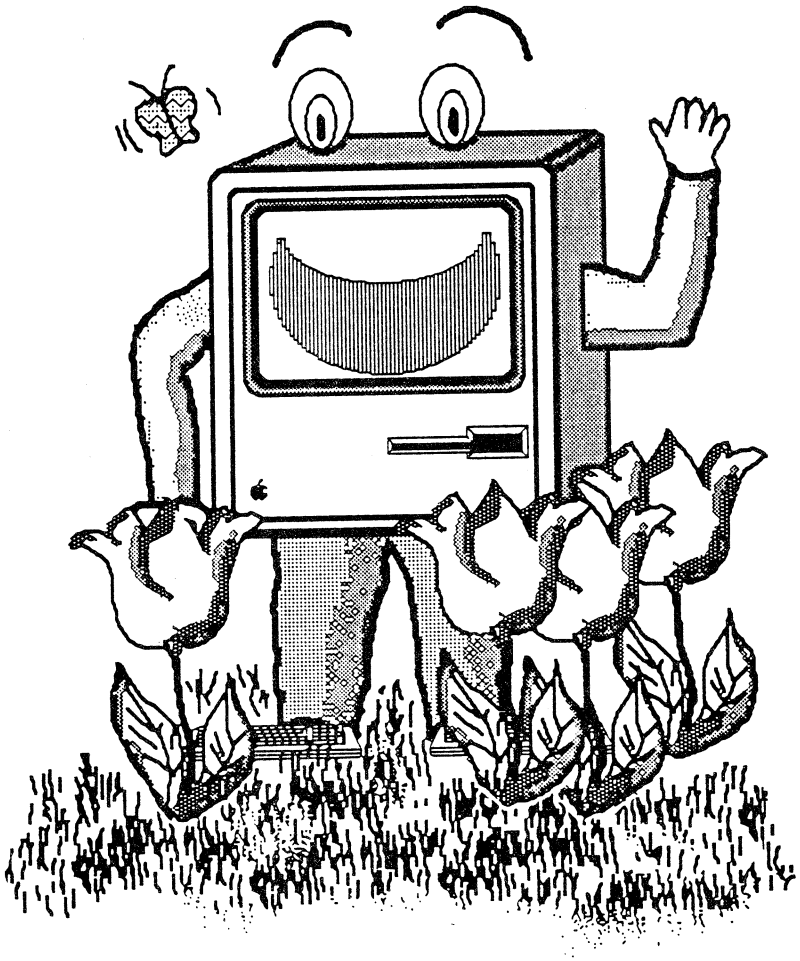
RUN-NYTT

Nr. 1
Årg. 16
5. mai 1989

Informasjonsorgan for RUNIT-D
Regnesentret ved Universitetet i Trondheim - Dataseksjonen



Lang artikkel om
DATAVIRUS på side 18!

RUNIT - DATASEKSJONEN

En oversikt over steder hvor brukerne kan henvende seg

1) DATASEKSJONENS EKSPEDISJON
Sted: 2. etg SB2, NTH.
Åpningstid: 1000-1400
Telefon: (59)3028

Generell informasjon
Brukerregistering
Salg av informasjon og programvare
Utdeling av diverse skriftlig informasjon

2) RUNITs MASKINHALL
Sted: Lerkendal
Betjent 0800 - 2100
Telefon (59)3025

Spørsmål om brukerens kjøringer
Magnetbåndmontering

3) FEILMELDINGSTELEFON-DATANETT
Sted: Maskinhallen, Lerkendal
Telefon: (59)2062
Betjent i maskinhallens åpningstid.

Melding av teknisk feil med terminallinjer og datanett generelt.

4) TEKNISK GRUPPE
Sted: 2. etg SB2
Telefon: (59)2978 -
0800 og 1600

Melding av teknisk feil på utstyr som RUNIT har vedlikeholdsansvar for.

5) VEILEDNINGSTJENESTE
RUNIT's brukere kan for å få hjelp, henvende seg til enten:

a) RUNIT's brukerstøttetelefon
b) RUNIT's orakeltjeneste

a) Brukerstøttetelefonen:
Sted: Gruppe for systemdrift og ytelsesvurdering, Lerkendal
Telefon (59)3024

Betjent 0800 - 1600. Etter kl. 1600 settes telefonen over til maskinhallen, og betjeningen der kan ta imot spørsmål og bringe dem videre neste dag.

Alle typer spørsmål kan ringes inn - betjeningen bringer dem videre!

Spesielt kan en ringe dit med spørsmål innen emner som:

. operativsystem - på NORD, SPERRY, VAX, CRAY, IBM
. editorer
. datanett
. UNIX - finnes på VAX 11/750
. bruk av magnetbånd
. innlegging av programvare på RUNIT's maskiner:
. maskinnær programmering
. elektronisk post - EAN, EARN

NB! Dette er bare en telefontjeneste.

b) Orakeltjenesten
Sted: 2. etg. SB2
Telefon (59)3004

Denne tjenesten er betjent av studenter, og er åpen 1000 - 1600 i høst- og vårsemesteret.

Også her kan en komme med alle typer spørsmål. Spørsmål bringes videre hvis oraklene ikke greier spørsmålet selv med en gang.
Studentene SKAL bruke denne tjenesten når den er betjent.

Spørsmål kan ringes inn, eller en kan møte opp og få hjelp!
Spørsmål kan også stilles vha. elektronisk post - til følgende adresser:

EAN:
orakel@vax.runit.unit.uninett

EARN:
orakel at norunit

DECnet:
RUNIT::ORAKEL

Emner som orakeltjenesten dekker spesielt:
. bruk av programvare innen matematikk, statistikk og grafikk
. språk - FORTRAN, PASCAL, SIMULA, C
. mikromaskiner - DOS, kommunikasjon mellom PC og stormaskin

6) PC - DEMOROM
Sted: 2 etg. SB2
Telefon: (59)6923
Betjent 1200 - 1500 mandag, onsdag og fredag

Informasjon og demonstrasjon av mikromaskiner, og programvare for slike maskiner. Veiledning ved kjøp av mikromaskiner.

7) SUPERDATAMASKIN-SENTRET
Sted: 5.etg, SB2
Telefon: (59)3048
Betjent i kontortiden:
0800 - 1600

Informasjon om bruk av CRAY og om programvaretilbud på CRAY.
Hjelp i programmering på CRAY.

RUN-NYTT

Adresse:	RUNIT 7034 Trondheim
EAN-adresse	vik@vax.runit.unit.uninett
Redaksjon:	Knut L. Vik Tlf. 07 593047 Anne B. Reitan Sivertsen Tlf. 07 593027
Utgivelse:	4 nummer pr. år
Abonnement:	Gratis ved henvendelse til RUNITs ekspedisjoner eller redaksjonen
Opplag:	1500
Trykkeri:	Nidaros Trykkeri, Trondheim
Bidrag:	Mottas med takk

Bruk gjerne artikler fra RUN-NYTT, men oppgi kilde!

INNHOLD:

Nyheter innen datalagring

Den teknologiske utviklingen går meget raskt, ikke bare for datamaskiner, men også for datalagring.

Det er ikke så lenge siden disketter var på 360 Kbyte, og at 10 Mbyte harddisk var en luksus. Idag?? Hvem ønsker ikke den raskeste maskina, med 60-100 Mbyte disk, streamertape og optisk disk? Mens disketter bare rommer usle 1 Mbyte!

Optisk lagring, ut fra samme teknologi som CD-plater for lyd, blir nå mere vanlig, ikke minst for distribusjon av data. Det er f.eks. flere leverandører som nå tilbyr sine hyllemetre med håndbøker på 1 CD-ROM-plate.

Men det skjer mere:

. Det kommer nå på markedet 3.5 tommers disketter på 20 og 40 Mbytes, de vil lett konkurrere med tape for sikkerhetskopiering

. Enda mere interessant er utviklingen av det som kalles "elektronisk papir", hvor CD-teknologien ikke fremstilles på harde plater, men som "papir".

  Det åpner for nye muligheter, f.eks. å lage disketter av dette materialet. Hva det gir av kapasitet? Hva med: 5.25 tommers disketter på 1000 Mbyte, eller 2 tommers disketter (til foto-apparatet eller video-kameraet?) på 100 Mbyte, vanlig 12 tommers magnetbånd på 1000 Gbyte (1 000 000 Mbyte), eller hva med noen Mbyte i kredittkortformat?

Så når vi ønsker tilgang til, og krever, mere plass for datalagring, går vi spennende tider i møte.

Priser? Tja, det blir nok ikke billig, i hvert fall ikke til å begynne med. Så jeg får nok nøye meg med disketter og harddisk en stund enda.

Bjørn Gifstad

Programvare-formidling

Utviklingen går mot at det blir mer og mer lokale datamaskiner - PC-er og større maskiner. Disse maskinene må ha tilgang til nødvendig programvare -ved at hver maskin har sin kopi, eller ved at en over nett har tilgang til felles filtjener med programvare.

Det betyr at det i UNIT/SINTEF miljøet trenges mange eksemplarer av noen programvareprodukt. Rundt om vil det også brukes ulike program for samme oppgave. Noen vil benytte bedre programvareverktøy enn andre. Det siste vil ofte skyldes at en ikke har hatt tid til å prøve andre produkter, men også at en ikke har fått vite om hvilke nyttige program naboen har, eller hva som ellers finnes på markedet.

Tidligere, da alle brukte en felles stormaskin fra en kortleser eller en terminal, kunne en kjøpe inn ett eksemplar av viktige programprodukt, og da anerkjente produkt av god kvalietet. Alle hadde tilgang til samme programvare. Det var ikke ekstra kostnader for den enkelte ved å benytte programvare.

Dette er selvsagt tilfellet for stormaskiner i dag også, og det vil alltid finnes programvare som er for stor eller for dyr til at en kan kjøpe den til sin egen PC. Så det vil kunne være nyttig å ha en stormaskin i bakhånden for mange. Det kan også være at en må over på en større maskin fordi utførelsen på ens egen maskin tar for lang tid.

