hvad betyder kvalitetsstyring konkret for edb-systemer?

Jeg vover næsten ikke at sige det højt, men de fleste edb-virksomheder er rene fejlfabrikker. Det er sagt før, at man aldrig har tid til at gøre arbejdet rigtigt, men altid tid til at gøre det om. Jeg har oplevet mange edb-projekter, hvor kun 20 procent af tiden blev anvendt til forberedelse og egentlig fremstilling, resten af tiden gik med at rette fejl og at tænke om, lave om. Men hvis man skal have det sande billede af situationen, er man nødt til i en periode at kigge nogle medarbejdere omhyggeligt over skulderen. De tror simpelthen ikke selv på resultatet!

Det må betyde, at alle edb-folk er ukvalificerede?

Nej, men udviklingsmiljøet har ligefrem tradition for at være håbløst. I kreativitetens hellige navn får næsten alle lov til at slippe med mangelfuld tænkning og beskrivelse før og efter de såkaldt kreative aktiviteter. Du skulle bare se skandaler på Storebælt, hvis de byggede broer og tunneller på samme måde, som vi fremstiller edb-systemer!

John, siger du så ikke nu, at edb-folk kommer i spændetrøje med et kvalitetssystem?

Nej, nej og atter nej. Hvis det skulle være så attraktivt at trampe rundt i evige fejlrettelser og tilretninger efter levering, hvorfor er det så altid de tunge drenge, som vrister sig løs af de gamle systemer og kaster sig over de nye? Nej da, vi har bare ikke øvelse i på en nem måde at undgå fejlfabrikationen. Men det får vi, hvis vi tænker os om, når vi indfører kvalitetssikring.

Hvis det er så rosenrødt, hvorfor høres der så beklagelser over bureaukratiske systemer?

Fordi nogle firmaer har fremstillet bureaukratiske systemer, det kan ingen standard forhindre. Det værste, der kan ske i en virksomhed, er at systemets ambitionsniveau er højere end medarbejderne magter. Arbejdsreglerne, procedurerne, skal skrives, så de passer med en realistisk virkelighed. Hvis de er udtryk for idealiserede forestillinger og ønsketænkning, er de værre end ingenting.

Et praktisk og gennemtænkt kvalitetssystem må være meget dyrt at fremstille?

Ja, det koster formentlig lige så meget at fremstille, som virksomheden i forvejen bruger på spild og snosk på et halvt års tid. Men selvfølgelig spares det hele ikke

hjem på en gang, så du må nok regne med et års tid, før de investerede penge er tjent ind igen. Derefter giver systemet overskud.

Hvordan skaber man sådan et system?

Ved at tage et skridt ad gangen. Det fornuftigste er for de fleste først at beskrive den virkelighed, de lever i. Altså kortfattet at beskrive de arbejdsregler, som i forvejen fører til godt håndværk. Så kommer resten næsten af sig selv. Der er en enkel og nem opskrift på arbejdsformen i min bog. Jeg tør godt påstå, at den opskrift kan alle arbejde efter.

Er det nødvendigt med hjælp fra en konsulent?

Nej, men det kan være praktisk og lønsomt med assistance fra en god fagmand udefra, en med begge ben på jorden. Selv om du er god til dit fag, er du ikke nødvendigvis specialist i kvalitetsstyring. På samme måde som det er de færreste bogholdere, der med fordel selv og alene kan fremstille deres bogføringsprogram. Jeg kan dog ikke dy mig for at sige, at mange bogholdere ville have mere egnede systemer til deres rådighed, hvis de selv havde taget aktiv del i fremstillingen. Derfor skal virksomhedens egne ansatte absolut være aktive i fremstillingen af et kvalitetssystem.

John Brix er kvalitetskonsulent hos COH Management i Ølstykke. Han har nylig udgivet bogen Kvalitetsstyring - ISO 9000 på Teknisk Forlag (ca. 140 sider, illustreret, 245 kroner)

Certificering er ikke slutmålet

Kvalitetschef Bjørn Runge Søren T Lyngsø A/S

Når et firma har opnået at få certificeret sit kvalitetsstyringssystem, som regel efter en betydelig indsats, er det fristende at sætte sig tilbage i stolen, puste ud og sige "det var så det". Men så let går det ikke. Et Kvalitetsstyringssystem er et dynamisk og levende system, der hele tiden skal tilpasses virksomhedens behov, på samme måde som økonomisystemet hele tiden ændres, for at opfylde behovene for den nødvendige styring af økonomien. Et Kvalitetsstyringssystem, der samler støv på hylderne, og hvor intet dokument er blevet revideret i flere år, er ofte et tegn på et system, der ikke er effektivt, eller i værste fald ikke bruges.

De særlige kendetegn ved kvalitetsstyring af programmeludvikling

Der er (i softwarebranchen) tradition for at betragte software som noget, der er så specielt og komplekst, at det ikke er muligt at kvalitetsstyre. Dette er en vrangforestilling.

Udvikling, konstruktion og fremstilling af systemer, der indeholder software, *kan* kvalitetstyres som alle andre tilsvarende produkter.

Kravene i DS/ISO 9001 til et kvalitetsstyringssystem gælder også for softwaresystemer, men da standardens sprogbrug sigter på "fabriksproduktion", skal sproget fortolkes, så standarden kan "læses" af softwarespecialister.

Der kan være to grunde til at anvende software i et system:

- enten er det politisk bestemt, at det skal være et softwaresystem
- eller det er den løsning, der bedst opfylder systemkravene.

I begge tilfælde er det en konstruktionsbeslutning og det skal eftervises, at de stillede kvalitetskrav bliver opfyldte af det producerede system.

Når det gælder kvalitetsstyring af software, skal man være opmærksom på, at indsatsen i de forskellige faser er forskellig fra hvad der gælder for en "normal" produktion.

For software er udviklings', konstruktions' og afprøvningsfasen væsentlig længere, medens selve produktionsfasen er meget kortere. Dette skyldes, at egentlig produktion begrænser sig til kodning og kopiering til databærende medier.

> *"Det må ikke være for bureaukratisk"*

Det er vigtigt at gøre sig klart, at der findes mange modeller for softwareproduktion (vandfaldsmodellen, V-modellen, delleveringsmodellen og så videre). Kvalitetsstyringen skal tilpasses den benyttede model, men i praksis er der ikke de store forskelle.

> *"den letteste arbejdsmetode"*

Det må endnu engang fremhæves, at også kvalitetsstyring af software kræver at kvalitetskravene specificeres målbart, ellers kan de ikke eftervises. Det er kvalitetskravene, der er afgørende for hvilken softwarekonstruktion, der er den "bedste".

Certificeringen

Søren T. Lyngsø A/S fik i august 1991 det første DS/ISO 9001 certifikat, udstedt af Dansk Standard, som også omfatter fremstilling af software. Kvalitetsstyringssystemet har samme struktur som DS/ISO 9001 standarden og ikke som ret-

ningslinien ISO 9000-3 "Guidelines for the application of ISO 9001 to software". Dette valg blev truffet for at tvinge os til at analysere programudviklingsprocessen som en produktionsproces og vi har ikke fortrudt denne øvelse.

Kvalitetsstyringssystemet

Ved fremstilling af software er langt de fleste produkter dokumenter. Det er derfor vigtigt at have en effektiv dokumentstyring/konfigurationsstyring. Husk at standarden kræver gennemgang (review), godkendelse og ændringsstyring af dokumenter. Dette kan virke bureaukratisk, men der er store gevinster ved at finde og rette fejl tidligt i udviklingsforløbet.

Standardens krav om identifikation og sporbarhed implementeres i et konfigurationsstyringssystem. Af hensyn til produktansvar er det vigtigt at vide nøjagtigt hvad, der er leveret til en kunde.

Afprøvning af programmel kræver struktur, hvis det skal være effektivt. Der skal altid foreligge en afprøvningsforskrift, der beskriver hvordan afprøvningen skal udføres og som angiver input og forventet output.

> *"Et mål kunne være at for hver ny formular, der indføres, skal der forsvinde to fra systemet"*

Resultatet af afprøvningen er en afprøvningsrapport, som skal godkendes af den afprøvningsansvarlige.

I rapporten skal eventuelle afvigelser fra forventet resultat tydeligt markeres, så afvigelserne kan analyseres og programmellet rettes.

Husk ny afprøvning, hvor det også skal eftervises at rettelserne ikke har uheldige bivirkninger.

Endelig er det vigtigt at fastsætte operationelle og effektive afslutningskriterier for afprøvningen. Afprøvningsudstyr skal naturligvis også konfigurationsstyres.

Hvis der indgår måleudstyr i afprøvningen, skal dette være kalibreret, hvis målingen bruges til at afgøre kvaliteten af systemet.

Motivation

For at vedligeholde en effektiv brug af Kvalitetsstyringssystemet i virksomheden skal ledelsen "gå i spidsen". Ledelsens engagement i kvalitetsstyringen skal fortsat kunne erkendes af medarbejderne og dermed motivere dem til at bruge systemet.

For at være effektivt og brugervenligt skal kvalitetsstyringssystemet beskrive den til enhver tid "rigtige" måde at arbejde på. Det må ikke være for bureaukratisk.

Et mål kunne være at for hver ny formular, der indføres, skal der forsvinde to fra

systemet. Medarbejderne skal opfatte brugen af kvalitetsstyringssystemet, som den "letteste" arbejdsmetode. For at sikre dette, skal medarbejderne have mulighed for at komme med ændringsforslag til arbejdsgange og disse forslag skal tages alvorligt af ledelsen.

Kvalitetsfunktionen må aldrig give anledning til at blive opfattet som en "politistation", men som en hjælpefunktion eller konsulent, der undersøger om systemet følges. Er dette ikke tilfældet indledes en dialog med de involverede personer, så en "fornuftig" løsning findes.

Da DS/ISO 9000 standarderne kræver kvalificeret personale til at udføre opgaverne, er styring af uddannelse og træning af medarbejderne nødvendig for virksomheden.

Medarbejdernes kvalifikationer skal holdes vedlige og opfylde identificerede nuværende og kommende behov, både virksomhedens og medarbejdernes.

Systemvedligehold

Det er ledelsens ansvar, at virksomhedens organisation er kendt af medarbejderne, som regel i form af et organisationsdiagram.

Ledelsen skal gennem ledelsesevalueringer, vurdere om kvalitetsmålsætningen er opfyldt, samt om systemet er effektivt og tilpasset virksomheden.

Registreringer vedrørende kvalitet, hvoraf de vigtigste er interne audit og afvigelsesrapporter, er værktøjer til at trimme systemet med. Her afsløres svagheder i virksomheden eller systemet og midlet til at rette op er korrigerende handlinger, som skal fjerne årsagerne til svaghederne og dermed forhindre gentagelser.

Endelig skal de nødvendige kvalifikationer til arbejdsprocesserne identificeres og den nødvendige uddannelse og træning gennemføres.På denne måde er det muligt, at holde kvalitetsstyringen levende og effektiv i virksomheden.

Workflow Automation

Eva Schlegel
Control Data A/S

Hvad er Workflow Automation - Hvorfor er der behov for det - Hvad får virksomheden ud af det?

Kvalitet, lave administrationsomkostninger og tiptop service er væsentlige konkurrenceparametre i de fleste virksomheder. De administrative omkostninger, serviceniveau og kvalitetsstyring har relation til arbejdsgangen - workflowet, hvor opgaven behandles og videregives fra person til person.

I følge en OECD rapport, er produktiviteten på kontorområdet kun steget med 3% i 80'erne, hvorimod produktivititen på fabrikationsområdet er steget med 75%. I de kommende år forventes workflowet at undergå store ændringer i takt med indførelsen af nyt software, som

kan automatisere virksomhedens administrative procedurer.

Elektronisk sagsbehandling i form af journaliseringssystemer, kontorautomationssystemer og imagescanning af dokumenter er helt eller delvist indført i mange virksomheder, ligesom mange edb-systemer tager sig af forskellige funktioner som opdatering af kundeoplysninger, bogholderi, salg og lagerstyring. Investeringerne har i mange tilfælde ikke givet de forventede resultater i form af effektivitet og besparelser.

"Man kan se, hvor langt en bestemt ansøgning er kommet"

Der er nu et stadigt stigende behov for at focusere på de administrative processer, på den sammenhængende sagsbehandling, hvor der er opgaver, der ifølge sagens natur, ikke kan afsluttes umiddelbart, eller opgaver der ofte går på tværs af funktioner/afdelinger, involverer mange personer og megen papirflytning.

Automatiserede procedurer og automatiseret sagsbehandling bliver et væsentligt aspekt af 90'ernes elektroniske sagsbehandling, og der er mange gevinster at hente ved en fornuftig implementering i virksomheden.

Hvad er en automatiseret procedure?

En procedure kan defineres som et sæt af logisk sammenhængende arbejdsopgaver, som resulterer i et bestemt udkomme. Når proceduren understøttes af et edb-system, som styrer workflowet og behandlingen af de enkelte sager, taler vi om en automatiseret procedure.

Når en procedure er automatiseret, involveres de relavante medarbejdere på de rigtige steder i processen. Trivielle, regelbaserede beslutninger træffes automatisk, mens al relevant information stilles til rådighed for de personlige og individuelle vurderinger.

Control Data tilbyder løsninger baseret på Staffware, der er verdens førende produkt indenfor Workflow Automation.

"der er mange gevinster at hente"

Når f.eks. en låneansøgningsprocedure skal automatiseres v.hj.a. Staffware, beskriver man pr. trin:

- Hvem der skal udføre arbejdet
- Hvad der skal foretages (med angivelse af hvilke oplysninger der skal indtastes, beslutninger der skal træffes og hvilke oplysninger, der skal vises)
- Hvad der videre skal ske i proceduren, når dette trin afsluttes
- Hvis arbejdet skal udføres indenfor en given deadline, beskriver man, hvad

der skal ske, hvis deadline ikke overholdes

Proceduren er nu køreklar, og

- Der kan registreres nye låneansøgninger
- Via et mail-system bliver den person/gruppe, der skal udføre aktuelle trin aktiveret
- Man kan se, hvor langt en bestemt ansøgning er kommet
- Man kan se, hvor mange ansøgninger der er under behandling (f.eks. under kreditvurdering eller afventer bevilling/afslag
- Der udskrives automatisk lånedokumenter eller afslagsbrev — evt. sendes orientering til kunden, hvis sagen trækker ud

Integration

Staffware procedurer kan være "stand alone" procedurer eller anvende generelle valideringsrutiner, slå op i databaser samt udveksle information med andre edb-systemer.

Staffware kan bygge bro mellem virksomhedens eksisterende edb- og kontorautomationssystemer. Staffware har eget menu- og mail-system, men kan underordnes andre systemer. Efter ønske kan en procedure flette standardbreve og sagsdata, udskrive breve automatisk eller efter godkendelse.

Sager kan startes fra andre Staffware-procedurer, fra andre systemer f.eks. et image-scanningssystem, et journaliseringssystem eller et økonomisystem.

Fordele ved Staffware-procedurer

Skærmbilleder med vejledning hjælper brugeren til korrekt indtastning af sagsdata. Indlagte regler styrer dynamisk billedopbygning og sagsforløb, og frigør beslutningstagere for trivielle beslutninger. Staffware er nemt at anvende, og nye medarbejdere behøver minimal indlæring.

Information om foranliggende sagsforløb, image scannede dokumenter og relevant sagsdata — også fra andre systemer, understøtter vurderings- og beslutningssituationer i de enkelte procedure-trin, og får den administrative proces til at fremstå som en helhed.