Det foretas store investeringer i lokal maskinvare for tiden. Et viktig spørsmål er hvordan en på programvaresiden kan effektivisere utnyttelsen av denne maskinparken.

En annen måte å stille spørsmålet på, er hvordan UNIT/SINTEF miljøet skal få tatt i bruk best mulig programvare på rimeligst måte, og hvordan en skal unngå at alle skal finne opp hjulet på nytt.

Det er dårlig økonomi for institusjonene at lokalmiljøene kjøper samme programvare hver for seg til full pris, hvis en ved å stå samlet kan oppnå mengderabatt. Det krever dog at mange velger samme verktøy for samme oppgave.

Programvarebehovet i et ingeniørteknisk miljø er heller ikke helt tilpasset hyllevaretilbudet i en programvarebutikk, så det vil alltid her foregå egenutvikling av programvare, og utprøving av eksisterende programvare litt utenfor den slagne landevei.

Programvare for, og erfaring i samspill mellom små og større maskiner er det vikig å ha i et miljø som dette.

Et viktig svar på det spørsmålet vi stilte, er informasjon, og hjelp til å knytte kontakt mellom dem som spør om hjelp og den som har erfaring. Det er også nyttig at erfarne brukere møtes og utveksler erfaringer og gode tips.

En programvareformidlingstjeneste er et annet svar. Det kan inngås "site" lisens for viktig mye brukt programvare slik at en kan kopiere programmet fritt i miljøet. En kan oppnå avtaler for innkjøp av enkelteksemplarer til redusert pris, og en kan formidle god gratis programvare. Slik gratis, eller nesten gratis, programvare finnes det ikke minst mye av for undervisnings- og forskningsmiljøer. Gjennom de internasjonale forskningsdatanettene er det meget enkelt å få tak i mye - både bra og mindre bra. En viss siling og kvalitetsvurdering kan være lurt.

Det er hverken juridisk eller moralsk rett å piratkopiere programvare. Det gjelder også programvare som er "nesten" gratis, dvs. at programvaren spres fritt for utprøving, men forfatteren vil ha en liten sum hvis den tas i bruk.

Med utviklingen av nett og filoverføringsprogram, er forholdene lagt til rette for en enkel programformidlingstjeneste for all gratis programvare. Også felles innkjøpt programvare kan i noen tilfeller

formidles gjennom en slik kanal med et passende sikkerhetsopplegg.

Programformidling har lenge vært en side av RUNIT's tjenestetilbud til UNIT/SINTEF miljøet. Vi har inngått "site" avtaler, vi har tatt inn og selger visse PC program som vi mener er nyttige for miljøet og som ikke så enkelt er å få tak i hos en vanlig programvaredistributør. I en annen artikkel i dette RUN-NYTT viser vi hva vi i dag tilbyr.

Vi har også filer med gratis programvare hvor alle brukerne kan forsyne seg selv. Dette er i dag først og fremst programvare for PC, bl. annet diverse hjelpeverktøy - slikt som også kan finnes på oppringbare BBS-er. I artikkelen "Programvarenytt" i dette RUN-NYTT nevnes 2 nye gratis program og ny utgave av KERMIT. PC programvaren finnes i underkataloger under katalog DISK3:<PC> på RUNIT's VAX 8600. Start med å lese filen AA-READ.ME på denne katalogen.

Vi tilbyr også kildekodeutgaver av en masse matematiske subrutiner (i FORTRAN). Vi har kalt biblioteket SYMBLIB - og rutinene er tilgjengelig på VAX 8600 og SPERRY (UNISYS).

Start på VAX8600 med å lese filen SYMBLIB.INFO i katalog DISK4:<PROGRAM.SYMBLIB>.
Logisk navn SYMBLIB peker til denne katalogen. Merk at denne programvaren er mottatt til bruk innen forskning og undervisning.

Vi har også tatt i bruk endel nyttige hjelpeprogram under VAX/VMS som også er gratis, og som andre kan få, bl. annet "UNIX" type verktøy. Se RUN-NYTT nr 4, 1988, s 14. Andre VAX/VMS installasjoner har sikkert annet nyttig.

Det finnes mye programvare for UNIX maskiner tilgjengelig på ulike steder som nye installasjoner bør ha glede av.

Tilsvarende finnes det mye gratis programvare for MAC som vi også kan legge ut på filer.

I en tid med angrep av virus og annet grums, kan en slik formidlingstjeneste være nyttig ved at programvaren sjekkes før den legges inn på VAX. Mens den er der, kan den ikke smittes. Alle kan hente fra samme kilde - istedenfor å bytte disketter, som kan være en forurensningskilde.

Vi mener dette er en nyttig tjeneste - hva mener du?

Har du nyttig program du vil dele med andre, og som vi kan formidle?

Har du program du vil anbefale til oppgaver også andre utfører?

Har du noe nyttig skriftlig informasjon vi kan formidle vha. informasjonsfiler tilgjengelig for alle?

Er det noen typer gratis program du savner i vårt tilbud?

Vet du om noen spesielt nyttige kilder for programvare?

Finnes det i miljøet lokal formidling av gratis programvare?

Knut L Vik

Siste NYTT

"site" lisens for statistikksystemet SAS

Etter et utstrakt samarbeid på tvers i miljøet, har vi fått i stand et "spleiselag" som har gjort det mulig å finansiere en "Campus licence" for PC-utgaven av SAS-systemet. Alle moduler er med.

SAS finnes for de fleste maskintyper, og det er aktuelt å anskaffe enkelte moduler for VAX. Da kan en utnytte både PC'ens gode egenskaper og VAX sin større behandlings- og lagringskapasitet.

SAS er et omfattende system, og krever i praksis en rask AT-maskin med disk.

Er du interessert? Er du nysgjerrig på betingelsene? Kontakt undertegnede!

Bjørn Gifstad, RUNIT-D

Tlf. 592966

Ny adressestandard i UNINETT for elektronisk post

UNINETT skal nå ta i bruk ny adressestandard for elektronisk post.

Dette medfører:

- vi må ta i bruk nye uvante adresser. Hvordan adressen skal skrives i en melding, vil avhenge av postprogrammets brukergrensesnitt.

- det blir mer logiske adresser som vil vise naturlig organisasjonstilknytning

- vi bruker internasjonal adressestandard - en standard som blir tatt i bruk nå rundt i verden.

- vi vil være forberedt for samtrafikk med nye X.400 MHS installasjoner - også utenfor forsknings- og undervisnings-verdenen.

- vi får bedre samtrafikk med andre postnett, som Internet og EARN/BITNET.

- en katalogtjeneste vil eksistere.

- det blir en enhetlig måte å oppgi adresser på, adresser som kan brukes uavhengig av hvor en er i verden.

- nye postprogram vil bli tilgjengelig - også på nye maskintyper.

Standard for elektronisk post

UNINETT benytter idag programvare som baserer seg på CCITT's X.400 MHS standard for elektronisk post. MHS står for "Message Handling System".

UNINETT har til nå distribuert postprogrammet EAN, som var den første installasjonen av denne standarden.

Alle installasjoner rundt i verden som bruker denne standarden, danner et felles postnettverk for forskere - "R&D MHS Service". Post til og fra andre netterk, dvs. til og fra installasjoner med postprogram som bygger på andre standarder, må passere en portner, som er en datamaskin som oversetter det som er nødvendig mellom postnettverkene.

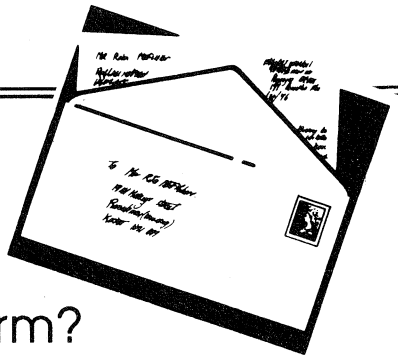
Adressestandard

Formen på den elektroniske postadressen - hvordan adressen ser ut og er bygget opp, er beskrevet i den standarden en bruker. I X.400 standarden er det definert en rekke adresseattributter - en har delt adressen opp i en rekke adresseenheter. Hver attributt har sitt navn som skrives sammen med tilhørende verdi når de brukes. (Eks.: C=no; - med ; til slutt!)

Alle disse attributtene trenger en ikke bruke f. eks. i Norge, men ved at de er definert, og blir forstått av postprogrammet, kan en rundt i verden bruke de attributter en synes er mest hensiktsmessig. En delmengde av disse attributtene - i en bestemt rekkefølge - danner en standard attributt adresse (SA adresse). Det er denne adresseformen som skal innføres innen UNINETT. Det er ikke nødvendig for en installasjon å ta i bruk alle attributtene i en SA adresse - men noen er nødvendige.

Da EAN ble laget i 1984, hadde ingen tatt i bruk SA adressene slik de var definert i standarden. De som laget EAN ved University of British Columbia i Canada valgte da å ta i bruk en annen metode - de brukte såkalte "domain defined attributes" til å lagre adressene på samme form som brukes innen Internet. Denne adressen kalles også en RFC adresse - etter definisjonsdokumentet RFC 822. På den måten fikk de en adresse som var tilpasset det ene store nettet i USA.

UNINETT tok i bruk EAN meget tidlig - i 1985 - og det er stadig RFC adresseformen vi bruker. Dette er en meget kompakt måte å skrive en adresse på, og det er praktisk å bruke samme adresseform som Internet bruker - et nett som også mange innen Norge er tilknyttet.



Hvorfor forandre adresseform?

Det viktigste svaret er at vi ønsker å sikre tilknytningen til nye X.400 tjenester som etter hvert dukker opp (eksempel: offentlig MHS. Andre FoU miljøer i Europa har valgt det samme. CEN/CENELEC er en europeisk standardiseringsorganisasjon som har definert en "funksjonell" standard for elektroniske postprogram. De sier at et postprogram skal bygge på X.400 standarden, og at programmet må håndtere SA adresser. Det er ikke nødvendig å kunne håndtere RFC adresseformen - det er dog mange implementasjoner som kan det. Dette er vel å merke SA adresser på RFC form, dvs. at det finnes en entydig oversettelse mellom de to formene.

Dette betyr at hvis vi i Norge skal kunne ta i bruk nye postprogram på eksisterende og nytt utstyr, og ha kontakt med nye postinstallasjoner rundt om, bør vi kunne sende og motta post som bruker denne adresseformen. Derfor blir SA adresser standard adresseformat innen UNINETT MHS , og post fra installasjoner med nåværende EAN adresseform må først oversettes i en portner til SA adresse, og så sendes ut i verden.

Norsk Data's X.400 implementasjon bruker SA adresser. Viktige X.400 implementasjoner vil i framtida komme for lokale datanett - f. eks. PC nett, og disse vil sikkert benytte internasjonal standard, dvs. SA adresseformen.

Et annet argument for omleggingen er nye tjenester som blir mulig med programvare som bruker SA adressering. En slik tjeneste er katalogtjeneste. For brukerne betyr det at det vil være tilgjengelig en katalog med brukernes elektroniske postadresser. En ber om en eller flere adresser i et elektronisk brev til katalogtjenestens adresse. (med kommando f. eks. Find olsen). Dette er en etterspurt tjeneste i dag. En slik katalogtjeneste vil også brukes av postprogrammene til å bestemme veien en melding skal sendes fra en node til en annen.

UNINETT vil etablere en nasjonal katalogtjeneste hvor brukerne ved installasjoner som har innført SA adresser kan registere seg.

Det finnes en egen CCITT standard for katalogtjeneste - X.500 standarden. Etterhvert vil det finnes både egne program for denne tjenesten bygd på denne standarden, og katalogtjeneste vil kunne være en del av postprogrammet, slik at en installasjon kan ha en egen lokal adressetjeneste. Merk at en slik adressetjeneste vil være tilgjengelig fra hele verden.

Et tredje argument er at UNINETT installasjonene med SA adresser går over til å bruke landkoden NO - som er rett navn ifølge internasjonal navnestandard. I dag er toppdomenenavnet UNINETT, som ikke er selvforklarende og ikke alle vet om i utlandet. Internettet bruker NO som toppdomenenavn, og UNINETT vil samordne navngivningen av noder innen X.400 MHS og Internet verdenen. UNINETT sekretariatet er såkalt "naveautoritet". Dette betyr at når en adresse er skrevet i RFC notasjon, kan en ikke uten videre vite om det er en X.400 MHS eller en Internet adresse - begge slutter med .NO

I dag er det overfor utlandet mye uklarhet når det gjelder hvordan vi skal oppgi vår MHS adresse, om vi skal oppgi portneradresse når nettgrenser skal passeres, om UNINETT som toppdomene er kjent, etc.

Ved å bruke internasjonal standard, og med navnetjenere tilgjengelig, vil våre adresser bli entydig forstått, og meldingene blir sendt til oss automatisk. Vi må dog oppgi vår adresse - på visittkortene f. eks., på 2 måter - både på SA adresseform og RFC form. De som skal sende oss meldinger, vil kjenne igjen enten den ene eller den andre adresseformen.

Standard attributt adresse

De viktigste og mest brukte adresseattributtene er:

G= ;	: fornavn
S= ;	: etternavn
OU= ;	: organisasjonsenhet(er)
O= ;	: organisasjon
P= ; evt PRMD= ;	: nettorganisasjon
A= ; evt ADMD= ;	: administrasjonsenhet
C= ;	: land

Nettorganisasjon er den organisasjon som tilbyr nettjenesten - i NORGE er det UNINETT for forsknings- og undervisningsinstitusjoner. En adresse kan bestå av flere organisasjonsenheter. Merk at adressen inneholder den organisasjon vi tilhører - det er ikke noe

→

UNINETT forts.

attributt for den maskinen meldingen til slutt skal havne på. Det kan være flere maskiner innenfor en organisasjonsenhet, og fordelingen av meldingene til rett maskin for en bestemt bruker skjer lokalt. Det er også mulig å ha forskjellig O= ; og OU= ; attributt for brukere på samme maskin.

En adresse vil se slik ut - med attributtene i følgende rekkefølge:

G=Alf; S=Hansen; OU=elab-runit; O=sintef;
P=uninett; C=no;

På RFC form - på "standard domain attributt" form blir denne adressen:

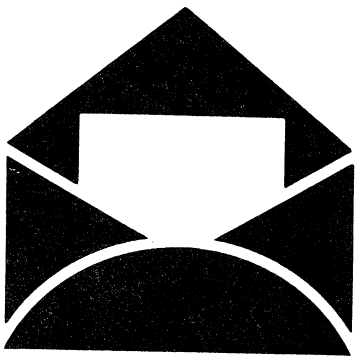
Alf.Hansen@elab-runit.sintef.no

Det er denne adressen som Internet-brukere skal bruke til Alf Hansen.

Begge disse formene skal stå på Alf Hansens visittkort.

UNINETT bruker ikke ADMD.

Nye adresser



Hvor mye vi må, evt. bør, forandre vår adresse når vår installasjon går over til SA adresser, vil variere. Det avhenger for det første om de nåværende domener — leddene til høyre for @ - blir oversatt ledd for ledd til SA atributter. Dette er en lokal avgjørelse i samarbeid med "UNINETT navneautoritet".Det er heller ikke alltid en slik oversettelse er mulig. Det vil bli endel forandringer rundt om.

UNINETT anbefaler alle å bruke både fornavn og etternavn, dvs. både G= ; og S= ;.

I stedet for de norske bokstavene æ, ø og å brukes a, o og a - i henhold til en nordisk telerekommendasjon.

I en overgangsperiode vil det være mulig å bruke både gammel og ny adresse - slik at en ikke trenger gi allebeskjed om ny adresse over natta.

Brukergrensesnitt

Den nye adresseformen slik den er etter definisjonen, kan for mange virke langt mer tungvint å bruke enn RFC formen, som er meget kompakt og fort å skrive. Men hvordan SA adressen skal skrives av brukerne, vil avhenge av brukergrensesnittet for det postprogrammet som er installert. Det kan være at en kan skrive adressen på RFC formen, eller en blir hjulpet av en skjermmeny.

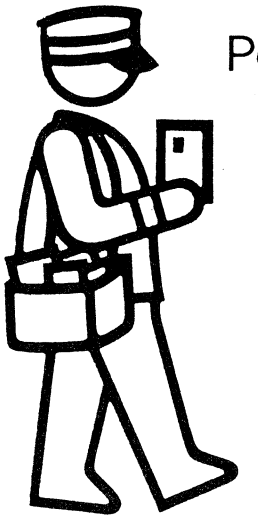
Men uansett må en vite om og forstå SA adresseformen - denne formen vil en kunne få fra andre X.400 MHS brukere, og en selv må kunne oppgi den. En som i det daglige skriver SA adressen på RFC formen , og oppgir sin adresse på denne formen til en som f. eks. bruker et menysystem, kan ikke forutsette å bli forstått - særlig hvis den andre brukeren er en lite erfaren nettbruker.

I den versjonen av EAN (2.1) som nå er installert rundt om, er det bare mulig å skrive SA-adressen slik den er definert - med alle attributtene. Det finnes en videreutviklet utgave av EAN fra Tyskland - DFN-EAN - som også tilbyr å bruke RFC formen. Utgave 3 av EAN skal visst også inneholde denne muligheten, og denne utgaven kommer antakelig i løpet av året. UNINETT vil tilby DFN-EAN, ev. EAN v. 3, i forbindelse med omleggingen, slik at de som måtte ønske det kan beholde RFC-adresseformen.

Det kan også for å forenkle skrivingen av adressen være lurt å utnytte mulgheten for å definere kortnavn - alias - for mye brukte adresser.

Post til utenlandske X.400 MHS installasjoner

Alle land har en landkode på to bokstaver. Hvilke attributter som brukes, vil avhenge fra land til land, og fra installasjon til installasjon. Noen land - som Tyskland og Belgia - bruker i dag ADMD=xxx;. Uavhengig av brukergrensesnittet vil postprogrammet oversette den mottakeradressen vi oppgir til SA form, og meldingen vil komme fram.



Post til andre nett

Følgende eksempler viser hvordan adressen til mottakere på andre nett - som EARN/BITNET og Internet - blir på SA adresseform.

Om en i brev som en sender skal skrive adressen slik, avhenger av brukergrensesnittet i postprogrammet. Hvordan avsenderens adresse vises i mottatte meldingers "From" felt avhenger også av brukergrensesnittet. Postprogrammet oversetter adressen fra den formen vi skriver den på til SA formen, og meldingen sendes fra oss til en portner. Portneren forstår SA formen, og sender meldingen til rett nett.

Til Internet:

a) Norsk adresse:

Internet adresse: ole@ifi.uio.no
SA form: S=ole; OU=ifi; O=uio; C=no;

Til Internet brukes ikke P=UNINETT;

b) Svensk adresse:

Internet adresse: ole@nadja.stacken.kth.se
SA form: S=ole; OU=nadja; OU=stacken; O=kth; C=se;

Her settes landkoden se, som både brukes av Internet og X.400 MHS, inn i C= ; Meldingen sendes over X.400 nettet til en Internet portner i Sverige.

c) Amerikansk adresse -
hvor det ikke er landkode på to bokstaver:

Internet adresse: netlib@research.att.com
SA form: S=netlib; OU=research; O=att; P=com; C=no;

Toppdomenenavnet settes inn under P= ; og C=no; brukes. Det betyr at meldingen skal sendes til den norske Internet portneren.

Til EARN/BITNET:

Bitnet adresse: jnpt1@nuyvm1.bitnet
SA form: S=jnpt1; O=nuyvm1; P=bitnet; C=no;

Her sendes meldingen til den norske EARN/BITNET portneren.