Når en procedure er automatiseret, sørger Staffware for at holde styr på sagerne og revisionsspor genereres automatisk. Staffware's baggrunds-processor ("motor") er altid igang, og overvåger interne og eksterne hændelser.

Staffware kan håndtere/understøtte alle typer sagsforløb — uanset kompleksitet. En procedure er kun beskrevet ét sted, og ændring af regler og forretningsgange slår igennem med det samme. Systemets fleksibilitet og talrige integrationsmuligheder, kan gøre det "papirløse kontor" til en realitet.

Eksempler på automatiserede procedurer

Behandling af låne- og kassekreditansøgninger, be-

handling af skadesanmeldelser, flytning af kundeengagement til anden bank, reklamation og kundesupport, rekvisition og indkøbsstyring, kvalitetsstyring af systemudvikling, godkendelse af nye produkter, salgsadministration, kursusadministration og uddannelsesstyring, styring af jobansøgninger og interviews.

Det er nemt og hurtigt at udvikle prototyper og procedurer.

Gevinster ved automatiserede procedurer

- Bedre udnyttelse af personaleressourcer
- Lavere omkostninger pr. sag
- Sikkerhed for at procedurer og sikkerhedsforeskrifter overholdes
- Forbedret kvalitet og højere serviceniveau.
- Fuld dokumentation af sagsbehandlingen

UKUUG LISA 93 - "Coping with change"

Preliminary Announcement and Call for Papers

London, 30th June 1993

The UKUUG announces that the theme of this year's System Administration and Management conference will be "Coping with Change", with an informal subtitle of "Strategies for hitting a moving target".

With the increasing complexity of the working environment and the rate of change of that environment, in terms of both the variety of hardware platforms and associated operating systems, as well as the increasing number of third party software products available for those platforms the task of the System Manager has become increasingly difficult.

How does one encapsulate the differences in System Administration procedures? How does one evolve strategies for supporting complex third party tools and their varying licensing methods? How does one set about evaluating new software and hardware?

"Coping with Change"

The requirements of quality certification procedures mean that much better system operation documentation is required, and must be produced. How can this documentation be generated, and then be kept up to date with the minimum of manual intervention?

SAGE/UK

It is not only the working environment that is changing, the very role of the System Administrator is chang-

ing. System Administrators are now being recognised as being more than just skilled operators. They need to be involved in the planning process when new systems and networks are being ordered. However, at the same time organisations often make inexperienced people take on the job of System Administrator without adequate training or support.

"Strategies for hitting a moving target"

In order to help raise the standard of System Administration and to advance it as a profession, this conference will see the creation of SAGE/UK — a UKUUG Special Technical Group for System Administrators. Successful SAGE groups are already running in the USA and Australia and the UK group will keep in close contact with their activities. The group will provide a focal point for System Administration activities and will organise workshops and tutorials as well as developing guidelines for the proper management of systems.

Call for Papers

Papers are requested on topics relating to the broad themes outlined above. Submissions on other System Management themes are also welcomed.

All accepted authors will be expected to submit a paper in electronic form conforming to the conference guidelines, copies of the guidelines are available from the UKUUG Secretariat.

You do not have to be a member of UKUUG to submit a paper. Submissions from speakers from outside of the UK are welcomed.

Significant dates

Closing date for abstracts: 2nd April 1993 Accepted authors notified: 7th April 1993 Final papers due: 15th May 1993

Method of submission

Potential authors may request further information by sending electronic mail to "ukuug-lisa-93@bnr.co.uk", or may contact a member of the programme committee directly.

Initial abstracts should be sent either to "ukuug-lisa-93@bnr.co.uk", or to the UKUUG Secretariat. Electronic submission is preferred. All submissions will be acknowledged.

Programme Committee

Neil Todd [Chair]
GID Ltd.
neil@pio.gid.co.uk

Lindsay Marshall
University of Newcastle
lindsay.marshall@newcastle.ac.uk

Andrew Macpherson
BNR (Europe) Ltd.
a.macpherson@bnr.co.uk

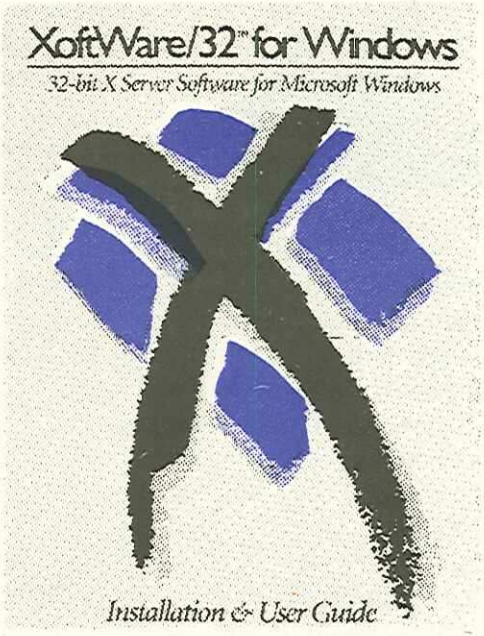
Bill Barrett
UKUUG Secretariat
bill@ukuug.uucp

32-BIT
X PERFORMANCE
TIL MICROSOFT WINDOWS PC'ER

UNIWARE introducerer XoftWare/32 til Windows, verdens første 32-bit X-server til Microsoft Windows-386/486 PC'er

oftware/32 for Windows er den første X-server
r drager fuld nytte af 32-bit arkitekturen i en
6/486 baseret PC. Dermed opnår man den
dste performance. Til forskel fra den gængse
-bit X-server udnytter XoftWare/32 hele din
. XoftWare/32 for Windows er baseret på
1R5 der understøtter skalerbare fonte. Nye
atures er blandt andet Xoftstart for automatisk
gin og MPSS der starter flere klienter op
mtidigt. Med XoftWare/32 følger også RAPID,
nyt tunings og optimeringsværktøj, der sikrer
timal udnyttelse af PC'en. XoftWare/32
derstøtter alle førende TCP/IP programmer til
OS. XoftWare/32 kan også leveres bundlet
ed Novell TCP/IP. Programmet udmærker sig
suden ved at være meget let at installere. Kun
oftWare/32 giver dig en 32-bit performance af
-Windows og Microsoft Windows på den
mme PC. Ring til Jens Mikael Jensen på 42 89
99 og rekvirer en gratis demo-diskette.

6.400/8.000 kr.



UNIWARE
danmark a/s

Unix System Security

Jens Fallesen

'Sikkerhed er et område, som nogle systemfolk går meget højt op i, mens andre overhovedet ikke skænker det en tanke. Langt de fleste går dog op i sikkerheden, men ikke alle er klar over, hvad det i praksis betyder på UNIX-systemer. Sikkerhed er jo ikke bare et spørgsmål om at alle brugere har et kodeord - det handler også om system i brugernes adgang til resourcer, beskyttelse af filer og kataloger samt at man kontinuerligt holder øje med de sikkerhedsmæssige aspekter.

I slutningen af januar arrangerede DKUUG et seminar om UNIX-sikkerhed, hvor Rik Farrow fra USA over to dage kom langt rundt i systemet og pegede på næsten hver eneste lille detalje, som måske syntes ligegyldig - men som faktisk kunne være et alvorligt hul. Rik Farrow er teknisk redaktør på bladet UNIX-WORLD og har skrevet bogen UNIX System Security, som blev udleveret til alle deltagerne.

"80% af sikkerhedsbrudene skete indefra"

Mange tror, at sikkerhedstruslen som oftest kommer udefra gennem f.eks. Internet, men denne opfattelse manede Rik Farrow i jorden ved at fortælle, at 80% af de sikkerhedsbrud, der var sket i USA, rent faktisk skete "indefra" - altså fra folk, der i forvejen havde adgang til systemet.