Tilsvarende som dette blir det til andre nett. Når landkoden har to bokstaver, settes den inn i C= ;. For de andre nettene som ikke har standardiserte nettnavn (vanligvis på mer enn to bokstaver), plasseres navnet i P= ;, og med C=no;, slik at meldingen sendes til den norske portneren. Hvis meldingen har kommet inn i X.400 nettet gjennom en portner i et annet land, vises det i meldingens "FROM" felt - i C= ;

Når en mottar post fra andre nett, vil den korrekte SA formen - evt. oversatt til den formen brukergrensesnittet benytter - vises i meldingen, og også "REPLY" kommandoen vil fungere mhp. adressen.

UNINETT portnere

UNINETT vil sende post til andre nett gjennom følgende portnermaskiner:

1) Mellom nåværende EAN installasjoner med RFC adresse og X.400 MHS installasjoner med SA adresser:

   RUNITs VAX 8600 (RUVE)

   Denne portneren trenges i en overgangsperiode.

2) Mellom X.400 MHS installasjoner med SA-adresser og Internet:

   NAC - som er en SUN/UNIX maskin på Kjeller

3) Mellom EARN/BITNET og Internet:

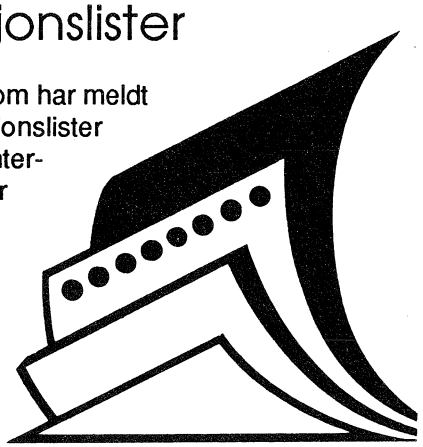
   RUNIX - som er en VAX/ULTRIX maskin i Trond heim.

Dette betyr at post mellom EARN/BITNET og X.400 MHS nettet med SA adresser må passere portnerene RUNIX og NAC.

UNINETT forts.

Men, merk at dette trenger ikke brukerne bry seg med, postprogrammene sender til rett portner automatisk!

Distribusjonslister



Det er mange som har meldt seg på distribusjonslister både lokalt og internasjonalt. Nå blir adressene endret for mange. Den som er lokal UNINETT MHS ansvarlig, vil endre adressene i de distribusjonslistene som er opprettet lokalt. Men alle må selv melde adresseforandring til listeansvarlig ellers i Norge og i utlandet.

UNINETT planlegger å etablere et videredistribusjonssystem i Norge for spesielt populære lister fra utlandet, så en slipper at nettlinjene fra utlandet belastes med mange like kopier av hvert innlegg. Dette utgjør en stor trafikkmengde i dag.

Tidsplan

De tre portnerne ble operative i april, så nye installasjoner bør ta i bruk SA adresser fra starten av. Eksisterende installasjoner kan konvertere hvis ønskelig når portnerne er operative.

For mange er det vesentlig at det før adressekonverteringen skjer, foreligger et postprogram som tilbyr et alternativt brukergrensesnitt til det å skrive rene SA adresser. DFN-EAN kan antakelig benyttes, og den skal uttestes.

Massiv adressekonvertering i UNINETT MHS planlegges foretatt i sep-okt 1989. Da har en samlet nok erfaring omkring det praktiske.

Knut L. Vik

Vi minner om:

Brukerinformasjon kan alle hente selv:

Fra filer på VAX 8600:

Les filene:
INFO:READ. ME og NETTINFO:READ.ME

Fra filtjeneren INFOSERV - med elektronisk post:

Adressen til INFOSERV:

EAN:
INFOSERVÄRUNIX.RUNIT.UNIT.UNINETT

EARN:
INFOSERV at RUNIX.RUNIT.UNIT on UNINETT

Internet:
INFOSERVÄRUNIX.UNIT.NO

DECnet:
RUNIX::INFOSERV

Send første kommandoen HELP - i meldingens emnefelt eller som første (og eneste) linje i meldingen.

UNINETT prosjektet har opprettet filtjeneren UNINETTINFO. Adressen er som over med UNINETTINFO istedenfor INFOSERV.

Se ellers RUN-NYTT nr. 4 1988.

Spørsmål kan sendes Orakeltjenesten gjennom elektronisk post:

Adresser:

EAN:
ORAKELÄAVX. RUNIT.UNIT.UNINETT

DECnet:
RUNIT::ORAKEL

EARN:
ORAKEL at NORUNIT

Svar vil komme tilbake samme veg, eller oraklene kan ta kontakt hvis telefonnummer oppgis.

Programvare som RUNIT-D formidler

RUNIT-D har "site" lisenser for noen program-produkter - først og fremst for distribusjon innen UNIT og SINTEF. I tillegg er noen få program for PC til salgs i RUNIT's ekspedisjon.

Her følger en oversikt over det som er tilgjengelig:

"Site" lisenser:

1) INGRES.

Programtype:	Databaseprogram
Maskintyper:	VAX/VMS, UNIX (SUN) og MS-DOS maskiner
Til:	UNIT/SINTEF
Kontakt:	Steivor Bjarghov, tlf. (59)3002

2) TEX

Programtype:	Tekstbehandlingsprogram
Maskintype:	MS-DOS maskiner (34 disketter!)
Til:	UNIT/SINTEF
Kontakt:	RUNIT's ekspedisjon, tlf. (59)3028

3) UNIRAS

Programtype:	Grafikkprogram - subrutinesamlinger og interaktive program
Maskintyper:	VAX/VMS, UNIX, NORD-500
Til:	UNIT/SINTEF. Frontendmaskiner mot CRAY ved de andre norske universitetene.
Kontakt:	Superdatamaskinsentret,tlf (59)3048

4) SAS

Programtype:	Statistikkprogram
Maskintype:	MSDOS maskiner
Til:	UNIT/SINTEF
Kontakt:	Bjørn Gifstad, tlf (59) 2966

I tillegg er en avtale under utarbeidelse for Word-Perfect produkter - WordPefect, PlanPerfect, Data-Perfect og WP-office. Nærmere opplysninger vil bli gitt senere. Avtalen gjelder for MSDOS PC'er og Mac-intosh maskiner.

RUNIT formidler følgende programvare fra NAG for VAX/VMS og NORD 570 i UNIT og SINTEF miljøet:

- NAG matematiske subrutinebibliotek
- NAG Graphical Supplement
- NAG Online Supplement

Dette er produkter som er installert på RUNIT's egne maskiner, og som derfor kan tilbys rimeligere til andre installasjoner av samme type.

Programvare som selges i RUNIT's ekspedisjon:

1) KERMIT for MSDOS maskiner

Dette er både et terminalprogram og et filoverføringsprogram.

Dette er et tilbud til dem som ikke kan hente KERMIT fra RUNIT's VAX 8600. Prisen dekker distribusjonskostnadene.

Det er også mulig å få kjøpt disketter med KERMIT for ND.

2) Terminalprogrammet VT100 fra Terje Mathisen

Dette programmet har RUNIT solgt i en rekke år. Gjeldende utgave som selges er v. 5.04k.

Programmet inneholder en VT100 og en TDV NOTIS terminal, og KERMIT filoverføring med bl. annet oversetting av æ, ø og å.

Dette programmet selges til UNIT/SINTEF miljøet og kunder på RUNIT's maskiner

3) MATCALC

Dette er et meget nyttig og billig beregningsprogram. Se tildligere nummer av RUN-NYTT om dette programmet (eks. nr. 2 1988, s 26)

Forts. side 15

GPGS-F Versjon 88-0

Som nevnt i RUN-NYTT nr. 3-1988 er det fremdeles liv i programpakken GPGS-F. I strid med hva mange trodde, har systemet ikke blitt utkonkurrert av GKS og andre standarder; det er faktisk stadig et økende antall brukere av GPGS-F. Antall nye brukere er særlig stort for Unix-versjonen, som er installert på bl.a. Sun, VAX/Ultrix, HP-9000 og Alliant FX.

GPGS-F har i løpet av de siste 1-2 år blitt utvidet med flere nye muligheter, og derfor gis det nå ut en ny versjon av systemet. Den nye versjonen har fått versjons-nummer 88-0 (det var meningen den skulle være klar i fjor).

Det er også skrevet ny utgave av GPGS-F User's Guide (7th Edition) som fås kjøpt på Tapir bokhandel (kr. 240).

Det følgende er en kort oppsummering av nye muligheter i versjon 88-0 i forhold til forrige versjon.

Bruker-definerte linjetyper

Det er mulig å definere linjetyper som en sekvens av synlige/usynlige linjesegmenter, hvor brukeren angir lengden på hvert segment. Det er også mulig å angi at linjesegmentet skal ha en gitt vinkel i forhold til retningen på linjen som tegnes.

I tillegg er det nå mulig å tegne tykke linjer, som en sekvens av parallelle linjer. Brukeren har full kontroll over total linjebredde og avstanden mellom enkeltlinjene.

Bakgrunnsdevice

Det er på en enkel måte mulig å få kopi av skjermbildet ut på plotter, med størrelse angitt av bruker.

Utvidet feilmeldingsformat

GPGS-F feilmeldinger har tidligere kun skrevet ut et feilnummer og et rutinenummer hvor feilen har oppstått. Det er nå mulig å få skrevet ut både feilteksten og navnet på rutinen som gir feil. I tillegg kan man velge om feilmeldinger skal skrives ut på skjermen og/eller på en fil.

Fjerning av skjulte flater og linjer

Den største nyheten i versjon 88-0 er en ny modul for fjerning av skjulte flater og linjer. Denne modulen kan behandle alle typer plane polygoner, og er implementert på en måte som gjør det enkelt å ta den i bruk også i gamle program. Det er ingen nye tegnerutiner som skal brukes, men de gode gamle 'LINE..' og 'POLY..' rutinene. Brukeren kontollerer en 'bryter' som sier om linjer og polygoner skal kopieres til den nye modulen for å ta del i beregningen av synlige flater/linjer. Resultatet tegnes ut ved et enkelt rutinekall.

Diverse mindre utvidelser

- Flere nasjonale tegnsett, bl.a. tysk,fransk,italiensk.
- Flere predefinerte mønstre og skraveringstyper for polygonfylling.
- Mulig å benytte opptil 8064 predefinerte hardware mønstre, mot tidligere 128.
- Det er ikke lenger nødvendig å tegne samme polygon to ganger hvis man ønsker både fylling og omriss.