Rik Farrow startede med at fortælle lidt om systemsikkerhed generelt. For eksempel kunne man klassificere data efter niveauer som uklassificeret, fortroligt, hemmeligt og tophemmeligt. Derudover kan data være opdelt, således at folk med adgang til én type fortroligt materiale ikke automatisk har adgang til alt fortroligt. Sikkerhed afhænger altså af en korrekt sikkerhedsstruktur samt verifikation af brugere og deres adgang til informationerne.

Sikkerhedsklasser

I USA har The National Computer Security Center (NCSC) udarbejdet en sikkerhedsvejledning kendt som Orange Book til det amerikanske forsvarsministerium. Denne bog definerer kriterier for god sikkerhedspolitik, identifikation og kontrol af brugere, sikkerhed for at det anvendte programmel er sikkert og klare administrative og bru-

Orange Book opdeler systemsikkerhed i 7 niveauer:

D: Minimal eller ingen beskyttelse overhovedet. Herunder f.eks. MS-DOS.

C: Frivillig beskyttelse - dvs. at beskyttelsen i høj grad afhænger af brugerne. Der er to C-niveauer:

C1: Ren brugerafhængig beskyttelse. Her bestemmer brugerne selv, hvorvidt deres data og informationer skal beskyttes overfor andre. De fleste UNIX-systemer ligger på niveau C1, dog de fleste med den undtagelse, at de ikke har usynlige passwords. Det er nemlig ikke nok, at de i /etc/passwd er krypterede - det er stadig muligt at se de krypterede passwords og ud fra disse forsøge at gætte sig til dem. De fleste nyere UNIX-systemer understøtter dog shadowed passwords, og så opnås fuld C1 sikkerhed.

C2: En overbygning på C1, hvor man i højere grad kan vælge præcis hvem, der har adgang til ens data, og hvor man kan holde øje med, hvem der tilgår hvilke data. Visse nyere UNIX-system understøtter mere eller mindre C2.

B: Tvungen beskyttelse - dvs. man ofte har omfattende sikkerhedsparametre fastsat for forskellige data på systemet. Niveau B består af tre niveauer:

B1: "Afmærket" sikkerhed med en uformel sikkerhedspolitik og afmærkning af sikkerhedsparametre for de forskellige data.

B2: Struktureret sikkerhed med en formel sikkerhedspolitik og hvor alt på systemet er dækket af tvungne sikkerhedsparametre. Endvidere er verifikationen af brugerne skærpet kraftigt.

B3: Sikkerhedsområder som er kraftigt sikret mod indtrængen, deciderede sikkerhedsadministratorer, meget omfattende verifikation og kontrol af brugere og datatilgang, betingelser for driftssikkerhed og administrativt definerede adgangsparametre.

A: Fuldkommen verificeret beskyttelse. Dette bruges stort set kun på maskiner i forbindelse med atomraketter og lignende.

gervejledninger.
Digitals VMS operativsystem har de fleste B1-funktioner men kan ikke blive godkendt, da systemets interne struktur er alt for kompleks - primært fordi den er skrevet direkte i maskinkode. Blandt andet derfor er DEC i gang med at skrive VMS om i et højniveausprog. VMS udmærker sig blandet andet ved omfattende adgangskontrol og -registrering samt et alarmsystem, der med det samme fortæller systemadministratorerne om forsøg på uautoriseret brug.

"Findes der er 100% sikkert system?"

IBM's MVS-system er C1 men kan med sikkerhedsprogrammel opgraderes til C2. Honeywells SCOMP er A1, Multics er B2. De fleste personlige computere (PC, Mac osv) kører niveau D men kan normal udvides med ekstra programmel og dermed opnå niveau C.

Indenfor UNIX snakker vi primært C1 (dog kun fuldstændigt på systemer med shadowed passwords), selv om systemer som HP/UX og SunOS 4.0 indeholder en del C2-funktioner. Især udmærker HP/UX sig ved at have ACL (access control lists), hvor brugerne meget præcist kan angive, hvem der har adgang til deres data.

Det er kun Gould og SCO, der har godkendte C2-systemer, mens en del andre også tilbyder de samme funktioner. Dette skyldes primært, at det kan tage ca. 3 år at få godkendt sit system - og til den tid er det godkendte system jo forældet.

I 1992 udarbejdede National Institute for Standards and Technology (NIST) i USA et udkast til en standard, der skulle erstatte C2. Denne standard kaldes Minimum Security Functionality Requirements for Multiuser Operating Systems (MSFR - nu blot MSR) og retter sig mere mod kommercielle systemer end militære.

MSR byder på udvidelser inden for brugerkontrol og -verifikation, adgangskontrol baseret på tid og sted, større kontrol med passwords (såsom kompleksistetskrav, forældelse og genbrug) samt bedre sikring af netværksadgang (både til og fra netværket).

"på C-niveauet kommer sikkerheden i meget høj grad an på brugerne"

MSR er i starten af februar forelagt både for FC i USA og for tilsvarende europæiske standardorganer - håbet er at skabe en verdensdækkende sikkerhedsstandard og dermed gøre det attraktivt at følge denne standard.

Efter at Rik Farrow havde gennemgået disse sikkerhedsniveauer, kom det

uundgåelige spørgsmål: Findes der er 100% sikkert system? Dette kunne Rik Farrow dog sige klart ja til - sådanne systemer findes blandt andet inden for forsvaret i USA.

For at bruge systemet skal man først og fremmest bevise sin identitet, dernæst skal man igennem en slags sluser (hvor der er skarpt bevæbnede vagter) ind i et specielt lokale, hvor *ingen* radiobølger, elektriske signaler eller andet kan komme hverken ind eller ud. Inde i lokalet befinder computeren sig så - uden anden forbindelse til omverdenen end gennem sin kraftigt beskyttede strømforsyning.

Kort og godt: Hvis et system skal være 100% sikkert, snakker vi *fysisk* sikring.

Sikkerhedspolitik

Én ting er at have sikret sit system - men især med systemer på C-niveauet kommer sikkerheden i meget høj grad an på brugerne.

Det er derfor vigtigt at fastsætte en sikkerhedspolitik, som ledelsen skal godkende - og brugerne af systemet skrive under på.

I denne sikkerhedspolitik skal det klart fremgå, hvad brugerne må og ikke må — f.eks. hvad systemet må bruges til, krav til passwords og beskyttelse af data, besked om at rapportere ting der virker underlige osv.

"Et sikkert system er naturligvis låst inde"

Ligeledes skal det klart defineres, hvilke beføjelser systemadministratorerne har til at kontrollere brugerne og kigge i disses filer og post ved mistanke om problemer - samt naturligvis hvad der kan og skal gøres i tilfælde af misbrug (f.eks. er det i mange firmaer fyringsgrund).

Det er meget vigtigt at sørge for, at dette dokument juridisk er i orden, da det kan være ulovligt at læse andres email. Man bør selvfølgelig aldrig læse andres email, men på den anden side kan det i en speciel situation være nødvendigt, hvis man har begrundet mistanke om, at systemet misbruges. Men er denne ret for systemadministratorerne ikke defineret tydeligt, kan en bruger sagsøge adminstratorerne.

Hvis man savner et forslag eller udkast til en sikkerhedspolitik, kan man evt. prøve at få fat i RFC 1244 på Internet. Har man adgang til FTP, kan man lede efter filen policy.Z på en række Usenet-arkiver.

Efter denne generelle introduktion til sikkerhed og sikkerhedspolitik gik Rik Farrow over til at snakke mere specifikt om UNIX.

Jeg har medtaget det meste af den generelle stof, da jeg mener det har bred interesse, men resten af seminaret vil jeg gennemgå noget mere løseligt - det vil føre alt for vidt at få bare halvdelen med her.

Sikkerhed under UNIX

Først snakkede Rik Farrow om den fysiske sikkerhed. med begrænset adgang, så ikke alle og enhver bare kan gå hen til maskinen og måske endda udnytte, at mange systemer har en speciel "maintenance funktion" som kan anvendes af teknikere til at få adgang til systemet uden password.

> *"Hvad der ofte glemmes er backups og masters"*

Ligeledes skal det sikres, at man ikke bare uden videre kan tappe lokalnettet i bygningen og på den måde finde passwords og andet interessant.

Hvad der ofte glemmes er backups og masters. Hvad hjælper en god fysisk og teknisk sikring af maskinen, hvis der backup-båndene alligevel ligger frit tilgængelige på en hylde? Det er jo meget nemt at låne et bånd, læse på det (måske endda ændre noget) og så aflevere det igen. Faktisk blev det på et amerikansk universitet udnyttet af en gruppe studerende, der først og fremmest benyttede adgangen til backup-båndene til at lægge huller ind i systemet - dernæst udnyttede de, at man med et lille simpelt program kunne forårsage et systemnedbrud, der krævede genindlæsning af backup'en.

Sørg også for at fortælle brugerne, at de ikke skal forlade en terminal uden at låse den eller logge ud. Selv om det umiddelbart virker indlysende, at en anden kan (mis)bruge ens konto på systemet, oplever man ofte brugere, der efterlader deres terminal i god tro. Især at det vigtigt, at selv om en bruger har sin terminal eller arbejdsstation stående på et aflåst kontor, bør han låse terminalen eller logge ud, når han forlader kontoret - bare fordi man låser døren, kan man jo ikke være sikker på, at ingen andre kan komme ind i rummet.

Rik Farrow kom også ind på, hvordan filsystemet er opbygget, og hvordan en evt. misbruger kan maskere sine aktiviteter - og hvordan man kan afsløre forsøg på maskering. Her kom han ind på en række detaljer, som mange egentlig ikke tænker nærmere over, men som faktisk kan være risici.

> *"Der bør f.eks. kun være én konto med uid 0"*

Kontrol af disse ting vil ofte være temmelig rutinepræget, hvorfor han præsenterede en lang række shellscripts og programmer, som kunne være en hjælp til at gennemgå systemet.

Især er det meget vigtigt at beskytte sin superbrugerkonto. Der bør f.eks. kun være én konto med uid 0, da der så også kun er denne ene konto at holde styr på.

Hvis en misbruger får superbrugeradgang til systemet, vil han nemlig være i stand til at maskere sit misbrug så effektivt, at det ikke kan spores - f.eks. ved at skrive direkte til filsystemet.

"Frem for alt, må det ikke være et genkendeligt password"

Kodeord skal også vælges omhyggeligt. Det er utallige gange skrevet og sagt, at passwords bør være på mindst 5-6 tegn og helst bør indeholde både tal og bogstaver - men også gerne specialtegn samt både store og små bogstaver. Frem for alt, må det ikke være et genkendeligt password, da det så vil være nemmere at gætte sig frem til. Det velkendte eksempel med at tage f.eks. første eller andet bogstav i hvert ord af en sætning samt evt. et tal man kan huske, er en god idé - passwordet alene vil ikke umiddelbart give nogen mening, mens det er ret nemt at huske - for man husker jo bare sætningen.

Det er et faktum, at i de fleste situationer, hvor en brugers konto misbruges af en anden person, er det fordi det valgte password har været for dårligt. Det kan derfor være en meget god idé med jævne mellemrum at lade et program forsøge at gætte sig til passwords på systemet - eller endnu bedre: At bruge en erstatning for passwd, som kontrollerer det indtastede password for, om det er for nemt.

"passwords bør være på mindst 5-6 tegn"

Har man mistanke om at en bruger ikke er den person, han udgiver sig for (det kan f.eks. være tilfældet, hvis ajensen sidder på systemet, mens Anders Jensen rent faktisk er på skiferie), vil det være en god idé at kigge på, hvilke processer han kører og har kørt. Hvis man bare har generel mistanke om, at et eller andet mistænkeligt foregår på systemet, kan man gennemse systems logfiler og kigge efter usædvanlige ting. Det kan nemt blive omfattende at kigge disse filer igennem, og det vil derfor ofte være en god idé at benytte et shellscript, der frasorterer "normale" ting. På denne måde kan man godt overse misbrug - f.eks. hvis misbrugeren giver sine programmer samme navne som eksisterende programmer, der ofte bruges.

Rik Farrow kom også ind på virus, som indtil nu ikke har været særligt udbredt under UNIX, og nok i øvrigt heller ikke bliver det. PC-virus udnytter jo netop, at der er binær kompatibilitet mellem PC'erne, så de nemt kan spredes. UNIX-systemer er ofte mere udbredte over forskellige arkitekturer, så en UNIX-virus kan enten kun spredes på maskiner af samme type - eller også skal den være imple-

menteret som et shellscript.

De eneste eksempler på UNIX-virus man kender, er da også netop shellscripts, som har formået at formere sig på et filsystem ved at inficere andre shellscripts og filer på systemet. Under NFS kan sådan en virus dermed brede sig over flere filsystemer og for den sags skyld arkitekturer.

Efter en gennemgang af en række forskellige ting vedrørende filer, kataloger, device filer, logs og shellscripts til disse, gik Rik Farrow over til anden del af seminaret: Sikring mod folk udefra.

Truslen udefra

Så snart et system er udstyret med modems og/eller er koblet på f.eks. Internet, har man mindre kontrol med, hvem der bruger systemet. Nu kan man ikke længere sikre mod fremmed adgang med ID-kort, nøgler, kodelåse osv. Her gælder det så i stedet om at gøre så meget som muligt for at sikre, at forbindelserne til omverdenen ikke blive rene sikkerhedshuller.

Modemlinier kan f.eks. sikres med callback systemer, hvor systemet ringer tilbage til brugeren og dermed kan registrere, hvor personen befinder sig. Der er dog mange, der installerer callback systemer og så føler, at nu er den hellige grav vel forvaret, men det er ofte en falsk tryghed, da et callback system sagtens kan snydes. De simple systemer lægger nemlig på og ringer så ud igen på samme linie. Hvis dette sker med det samme, kan en hacker bare undlade at afbryde forbindelsen men så i stedet sige en lyd, der minder om en klartone, når modemet "løfter røret" for at ringe tilbage. Men også de mere avancerede callback systemer kan snydes, hvis der ikke anvendes specielle linier, som der kun kan ringes ud på.

Man kan også benytte specielle modems med kryptering eller specielle interfaces mellem modem og computer som benytter specielle krypteringsnøgler og ID-koder, men disse funktioner er ofte ret dyre og vil i mange tilfælde ikke kunne betale sig.

En forbindelse til Internet er straks sværere at sikre. Her skal man gardere sig mod mange forskellige forsøg på misbrug - blandt andet gennem huller i eksisterende netprogrammer. F.eks. findes der en tidligere udgaver af sendmail, hvor man med en bestemt udokumenteret kommando kan opnå en superuser shell på maskinen.

"Men også lokalnettet byder på problemer"

Udover deciderede huller, som kan give adgang til at arbejde på systemet, skal man være opmærksom på, at man med tftp kan hente en hvilken som helst fil på et system, hvis systemet tillader det - og det gør

de fleste systemer, der stadig understøter TFTP protokollen. En forkert opsat ftpd kan endda betyde, at folk med anonym FTP kan hente password-filen.

En anden mulighed er at benytte SMTP-porten til at skrive et falsk brev til en bruger og bede denne om at ændre sit password. Man kan så uden videre underskrive brevet som "systemchefen" eller andet. Det bør derfor indskærpes over for brugerne, at de *aldrig* må følge sådanne breve men i stedet skal præsentere dem for adminstratorerne.

"Det er derfor vigtigt at sikre, at det ikke er muligt at aflyttet nettet"

Det drejer sig ikke kun om at sikre, at brugere udefra ikke kan komme ind via nettet. Det skal naturligvis også undgås, at ens egne brugere ikke benytter netforbindelserne til at skaffe sig ulovlig adgang til andre systemer. Dette kan ofte sikres ved at sørge for at kun nogle få maskiner har adgang ud af huset, og at disse maskiner måske kun har bestemte programmer, som der er brug for. Alternativt kan man benytte routere, der kun tillader visse pakker at slippe igennem.