Drivere

Det er også utviklet flere nye drivere i det siste. Det gjelder bl.a.

- Tandberg 1200 (RUBY)
- Tektronix 4510 rastreriseringsenhet
- VT 340
- ND Technostation
- ND-720/730 laserskrivere
- Interface mot X.11 (snart klar)
- CGM generator (foreløbig kun 'Clear Text Encoding')
- PostScript (klar til sommeren/høsten)

(Extended) GRAPHISTO

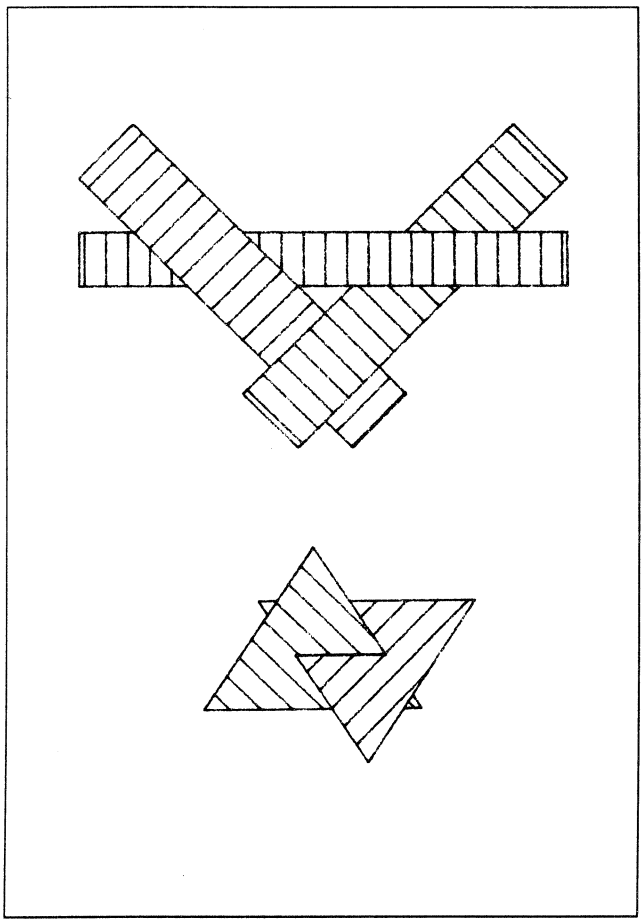
Det finnes fremdeles to utgaver av GRAPHISTO. Den 'gamle', som har vært uendret i snart 10 år, og den nye 'Extended GRAPHISTO'. Den gamle vil forhåpentligvis forsvinne i løpet av året, og 'Extended GRAPHISTO' vil overta dens plass også utenfor NTH/SINTEF.

SURRENDER

SURRENDER har også blitt utvidet en god del i det siste, men problemet er at dokumentasjonen foreløbig ikke er oppdatert tilsvarende. Ny SURRENDER brukermanual vil bli skrevet i løpet av året.

Spørsmål?

Kontakt Magnar Granhaug
ELAB-RUNIT
Tlf. 592963



Konvertering av filer mellom DOS-verdenen og Mac-verdenen

Har du dokumenter laget ved hjelp av DOS programmer, og vil ha disse over til en Macintosh eller omvendt? Dette problemet lar seg løse på flere måter, og hvis det dukker opp ofte, vil jeg anbefale deg en permanent løsning. Ta kontakt hvis du vil diskutere alternativer.

Det jeg skal fortelle om nå, er hvordan vi kan ordne en slik konvertering ved hjelp av det utstyret vi har på RUNITs demorom. For å få gjort det, trenger vi den/de filene som skal konverteres på diskett, samt en ekstra 3 1/2 " diskett.

Vi bruker følgende DOS-utstyr:

IBM PS/2 med intern 3 1/2 " intern og 5 1/4 " ekstern diskettstasjon. På denne måten kan vi håndtere begge diskettformater.

og følgende Mac-utstyr:

Macintosh IIx som kan lese, skrive og formattere DOS-disketter av 3 1/2 " format. Av programvare bruker vi Apples filkonverterer sammen med MacLink Plus. Dermed kan vi oversette dokumenter fra en del databaser, regneark og tekstbehandlingsprogrammer. Dokumentene blir oversatt slik at de kan leses av tilsvarende programmer i den andre "verdenen". I tekstdokumenter oversettes f.eks. tabulatorer, uthevet og sentrert tekst osv.

Listen over de programmer vi kan oversette fra/til er lang, så hvis du har et behov, ta kontakt!

Kontaktpersoner:

Bjarne Kjøsnes (tlf. 592996)

Steivor Bjarghov (tlf. 593002)

Programvarenytt

GKS er installert på CRAY

Versjon 4V0 av GKS fra UNIRAS - UNIGKS - er installert på CRAY. Denne utgaven er kompatibel med versjon 5V4 av UNIRAS subrutinebiblioteket. Det betyr f. eks at UNIRAS segmentfiler laget av UNIGKS kan tegnes ut med denne UNIRAS utgaven, og at en derved har langt flere typer drivere tilgjengelig.

Mer informasjon fås ved henvendelse Superdata-maskinsentret, tlf. (07) 593048.

NAG versjon 13 (MARK 13)

Utgave MARK 13 av NAG er installert på SPERRY (UNISYS), VAX 8600 og CRAY.

Bibliotekene lenkes inn i brukerens program med samme navn som før.

På CRAY finnes biblioteket under

PDN=$NAG
ID=NAG13
OWN=PROGRAM

Prosedyren NAG tilordner denne filen.

Mark 12 er fortsatt tilgjengelig under

PDN=$NAG
ID=NAG12
OWN=PROGRAM

Se ellers: @HELP PROG.NAG
på SPERRY (UNISYS), og
HELP NAG på VAX 8600

På SPERRY (UNISYS) og VAX 8600 er også MARK 13 utgaven av informasjonsprogrammet NAG Online Supplement installert, og det startes slik:

SPERRY (UNISYS): @RUNIT*NAGDOK.ONLINE
VAX 8600: NAGONLINE

Dette programmet anbefales! En får både hjelp til å finne fram til rett rutine, og informasjon om rutinekallet og beskrivelsen av parametrene i kallet. Dette er et nyttig program også for CRAY- brukere av NAG biblioteket.

På VAX 8600 er det også en VAX/VMS HELP utgave fra NAG.
Kall: NAGVMSHELP.

På NORD 570 er fortsatt utgaven MARK 12.

TEX på VAX 8600

TEX er nå tilgjengelig på VAX 8600.
Se filen disk6:<program.tex>read.me for mer informasjon.

Den installerte utgaven av LATEX er lik utgaven for PC og SUN.

PC programvare

Følgene ny PC programvare er lagt inn på VAX 8600, og kan fritt hentes derfra:

1) PEP

Dette er et program som er skrevet av Gisle Hannemyr. Programmet kan ekspandere/komprimere tabulator, konvertere til og fra Macintosh, IBM PC, ISO 8 bits og norsk 7 bits tegnsett, fjerne kontrolltegn og annet grums. Kildekode i C og en fyldig dokumentasjon på 13 sider er inkludert i arkivfilen.

Arkivfilen heter: DISK3:<PC.PD>PEP20.ARC

Denne filen må pakkes ut med programmet ARC.

En VAX/VMS versjon av dette programmet finnes også på RUNIT's VAX 8600:

Programmet startes med RUN UTILITY:PEP

Brukerveiledningen finnes på filen:
UTILITY:PEP.DOC

2) EPSONGR

Dette er et resident hjelpeprogram for å "dumpe" EGA grafiske skjermbilder på EPSON FX-serie skrivere

(med Shft PrtSc). Programmet virker f. eks. også mot IBM's Proprinter

Programmet er ekvivalent med IBM's GRAPHICS.COM som bare virker for CGA grafikk - dette er altså GRAPHICS.COM for EGA skjermer.

Programmet er hentet fra KERMIT distribusjons-maskinen i USA.

Arkivfilen heter: DISK3:<PC.PD>EPSONGR.ARC

3) KERMIT versjon 2.32A for MSDOS maskiner

Denne utgaven av KERMIT er tilgjengelig på katalog:
DISK3:<PC.KERMIT>
Her er både programfil og dokumentasjon.
Se filen AA-READ.ME

Merk at de initialiseringsfilene RUNIT laget til versjon 2.31 kan brukes også for v. 2.32, og disse finnes på samme katalog. Det gjelder også filen NORSK.INI som oversetter æ, ø og å fra og til terminalen.

Ved filoverføring oversettes ikke de norske tegnene, så det må gjøres enten før eller etter overføringen - med program som CRUNCH eller PEP.

Av endringer fra v. 2.31 nevnes:

- I v.2.31 får en ikke feilmelding hvis en ber om en fil (med GET) som ikke eksisterer på fjern maskin - en skriver f. eks. feil navn. En får bare "Completed" og ikke noe overført selvsagt. I den nye utgaven får en beskjed om at filen ikke finnes.

- I v. 2.32 er det gjort en endring slik at liten ø (ASCII 155) sendt til IBM-PC skjermen fra den maskinen en er koplet opp mot, ikke vises. Dette tegnet oppfattes som start på en ESC sekvens. Dette er løst ved i filen NORSK.INI å oversette 7 bits ASCII ø til svensk ø (ASCII 148)

- En hel tekststreng kan legges inn i en makrovariabel

- Teksten starter og slutter med klammeparanteser.

- Nye "Skript" kommandoer:

ASK:
ASK <makronavn eller variabelnavn> <ledetekst>

Merk at ASK kommandoen ikke er beskrevet i brukerhåndboka.

Test: IF <NOT> EQUAL ord1 ord2 kommando.
IF EQUAL fører til at "kommando" utføres hvis ord1 og ord2 er like. Ord1 vil være en variabel.