Men også lokalnettet byder på problemer. Hvis en person har held til at koble en maskine på nettet, kan denne person med f.eks. tcp-dump få fingre i alt, hvad der cirkulerer på nettet. Og hvis folk bruger rlogin eller telnet til at benytte flere maskiner på nettet — eller hvis tilslutning generelt foregår via terminalservere, går der jo blandt andet passwords ukrypterede på nettet.

Selv hvis der ikke benyttes logins via nettet, kan NIS (Network Information Service - tidligere Yellow Pages) give problemer, da passwordforespørgsler også sendes ukrypteret via nettet.

Det er derfor vigtigt at sikre, at det ikke er muligt at aflyttet nettet - og hvis det ikke kan sikres, bør alternativ sikkerhed overvejes.

Det bedste alternativ på nuværende tidspunkt er nok Kerberos. Kerberos bygger på et system baseret på "billetter". Når en bruger laver login, sendes krypteret en anmodning om en loginbillet til Kerberos-serveren. Alting foregår krypteret og alle billetter udstedes af en Kerberos-server, som skal være placeret fysisk sikkret. Systemet giver en smule overhead men er til gengæld meget sikkert - desværre kræver det også en dedikeret Kerberos-server, som på systemer med mange brugere og/eller maskiner skal være af betragtelig kapacitet for at undgå, at udstedelse og kontrol af billetter ikke går for langsomt.

Hvem kan hjælpe

Efter at have gennemgået en række mulige sikkerhedsproblemer og metoder til at kontrollere og evt. løse disse, gik Rik Farrow over til at fortælle, hvad man kunne gøre i tilfælde af misbrug via nettet. Dette omfattede metoder til at finde frem til, hvor misbruget kom fra, finde ud af, hvem der administrerede dette system - og i sidste instans hvordan man tog kontakt til Computer Emergency Response Team (CERT), hvis det var nødvendigt.

CERT tager sig primært af sager i USA, så har man seriøse problemer her i Danmark, bør man først og fremmest prøve at tage kontakt til netoperatøren - for DKnet er dette DKUUG og for DENet er det UNI•C. Netop UNI•C har en række konsulenter, som beskæftiger sig meget med hacking, men så vidt vides, har hverken DKUUG eller UNI•C oprettet en gratis hotline som CERT - rygtet vil dog, at UNI•C har planer om en sådan.

Generelt må det siges om seminaret, at det var utrolig givtigt. Rik Farrow var godt inde i stoffet og var også god til at formidle det. Det var dog lidt ærgerligt, at der på Symbion ikke var en projektor, så Rik kunne have vist nogle af sine eksempler i praksis på den opstillede RS/6000 maskine. Til gengæld havde han et godt materiale med overhead transparenter, som deltagerne fik udleveret kopier af, så det gik faktisk fint alligevel.

Rik Farrow havde i forbindelse med seminaret medbragt en diskette med en række scripts og utilities, som han kunne anbefale. De kan hentes via anonym FTP fra dkuug.dk i kataloget /dknet/tmp/seminar. Har man ikke adgang til FTP, kan de også fås ved email-henvendelse til undertegnede på fallesen@login.dkuug.dk.

Der er tale om følgende filer:

Book.tar.Z: Scripts og programmer fra UNIX System Security

Course.tar.Z: Scripts fra selve kurset

cops_104.tar.Z: Passwordcracker inkl. ordbog til kontrol af passwords

passwd+.tar.Z: Erstatning for passwd som stiller krav til passwords

swatch.tar.Z: SimpleWatcher - bruges bl.a. i hans shell-scripts

tcp_wrapper.tar.Z: Program til indpakning og sikring af TCP-services

De to første filer har mest relevans for deltagere i seminaret, mens de andre også kan have mere generel interesse.

Rik Farrow

Medlemsmøder i 1993

25/3	Heterogene løsninger
22/4	Downsizing
27/5	Virksomhedsbesøg v/ Hewlett-Packard
16/6	Standardisering
26/8	UNIX-markedet
28-29/9	X Windows & 3GL
28/10	CAD-løsninger
25/11	Sikkerhed & Generalforsamling

32-bit X-Window Server til PC'er med MS-Windows 3.1

Kim Biel-Nielsen
UNIWARE danmark a/s

Med 32-bit X-servere til Windows bygges der bro over kløften mellem 32-bit client/server-hardware og Microsoft Windows. Med en speciel konfiguration til Microsoft Windows udnyttes PC'ens datakraft fuldt ud.

Fuld udnyttelse af 386/486-processoren

De fleste PC-baserede softwareprogrammer, inklusiv PC-baserede X-servere, blev udviklet på den tid, hvor det drejede sig om 16-bit processorer. Medens processor-kraften og clockfrekvensen jævnligt forøges, har de 16-bit X-servere ikke draget fuld fordel af dagens 32-bit processorer.

"Windows- og UNIX-applikationer på samme PC"

Det at afvikle 16-bit ord gennem en 32-bit processor svarer til at anvende 2 vejbaner af en 4-sporet motorvej. Ved at forsyne processoren med alle data i 32-bit ord, optimerer en 32-bit X-server hver processor-operation. Dette betyder at tunge opgaver løses meget hurtigere.

Adressering af 32-bit hukommelse

For at kunne adressere den store mængde hukommelse, der er påkrævet i dagens opgaver, anvender DOS paging af hukommelsen i 16-bit segmenter. Man vælger data ved at specificere et segment i 16-bit store vælgerregister og dernæst lokaliserer i segmentet denne 16-bit store offset-register. Eftersom kun 64K hukommelse kan adresseres på ethvert tidspunkt, må store datastrukturer nedbrydes i mange hukommelsessegmenter. Dette resulterer i længere søgetider efter data i hukommelsen end med en fuld 32-bit adressering.

32-bit X-serveren fjerner det store 16-bit overhead ved at benytte 386/486-egenskaber til direkte af få adgang til en fuld 32-bit adressering.

En programmør sidestillede denne ændring med forskellen mellem at lede efter en ven på et overfyldt stadion række for række -

og at lede efter ham i hele områder ad gangen.

Forøget "Maximum Request Size"

En anden fordel ved at benytte 32-bit datastrukturen er muligheden for at forøge Maximum Request Size (MRS).

Selvom standard-X-modellen giver 256K som MRS, begrænser de 16-bit PC-implementeringer MRS til kun 64K. Dette betyder, at fire gange så mange request-pakker er nødvendige i et 16-bit miljø.

Ved at forøge MRS til 256K opnår 32-bit X-serveren en dobbelt ydeevne-fordel. Ikke kun er den lokale databehandling forøget ved at håndtere færre og større requests, men hele systemet drager fordel af det. Ved at gøre brug af 256K MRS er client-processen i UNIX i stand til at undgå unødvendig segmentering. Netværks-overhead reduceres også, da kun en fjerdedel af request-pakkerne skal overføres.

Optimeret brug af 386/486-instruktioner

Grafiske billeder kræver en lang række taloperationer af X-serveren. Disse er nødvendige for at nedbryde grafikken, så den kan vises i Windows-GDI-modulet.

Ved at rykke op fra 16-bit til 32-bit talregningen, reducerer 32-bit X-serveren antallet af disse operationer i betydelig grad. Dette forbedrer også svartiderne på det lokale system.

32-bit X-servere er tilpasset fremtidens hardware

Fordi en 32-bit X-server når op omkring grænsen for dagens 16-bit verden og gør brug af fuld 32-bit egenskaber af det underliggende hardware, giver det også brugeren store fordele. Når clock-frekvensen øges, vil det automatisk give en bedre ydeevne i en 32-bit processor.

Xoftware/32, en 32-bit X-server til Windows.

Markedets første 32-bit X-server til Windows hedderXoftWare/32.

XoftWare/32 til Windows er baseret på MITs nyeste X11R5-serverkode og giver brugere mulighed for sideløbende at afvikle Windows- og UNIX-applikationer på samme PC.

Ud over den forbedrede ydeevne omfatter Xoftware/32 til Windows også en række særlige funktioner til forbedring af produktiviteten. Disse omfatter et antal valgmuligheder, der giver brugeren mulighed for at tilpasse windows-miljøet til optimal anvendelse og ydeevne.

XoftStart automatiserer informationer om host-login og start af applikationer således, at click & start MS windows-ikonerne kan tilpasses.

CascadeX fjerner søgningen efter skjulte vinduer ved at give mulighed for at få

vist en MS Windows-lignende undermenu af nyligt åbnede X-vinduer.

RAPID er et tuningsværktøj med grafisk brugergrænseflade, som sikker optimal anvendelse af ressourcerne på PC'en..

Automatic Font Substitution (AFS) sikrer, at alle de overførte informationer vises, også når den ønskede font ikke kan anvendes.

Color Map Reservation System (CMRS) bevarer farvemapning fra Microsoft Windows.

Xoftware/32 til Windows giver adgang til ægte 32-bit applikationer.

Det har været klart for alle, at PC-verdenen bevæger sig mod 32-bit implementeringer. Computer-producenter har besvaret brugernes krav om forøget ydeevne ved at flytte underliggende hardware-arkitektur til 32-bit. Uheldigvis har de 16-bit PC-baserede X-servere hindret en forbedring af X-Window ydeevne på PC'er.

Ved at overskride 16-bit begrænsningen på 386/486-PC'er opnår Xoftware/32 til Windows morgendagens ydeevne i dag. Dets enestående arkitektur udnytter PC'ens underliggende styrke og benytter den til at opnå hidtil ukendt funktionalitet og ydeevne på PC-baseret X.

Nye DKUUG-medlemmer

Der er pr. 20. februar 1993 kommet flg. nye DKUUG-medlemmer:

713 o Hovedstadens Trafikselskab
714 o Forsvarets Datatjeneste
715 o Dansk Standard
716 o Kampsax Geoplan

o = organisationsmedlem
s = stormedlem
i = individuelt medlem

Sekretariatet flytter

Keld Simonsen

DKUUGs sekretariat flytter pr 1. marts til:

DKUUG
Forskerbyen Symbion
Fruebjergvej 3
DK-2100 København Ø
Tel: 39 17 99 44

Flytningen er foranlediget af langvarig sygdom hos det gamle sekretariat, som derfor ikke mente de kunne varetage funktionen.

Det er firmaet Symbion Videnformidling der overtager sekretariatesfunktionen. Vores nye "mødre" hos Symbion hedder Jette Balslev og Tina Thorup, og de kan træffes hverdage 8:30 - 16:30 på ovennævnte nummer. Faxnummeret 3160 6649 beholdes en måned endnu, så det kommer der besked om i næste nummer af DKUUG-Nyt.

UNIX-datamater som multiservere i Client/Server-arkitekturer

Søren Steenberg
DDE

Er der forskel på en server og en minidatamat? Ja, — en ægte multiserver indeholder en minidatamat men er mere end det.

En moderne UNIX-datamat udgør en stærk multiserver i et netværk, hvor arbejdspladserne — klienterne — kan være PC'er, Macer, X-terminaler, workstations etc. Arbejdsfordelingen mellem klienter og server er bestemt af, at arbejdspladsudstyr — f.eks. PC'er — har sine stærke sider, mens UNIX-multiservere har andre stærke sider:

PC'er er bl.a. gode til:

- Præsentation af data for brugeren
- Afvikling af en enbruger-applikationer.

UNIX-multiservere er bl.a. gode til:

- Lagring af data og behandling af store databaser
- Afvikling af flerbruger-applikationer
- Transaction processing
- Datakommunikation.

Endvidere er regnekraft typisk billigere på PC'er end på UNIX-multiservere. Modsat kan det være billigere at udbygge regnekraften i én UNIX-multiserver end på alle PC'erne i et netværk, da de bedste UNIX-multiservere er modulære, hvor PC'erne normalt alle skal udskiftes med en kraftigere model.

Disse forskelle udnyttes i en UNIX-baseret Client/Server-arkitektur, hvor applikationer fordeles og opdeles således, at de enkelte dele afvikles dér, hvor det er mest optimalt. Moderne UNIX-multiservere er forsynet med en række egenskaber og faciliteter, der gør dem specielt velegnede som servere.

Åbent system

Det er vigtigt, at en server er et "åbent system". Åbne systemer overholder en række standarder — bl.a. vedrørende kompatibilitet (bagud og fremad i tiden), portabilitet (mellem leverandører), skalerbarhed (fra små til store anlæg) og interoperabilitet (mellem systemer i et netværk).

Skalerbarhed

Som server tilbyder UNIX-multiserveren en grad af

skalerbarhed, der er helt unik i forhold til andre servere. Nogle UNIX-multiservere har ligefrem en multi-CPU-arkitektur og modularitet, der muliggør en konfigurationsspændvidde lige fra små workgroup-servers med 2-3 arbejdspladser/klienter til helt store enterprise-servers med flere hundrede arbejdspladser/klienter.

Fordelene ved den høje skalerbarhed er, at nye anlæg kan dimensioneres til præcis den størrelse, der initielt er behov for, og at anlæggene senere kan udbygges løbende i takt med, at edb-anvendelsen og/eller antallet af brugere forøges. Desuden kan organisationer med afdelinger af forskellig størrelse anskaffe samme system til både små, mellemstore og store afdelinger. Alle konfigurationsstørrelser er binært kompatible og betjenes ens, hvorved kundens investering i programmel og arbejdsgange bevares, selvom edb-systemerne udbygges.

Én samlet server

Når PC'er anvendes som servers, skal der normalt en PC til pr. service. UNIX-multiserveren tilbyder en række serverfaciliteter samlet i én server, idet den på én gang kan fungere som file-, printer-, boot-, mail-, kommunikations-, database og applikations-server for de PC'er, der findes i lokalnettet. Det, at alle serverfaciliteter er samlet i én server, medfører bedre integrationsmuligheder og letter administration og overvågning af systemet.

Sikkerhed og systemadministration

Nogle af UNIX-multiserverens største fordele er høj sikkerhed mod uautoriseret adgang til data og høj robusthed mod nedbrud og tab af data. Desuden muliggør den en meget lettere centraliseret administration og overvågning af netværket og systemerne.

En anden måde at belyse UNIX-multiserverens styrke er at se på de faciliteter eller services, de bedste UNIX-multiservere bør stille til rådighed for klienterne

Fileserver

Med en UNIX-multiserver som fileserver kan en PC-klient lagre sine filer på serverens disksystem. Da alle klienter kan lagre og læse filer på serveren, gør fileserver-funktionaliteten det muligt for klienterne at dele data på filniveau. Desuden muliggøres en centraliseret, systematisk backup af alle PC-data vha. UNIX-multiserverens backup-system.

UNIX-multiserveren kan f.eks. anvende netværksoperativsystemet Lan Manager. Som Lan Manager-server muliggør UNIX-multiserveren en god integration af DOS-, Windows, OS/2- og UNIX-miljøer, idet filsystemerne fra de tre miljøer kan samles i ét fælles filsystem, der optræder uændret (set fra både applikationer og brugere i hvert af de tre miljøer.

Printerserver

UNIX-multiserverens printerserver kan ligeledes bygge på Lan Manager, hvorved klienter tillades at udskrive på alle printere tilkoblet UNIX-multiserveren direkte eller via lokalnettet. Print fra klienterne udskrives via UNIX spool-systemet med de fordele, som findes heri.