ASSIGN: ASSIGN makronavn tekst
Hvis et variabelnavn finnes i "tekst", blir innholdet i variabelen del av den teksten som lagres i makro-navnet. DEFINE kommandoen brukt på samme måte overfører bare variabelnavnet.

Se ellers filen VER232.NEWS om mer om disse kommdoer, og andre nyheter i denne utgaven.

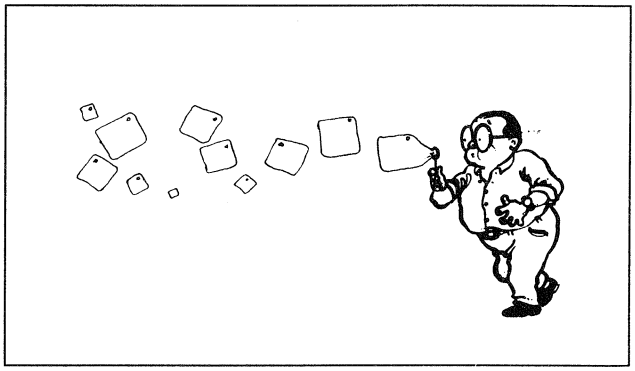
En stor håndbok er også tilgjengelig på VAX - i filen MSKERM.DOC

En Postscript utgave av håndboka er skrevet ut, og kopi kan kjøpes i RUNIT's ekspedisjon.

Versjon 2.31 av KERMIT finnes inntil videre i katalog:
disk3:<PC.KERMIT231>

Vi minner om at KERMIT inneholder en TEKTRONIX 4010 emulator, og en PC med dette programmet kan brukes som grafisk terminal.

Knut L. Vik



Programvare som RUNIT-D formidler forts. fra side 11

4) ACTO-WP

Dette er NOTIS-WP for MSDOS maskiner. Program-met selges til UNIT/SINTEF miljøet.

Gjeldende utgave er v 3.03. Sammen med program-met leveres et CLASS opplæringsprogram for ACTO-WP.

Hvordan skal vi forholde oss til virus?

En annen artikkel behandler "virus" nærmere, her benyttes virus som et samlebegrep for de definisjonene som er gitt der.

Omfanget av slike "infeksjoner" er umulig å anslå. I USA blir noen angrep rapportert, og det anslås at 200 000 maskiner var utsatt for dette i 1988. En ting er de direkte problem slike "infeksjoner" medfører, noe annet de kolossale summer det koster i tapt maskintid, direkte og indirekte lønnskostnader, og kanskje også tapte data. Hvem hørte ikke om "ormen" i fjor høst, som spredde seg til 6200 UNIX-system på få timer?

Heldigvis har de fleste virus vært rimelig godartet, selv om det kan være irriterende å bli rammet. Men det er vel bare et spørsmål om tid før en forskrudd hjerne lager noe som er virkelig destruktivt.

Jeg er imidlertid mere redd for hva en kunne oppnå hvis noen bevisst etablerte en ekspertgruppe for å infiltrere andre bedrifter eller nasjoners datasystem. Da ville en lage "virus" som ikke skulle sette spor etter seg, f.eks. ved å modifisere et komplisert operativsystem til å gi visse brukere spesielle privilegier. Med verdensomspennende datanett kan dette gi muligheter for industrispionasje og ødeleggelser en vanskelig kan fatte omfanget av.

Det finnes enklere varianter: Hva er f.eks. konsekvensene av at tyske "hackere" har solgt brukernavn og passord til amerikanske datamaskiner og nett til et østblokkland, og hva kan ha skjedd før dette ble oppdaget? Hva med om ansatte "låner bort" sine passord, klarer vi å oppdage hva som skjer?

De fleste virusangrep gjelder personlige datamaskiner. Virus er også vanskelige å utrydde, fordi de sprer seg raskt, og det er umulig å vite om alle kopier er borte. Derfor må vi regne med at virus dukker opp igjen, selv om vi har gjort vårt beste for å fjerne infiserte disketter ol..

Situasjonen vil være relativt oversiktlig så lenge det bare er frittstående maskiner som er infisert. Problemet kan få helt andre dimensjoner hvis mye brukte tjenere i et datanett blir smittet, f.eks. server i et omfattende lokalnett. Hvis det da er en utstrakt utkopiering til egen maskin eller diskett, kreves det svært restriktive tiltak for å rette opp problemene. En må også være forberedt på at sikkerhetskopier kan være infisert, slik at arbeidet med å få startet opp en "ren" tjener kan bli omfattende.

Nå må en ikke tro at større maskiner ikke er utsatt for virus. Risikoen øker etter hvert som datanett blir mer transparente, og om det er hackere eller virus som trenger seg inn, er vel av mindre betydning? Ingen kjede er sterkere enn det svakeste ledd, derfor må en respektere de restriksjoner datanett blir pålagt - det er ikke bare for å være vrang!

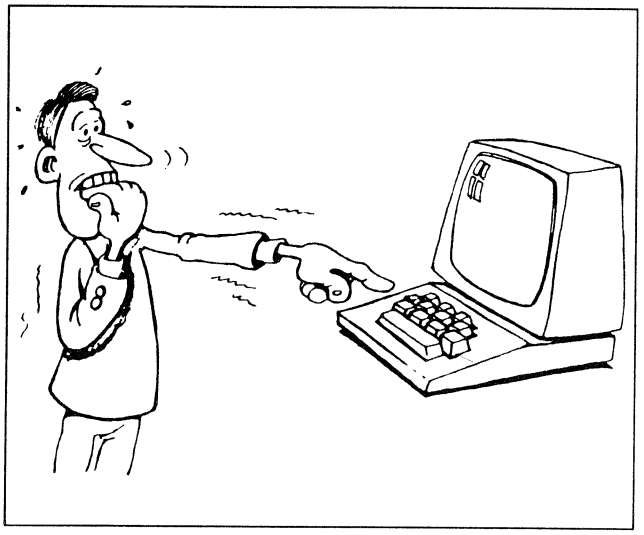
Det er to ganske effektive forholdsregler som kan begrense mulighetene for et virusangrep på personlige datamaskiner:

- Vær svært forsiktig med program en får i kopi fra andre, en vet aldri hvor de kommer fra, eller har vært utsatt for. Hent derfor også gratisprogram fra en pålitelig kilde, som kontrollerer det som skal distribueres.

- Ikke bring med deg program mellom maskiner, bare data. De fleste virus henger seg ikke på datafiler som tekst eller regneark, bare vanlige program (det er så mye enklere).

Jo raskere vi oppdager et virusangrep og informerer om det, jo bedre muligheter har vi for å begrense skadevirkninger og spredning!

Bjørn Gifstad



Diverse

1) Hvis en starter postprogrammet EAN, vil en bli registrert som EAN bruker under den kontoen en har på maskina. På RUNIT's VAX 8600 betyr det at en får en regning for en fast avgift. Samtidig opprettes det en underkatalog med navn EAN på ens bruker.

Hvis en vil slutte som EAN-bruker, må følgende gjøres:

a) Sende melding til adressen POSTMASTER på ens maskin og be om å bli slettet som bruker. EAN-brukere på RUNIT's VAX 8600 sender meldingen til POSTMASTER@VAX.RUNIT.UNIT.UNINETT

b) Selv slette alle filer i underkatalog EAN og etterpå selve katalogen.

2) Hvis en ikke bruker EAN på en stund og pleier å få mye post, f. eks. fra distribusjonslister, vil en risikere at en ikke har nok plass på ens bruker til å ta inn alle meldingene. Når det ikke er plass til mer, får en feilmeldingen "file system error". Ingen av de uleste meldingene kan leses, og en får ikke inn alle. Dette problemet kan omgås på følgende måte:

a) Avslutt EAN når feilmeldingen kommer.

b) Start EAN på nytt uten å lese inn flere meldinger - ved å skrive: EAN -a. Nå kan en lese de uleste meldingene en har tatt inn så langt. Slett så mange meldinger som mulig. Ta heller vare på viktige meldinger på fil (selv om lagerplass brukes til det også) eller helst skriv dem ut.

c) Start EAN på nytt på vanlig måte - nå tas nye meldinger inn.

d) Hvis en på nytt får "file system error", begynner en på pkt. a igjen

Merk at det er lurt å starte EAN med EAN -a hvis en skal sende en melding og en har dårlig tid, og en vet det er mange meldinger som ligger i kø for å bli tatt inn.

3) En "Postscript" laserskriver er tilkoplet VAX 8600 i RUNIT's maskinhall.

En kan også skrive vanlig tekst på den - men merk at den fungerer rett bare for 8 bits ASCII tegnsett (DEC Multinational Character Set). Tekst skrevet med norsk 7 bits tegnsett (f. eks. med VED) vil ikke få skrevet ut æ, ø og å rett.

Denne skriveren kan også brukes for tegning av grafikk - fra programvare som har "Postscript" driver.

Kønavn:
Postscript utskrift: PRINT /QUEUE=LAMH$POST
Vanlig tekst: PRINT /QUEUE=LAMH$ANSI

4) På VAX 8600 er brukerhåndboken for TCP/IP programmene tilgjengelig på terminalen. Det gjelder bl. annet programmene FTP og TELNET - som brukes til henholdsvis filoverføring og terminaloppkopling innen Internettet.

Når det gjelder bruk av Internet nodenavn og navnetjenesten i Internet, er dette beskrevet under kapittel 'navn'.

Under kapittel 'intro' vil en finne en oversikt over alle TCP/IP programmene. Noen er ikke tilgjengelig.

Skriv: MAN FTP
MAN TELNET
MAN NAVN
MAN INTRO

5) Utgave L av SINTRAN er installert på RUNIT's ND570. Det er få eller ingen endringer for en vanlig bruker - hovedtrekkene er listet nedenfor

a) @MODE søker på filtype :MODE først !!

Rekkefølge blir da : :MODE på egen bruker
:MODE på system
:SYMB på egen bruker
:SYMB på system

b) Alltid 'logout-on-missing-carrier' , denne parameteren er også fjernet fra @TERMINAL-MODE.

c) @FILE-SYSTEM-ERROR-MESSAGES
- ny kommando som vil mer detaljerte opplysninger ved feil fra filsystemet
(eks 'no such file name ')
- parameter : yes/no
- denne gjelder bare for den aktuelle kjøring slik at du bør ha
'@F-S-E-M YES' i din LOGIN:MODE fil !

d) Endel endringer i monitorkall.

e) Endel endringer i XMSG og ND-500 monitor.

Knut L. Vik

DATAVIRUS

* Introduksjon

I denne artikkelen skal vi se nærmere på datavirus. Vi vil forsøke å unngå noe av det sensasjonsjaget som ofte kommer frem når datavirus omtales i magasiner og aviser. I stedet vil vi forsøke å se mer saklig og nøkternt på problemet.

Vi vil holde oss til datavirus for personlige datamaskiner, som PC, Macintosh og Amiga. Det vil si at vi ikke vil komme særlig inn på større maskiner, eller andre typer uønskede programmer som ormer o.l.

Vi ser svært gjerne at det kommer kommentarer, korrigeringer og spørsmål til artiklen.

* Avliving av myter

La oss først se på noen fakta om datavirus. Det finnes endel myter og overtro som det til å begynne med kan være nyttig å avlive.

Et datavirus for en bestemt type datamaskiner kan kun angripe andre datamaskiner av samme type. Dvs at et virus som angriper f.eks. PC'er bare kan smitte PC'er og ingen andre typer datamaskiner.

Et datavirus kan ikke infisere disketter som er korrekt skrivebeskyttet, siden det ikke er mulig å endre informasjon på en korrekt skrivebeskyttet diskett. Med 'korrekt skrivebeskyttet diskett' mener vi en diskett der skrivebeskyttelsen er satt rett på. Endel 5.25" disketter kan tilsynelatende være skrivebeskyttet uten å være det. Det kan skyldes at skrivebeskyttelsen er slitt eller gjennomsiktig. (Du kan lett teste dette, bare forsøk å kopiere en fil til en diskett du mener er skrivebeskyttet, klarer du det, er den ikke korrekt skrivebeskyttet).

Datavirus kan ikke oppstå av seg selv. De kan kun oppstå som resultat av målbevisst arbeid av en programmerer.

Et datavirus kan kun smitte ved utførelse av programmer eller programdeler. Dvs at for at en infisert diskett skal kunne smitte maskinen din, må maskinen hente inn programkode fra disketten inn i minnet og starte utførelsen av denne koden.

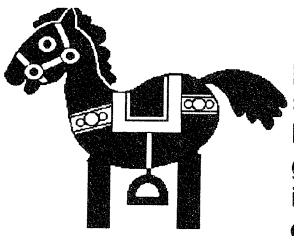
Dessuten er det viktig å være oppmerksom på at selv om vi bruker medisinske uttrykk som 'virus', 'smitte' og 'epidemi', er det kun en symbolsk forbindelse mellom medisinske virus og datavirus. Endel av egenskapene ved datavirus kan minne om de egenskapene en ser ved medisinske virus. Det skulle være unødvendig å si at datavirus ikke kan smitte mennesker ...

* Forklaring av ord og begreper

Det en oftest opplever når en ser datavirus omtalt i aviser og magasiner, er misforståelse av begreper. La oss derfor forsøke å klare opp i en del ord og uttrykk som vi av erfaring vet det hersker endel forvirring om.

Et *VIRUS* er "... et program som kan infisere' andre programmer ved å modifisere dem til å inneholde en mulig endret kopi av seg (altså viruset) selv" (Fred Cohan).

En *ORM* er et program eller sett av programmer som sprer seg via et nettverk ved egen hjelp. En orm vil typisk utnytte sikkerhetshull for å nå nye maskiner ved å kopiere og starte versjoner av seg selv på disse maskinene.



En *TROJANSK HEST* er et program som utfører noe programmereren ville det skulle gjøre, men som brukeren ikke vil det skal gjøre. Normalt ville brukeren ikke ha utført programmet dersom han på forhånd hadde kjent til programmets rette natur. En trojansk hest vil typisk prøve å skjule sin sanne natur og forsøke å gi inntrykk av at den gjør noe nyttig for å få deg til å starte den.

En variant av en trojansk hest er en *TIDSBOMBE.* Mens en trojansk hest vil gjøre ugagn hver eneste gang den utføres, vil en tidsbombe kun gjøre ugagn på et bestemt tidpunkt, f.eks. etter å ha blitt kjørt ett bestemt antall ganger, eller på en bestemt dato.

En mutasjon er en modifikasjon av et eksisterende virus, orm eller trojansk hest, som f.eks. gjør program-

met mer ondsinnet eller mer motstandsdyktig mot antiprogrammer. Mutasjoner er, slik som virus, et resultat av målbevisst programmering - de kan ikke oppstå av seg selv.

En viktig forskjell mellom virus og ormer er at en orm er et selvstendig program som kan spre seg gjennom et nettverk på egen hånd, mens et virus er en programdel som spres som 'blindpassasjer' i andre programmer og som trenger en viss 'hjelp' fra brukere for å spre seg.

Således var altså ikke det såkalte 'internet-viruset', som ble omtalt i TV og aviser i desember -88, et virus, men en orm. Og 'CHRISTMA EXEC-viruset' på BITNET for et år tilbake var nærmest en trojansk hest.

Hvilken nytte har man av å kjenne disse definisjonene? Å sette navn på tingene er første og kanskje viktigste skritt på veien til å forstå hvordan de fungerer og dermed kunne beskytte seg mot dem. Dessuten er det viktig å kjenne terminologien for i det hele tatt å forstå hva andre mener når de snakker om disse tingene.

* Hvordan et datavirus smitter

Det finnes bare en måte et virus kan smitte en datamaskin på, og det er ved at datamaskinen utfører et program som allerede er virusinfisert. Det er hovedsaklig to teknikker som virus benytter seg av for å infisere en datamaskin.

Infisering av oppstartkode. Datamaskiner som PC, Mac og Amiga trenger en diskett eller harddisk for å kunne starte. Disse virusene infiserer programmet som utgjør oppstartkoden på disketten eller harddisken. Når du starter med en infisert diskett eller harddisk, vil maskinen bli infisert. Maskinen vil så kunne infisere oppstartkoden på alle disketter den får skrivetilgang til.

Disse virusene vil bare bli aktivert om du starter opp fra en infisert diskett eller harddisk. De er dessuten lette å finne for en virusindikator.

Infisering av vanlige programmer. Disse virusene er mer avanserte og det er færre typer av dem. De infiserer programmer, og når et infisert program blir kjørt vil maskinen din bli infisert. Er maskinen din infisert av et slikt virus, vil alle programmer maskinen får skrivetilgang til kunne bli infisert ved at viruset legger en kopi av seg selv inn i programmene som skal infiseres.

Du vil kunne oppdage en slik infisering ved at programmene endrer lengde, dato for siste modifisering, eller sjekksum.

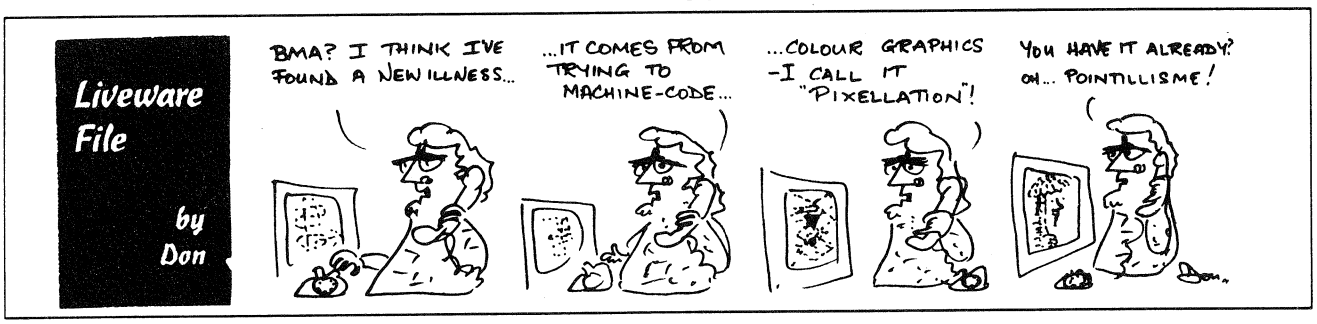
* Hvordan datavirus IKKE smitter

Like viktig som å vite hvordan datavirus sprer seg, er det å vite hvilke metoder et virus ikke kan bruke for å infisere nye maskiner. Man opplever stadig at brukere i mangel av konkret viten tar gale forhåndsregler, som ikke har noen praktisk virkning for å stoppe virus.Det eneste man oppnår ved det er en falsk trygghetsfølelse.

Datavirus kan ikke laste seg selv ned over modemlinjer. Programmer du overfører over modem kan være infisert, men du vil ikke kunne få andre programmer enn de du spesielt ber om å få. For en tid tilbake gikk det rykter om et virus som kunne laste seg selv ned i bakgrunnen over en modemlinje. Dette er etterpå blitt avslørt som en 'spøk'. Ikke desto mindre har ryktene blitt til en seiglivet vandrehistorie.

Infiserte disketter kan ikke smitte datamaskiner uten at de settes inn og leses i en diskettstasjon.

En diskett kan kun bli infisert ved at det blir skrevet data til den i en diskettstasjon. En diskett kan følgelig ikke bli infisert ved oppbevaring, selv om den oppbevares sammen med disketter som er infiserte.



DATAVIRUS forts.

En diskett som er korrekt skrivebeskyttet kan ikke bli infisert.

En datamaskin kan ikke bli infisert mens den er slått av (med strømbryteren), siden infisering krever at det blir utført et program.

Et datavirus som er beregnet for en type datamaskin, kan ikke angripe en datamaskin av en annen type. Dvs. at et virus beregnet for en PC ikke kan angripe en Amiga. Dette kommer av de store forskjellene i datamaskinenes indre oppbygging og forskjellene i operativsystem.