Bootserver

UNIX-multiserverens bootserver sørger for, at PC'ernes styresystem DOS via lokalnettet bliver loaded og startet på alle PC'er. Dette kombineret med fileserverfaciliteten kan helt overflødiggøre diskette- og diskdrev på PC'erne, der således kan være diskløse. Fordelene herved er bl.a., at PC'erne bliver støjsvage, samt at den sikkerhedsmæssige fare for uønsket input og output af data og programmel, et diskettedrev frembyder, elimineres.

Mailserver

På UNIX-multiserveren bør findes standard mail-protokollerne UUCP, SMTP, SNADS og X.400. Denne kan derved være mailserver i alle gængse netværk: UNIX, TCP/IP, SNA og OSI. Alle mail-protokollerne bør samtidigt være integreret, hvorved UNIX-multiserveren, ud over at være mailserver, kan være gateway mellem de forskellige netværk. Endeligt kan UNIX-multiserveren være fælles FAX-server for de tilsluttede arbejdspladser.

Kommunikationsserver

En kommunikationsserver skaber forbindelse fra klienter på lokalnettet til andre edb-systemer — eksternt eller internt. UNIX-multiserveren skal understøtte alle gængse standard-protokolfamilier: UUCP, TCP/IP, SNA og OSI, hvilket gør den velegnet som multi-protokol kommunikationsserver. På hver protokolfamilie skal både understøttes filoverførsel, terminal-opkobling, elektronisk post og program-til-program kommunikation.

Databaseserver

De nyere databaseværktøjer understøtter idag distribueret drift, hvor databasedele og applikations-dele kan splittes op på hhv. server og klient. UNIX-multiserveren bør understøtte et bredt udvalg af sådanne databaseprodukter for derved at kunne tilbyde databaseservices til klient-applikationer, der afvikles spredt på andre UNIX-datamater, PC'er, minidatamater eller mainframes. Applikationer på mange forskellige maskintyper og forskellige lokationer kan på denne måde dele fælles data beliggende på UNIX-multiserveren — med fuld dataintegritet og -sikkerhed.

Applikationsserver

UNIX-multiserverens styrke som UNIX-datamat gør den velegnet som applikationsserver i et netværk. Nogle applikationer afvikles bedst

ude på brugerens arbejdsplads (f.eks. en PC), mens nogle afvikles bedst centralt i UNIX med brugerens arbejdsplads opkoblet som terminal (f.eks. med et PC-terminalemuleringsprogram). I sidstnævnte tilfælde optræder UNIX-multiserveren som applikationsserver.

"Nogle hævder, at UNIX-mini'en er død"

I praksis vil brugere med PC'er som arbejdsplads typisk anvende et mix af PC- og UNIX-applikationer. I dette tilfælde optræder UNIX-multiserveren som applikationsserver samtidigt med, at andre serverfaciliteter anvendes.

Eksempler på applikationer, der bedst placeres på UNIX er økonomistyring, produktionsstyring, personaleadministration, journalisering etc. Der er flere kriterier for, hvornår en applikation eller dennes centrale dele bør placeres på UNIX. Eksempler herpå er:

- Flerbruger-applikationer, hvor mange brugere samtidigt skal kunne både forespørge og opdatere i fælles data.
- "Mission critical" applikationer — dvs. applikationer, der er afgørende for virksomhedens forretning og derfor kræver høj sikkerhed og robusthed. Et salgsordresystem er normalt mission critical, hvorimod kontorautomation eller bogholderi ikke nødvendigvis er det.
- Applikationer, der er udviklet til UNIX og ikke til DOS.
- Applikationer, der indgår i større distribuerede systemer. Årsagen hertil er, at UNIX-multiserveren generelt er bedre egnet til avanceret datakommunikation end PC'er.

Server for distribuerede applikationer

Fremover vil en række applikationer med fordel kunne placeres fordelt på UNIX-multiserveren og PC'er som distribuerede Client/Server-applikationer. Til udvikling af sådanne applikationer bør UNIX-multiserveren stille en række programmerings-interfaces til rådighed såsom Remote Procedure Calls (RPC), Named Pipes, NetBIOS, TLI-interface og APPC/LU6.2.

Konklusionen er, at UNIX-multiserveren, hvis den lever op til de nævnte krav, er langt overlegen i funktionalitet i forhold til PC-baserede servere, og at UNIX-multiserveren vil være en meget vigtig komponent i fremtidens mere og mere avancerede netværk. Nogle hævder, at "UNIX-mini'en er død", men til gengæld er UNIX-multiserveren kommet for at blive og for at opleve en kraftig udbredelse fremover, og dette takket være de leverandører af UNIX-datamater, der har tilpasset strategien og formået at udbygge deres produkter til ægte UNIX-multiservere.

Klubaften i København

Tirsdag den 30. marts 1993
kl. 19:00 - 22:30
Datalogisk Institut (DIKU)
Universitetsparken 1
(indgang fra Nørre Alle)

Brugergrænseflader —fra Human Factors og Cognitive Science til Cyberspace.

Foredragsholder: Michael Reich SuperUsers a/s

"I løbet af 70erne begyndte forskningen i Human Factors at interessere sig for andet end korrekte arbejdsstillinger og rigtig belysning.

Man gik — i den grænsedisciplin, der under navnet "cognitive science" opstod mellem datalogi og psykologi — for alvor i gang med at kigge på brugermodeller, dvs. den forståelse en person har af et givet system. Og man undersøgte hvordan brugervenlighed og konsistente brugermodeller hænger sammen.

Det har betydet meget for den konkrete udformning af de brugergrænseflader vi mødes af idag.

I 1986 udsender science fiction-forfatteren William Gibson den første bog i sin cyberspace-trilogi, "Neuromancer", hvor helten er en informationscowboy, der rider i datastrømmenes store matrix.

Hvad det kan komme til at betyde for udformningen af de brugergrænseflader vi mødes af imorgen, vil være emnet for foredragets sidste halvdel."

Vel mødt — den sidste tirsdag i måneden i DKUUG-klubben

Kolofon

DKUUG-Nyt udgives af:
Dansk UNIX-system Bruger Gruppe

DKUUG, sekretariatet
Symbion
Fruebjergvej 3
2100 Kbh. Ø
Tlf. 3917 9944
Fax 3160 6649
Giro: 137-8600
Email: sek@dkuug.dk
Man - tors kl 9 -16.30
Fredag kl 9 - 15.30

Redaktion

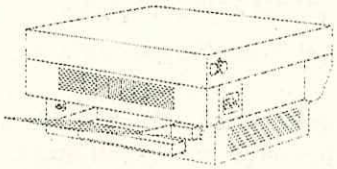
Søren Oskar Jensen (ansv.)
Christian D. Jensen

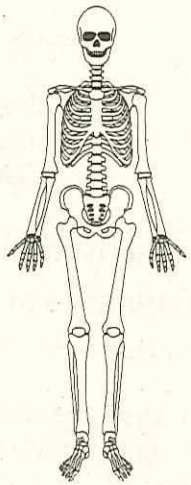
DKUUG-Nyt
C/O Søren O, Jensen
Blegdamsvej 128A, 1.tv.
2100 Kbh. Ø
email dkuugnyt@dkuug.dk

Deadline

Deadline for næste nummer, nr. 58, er fredag d. 19.3.93

Kender du fornemmelsen af at vente en evighed på print ??





IOPRINT ER LØSNINGEN

IOPRINT er en højhastigheds TCP/IP-baseret printerserver. Når man benytter IOPRINT, kan man opnå en udskrivningshastighed på op til 65.000 tegn/sekund på printere og plottere. Den direkte opkobling på lokalnettet giver en udskrivningshastighed der ofte overgår direkte opkobling til serveren og en total fleksibilitet med hensyn til placering af printerne. En IOPRINT-server leveres med to serielle porte og en parallelport. Mod ethernettet kan man vælge enten tykt, tyndt eller parsnoet kabel.

Ring straks og hør nærmere på 42 89 49 99

UNIWARE
danmark a/s