Teoretisk sett kan et virus være beregnet på flere forskjellige maskintyper, men dette vil drastisk øke størrelsen på viruset og gjøre det lettere å oppdage. Internet-ormen var beregnet for flere varianter av UNIX, men det er viktig å huske på at dette var en orm, ikke et virus. Dessuten brukte Internet-ormen konsepter som ikke ville virke på maskiner som PC, Mac og Amiga.

Jeg kjenner ikke til noe virus som har vært beregnet for å angripe mer enn en type datamaskiner.

* Eksempel på forløp av et virusangrep

Du har fått et program fra en venn eller bekjent som ikke selv er klar over at hans system er infisert. Du setter disketten i din egen maskin og kjører programmet.

Vi vil her dele opp infiseringen i tre forskjellige faser.

Første fase: Mens programmet tilsynelatende utfører en mer eller mindre nyttig oppgave, infiserer det systemet ditt. Dvs. at virus-delen av programmet tilordner seg en del av minnet på maskinen og legger seg der (legger seg resident).

Nå er maskinen din infisert, i tillegg til det programmet/disketten som infiserte den.

Andre fase: Viruset begynner nå å forsøke å spre seg. Det kan bruke forskjellige metoder, men typisk vil det legge kopier av seg selv inn i programmer som befinner seg på disketter og harddisker som det får skrivetilgang til.

Endel virus er såkalt 'harmløse' og vil ikke forsøke å gjøre mer ugagn enn å spre seg mest mulig, i så fall vil de fortsette i denne fasen inntil du oppdager og fjerner programmet. Du bør alltid fjerne et virus hvis du oppdager et, selv om det er klassifisert som såkalt 'harmløst'.

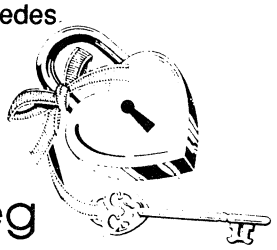
Tredje fase: Nå forsøker viruset å gjøre skade. I mange tilfeller kan dette være barnslige og relativt ufarlige påfunn, slikt som å forstyrre utskrift til printer, vise meldinger på skjermen eller manipulere teksten på skjermen på ulike måter.

Dersom du er blitt angrepet av et 'ondsinnet' virus, vil den stort sett unngå slike barnslige påfunn, og i stedet forsøke å gjøre mest mulig skade fortest mulig. I praksis vil dette si at man overskriver vitale deler av disketter eller harddisker. Spesielt ille vil dette være om backup-programmet angripes på en slik måte at sikkerhetskopiene er uleselige!

Tidsrommet fra infisering og til viruset eventuelt starter å slette data på systemet ditt vil typisk kunne variere fra timer til uker. Viruset vil kunne være innstilt på å gå av en bestemt dato, et bestemt tidsrom etter infisering, eller etter at et bestemt antall nye programmer er blitt infisert.

Dette er selvfølgelig kun et grovt omriss av hvordan noen virus oppfører seg. Det finnes naturligvis virus som oppfører seg helt annerledes.

* Hva kan du gjøre for å beskytte deg



Det er flere ting brukeren selv kan gjøre for å beskytte seg mot angrep av datavirus.

Ta regelmessig backup av alle viktige filer. Det vil redusere skaden dersom du skulle bli angrepet. Dessuten vil en backup være nyttig i andre tilfeller når du har fått ødelagt data av andre årsaker enn virus.

Ha skrivebeskyttede originaldisketter med alle viktige programmer liggende på et trygt sted. Unngå å bruke originaldiskettene til daglig bruk, benytt dem kun ved

installering av systemet. I tilfelle et virusangrep kan du da raskt installere de forskjellige programmene på ny fra originaldiskettene, (dessverre er det endel firma som bruker kopieringsbeskyttelse på en slik måte at dette er vanskelig eller umulig).

Vær forsiktig med ukjente programmer. Før du bruker et nytt og ukjent program kan det ofte være nyttig å teste programmet med spesialprogrammer for å oppdage virus og trojanske hester.

Disketter som du ikke trenger å ha skrivetilgang på bør skrivebeskyttes. En god (men tidkrevende) regel er at alle disketter skal være skrivebeskyttet, og så kan du fjerne beskyttelsen for de diskettene du trenger skrivetilgang til når behovet oppstår.

Vær på utkikk etter unormale ting. Et av symtomene på at maskinen din er infisert av virus vil være unormale og 'rare' hendelser. Som regel vil slikt ikke være forårsaket av virus, men har naturlige årsaker.

Forsøk å skaffe programmer mest mulig direkte fra programmets kilde. Filosofien er: Jo færre ledd et program har gått gjennom før det når deg, desto mindre er sjansen for at det er virusinfisert.

Om mulig, forsøk å få tak i kildekode til programmer. Virus vil kunne infisere utførbare filer, men infisering av kildekode vil være svært vanskelig. Med kildekode vil du dessuten langt enklere kunne avgjøre om programmet f.eks. inneholder en trojansk hest.

Den typiske trojanske hest er et program med et iøynefallende navn, som distribueres uten kildekode eller annen dokumentasjon.

Kjør jevnlig kontroll av sjekksummer på filene dine. Det vil si deg hvilke av filene som har fått endret innholdet sitt.

Få tak i og bruk virusindikator. Dette er programmer som lastes inn i maskinens minne ved oppstart, og som vil kontrollere om et infisert program forsøker å infisere systemet. I så fall vil virusindikatoren stoppe viruset, og gi deg beskjed om hvilket program eller diskett som er infisert.

Det finnes en mengde slike virusindikatorer, vi kommer senere tilbake til en liste over de mest brukte.

I visse tilfelle kan det være nok å ha et system som avviker fra standardsystemet. De fleste virus er svært små programmer, som gjør en del antagelser om hvordan systemet ditt er satt opp. Dersom ditt system avviker, kan endel av de forutsetningene som viruset tar for gitt ikke være til stede, og viruset klarer ikke å infisere systemet.

F.eks vil endel PC virus kunne stoppes ved å legge COMMAND.COM et annet sted enn på roten av filsystemet. Virusene vil forsøke å infisere COMMAND.COM på rot, og vil derfor mislykkes.

* Liste over endel virus på forskjellige datamaskiner

Her er en liste over endel av de mest utbredte virusene for PC, Amiga, Macintosh og et par andre maskiner. Selv om lista ikke er komplett, dekker den de fleste 'levedyktige' virus. Vær dessuten oppmerksom på at et og samme virus kan være kjent under mange forskjellige navn.

IBM PC og kompatible (under MS-DOS og PC-DOS)

Lehigh-viruset (2 varianter)
Wien-viruset
Det italienske viruset (ping-pong-viruset)
Det israelske viruset (Jerusalem-viruset)
Det pakistanske viruset (brain-viruset)
Blackjack-viruset (1704-viruset)
Yale-viruset

Apple Macintosh:

NVir (type A, B og Hpat)
INIT 29 viruset
Peace viruset (MacMag-viruset)
Scores-viruset
ANTI-viruset
Tsunami-viruset

Amiga:

SCA-viruset (+ en mengde kloner)
IRQ-viruset
Byte Bandit viruset
Revenge viruset
Byte Warrior viruset
Obelisk viruset
Lamer viruset
Disk Doctor viruset

DATAVIRUS forts.

Det virker som om Amiga og Mac virusene har lettere for å spre seg enn virusene for PC. Dette kan skyldes at Amiga og Mac har et mer avansert operativsystem enn PC, og at det er lettere å få infisert maskiner og disketter uten at brukeren oppdager det. Det enklere operativsystemet på PC gir virusene færre muligheter for infisering, samtidig som det er lettere for brukeren å holde oversikten over systemet på et lavt nivå.

* Oversikt over endel antivirusprogrammer

Vi kan grovt sett dele antivirusprogrammer inn i fem hovedgrupper, etter hva slags effekt de har, og hvilke metoder de bruker for å beskytte datamaskinen.

- *VIRUSINDIKATORER* er programmer som sier ifra dersom det finner et virus resident i minnet, eller det finner infiserte disketter eller programmer.

- *VIRUSUTRYDDERE* er programmer som fjerner viruset fra infiserte programmer eller disketter. Typisk vil du ta i bruk en virusutrydder etter at en virusindikator har varslet om at maskinen din er i ferd med å bli infisert.

- *FILSJEKKERE* er programmer som kontrollerer integriteten til enkelte eller alle filene på diskettene og harddisken. Filosofien bak denne typen programmer er at et virus må endre innholdet i programmer når disse blir infisert, og derfor kan en eventuell infisering oppdages ved å sjekke om innholdet av programmene er blitt endret.

- *DISKOVERVÅKERE* er programmer som kontrollerer all kommunikasjon mellom programmer og diskene. Visse programmer eller visse typer diskoperasjoner (f.eks. formatering) kan på forhånd være merket som ikke bra, og diskovervåkeren kan filtrere ut disse operasjonene.

- *PROGRAMANALYSATORER* er programmer som forsøker å analysere innholdet i et program, for å avgjøre om programmet kan være farlig. Det er så godt som umulig å gjøre dette arbeidet skikkelig, slik at denne typen programmer bare gir en svært begrenset beskyttelse. Dessuten har programanalysatorene lett for å gi falsk alarm.

Især programanalysatorer og diskovervåkere vil gi beskyttelse ikke bare mot datavirus, men også mot trojanske hester.

Her er en kort oversikt over noen av de programmene som er tilgjengelig for å bekjempe virus.

Programmer for PC

Alert v.1.3	- Filsjekker
Bombsquad v.1.2	- Diskovervåker
Chk4bomb v.1.00	- Programanalysator
FluShot v.1.51	- Filsjekker og virusindikator
VacBrain v.1.10	- Virusindikator og virusutrydder (Brain)
Checkup v.2.1	- Filsjekker

Programmer for Macintosh

Virus RX v.1.4	- Virusindikator og filsjekker
Ferret v.1.1	- Virusindikator og virusutrydder (Scores)
KillScores	- Virusindikator og virusutrydder (Scores)
VirusCheck	- Filsjekker
Interferon v.3.0	- Virusindikator, virusutrydder og filsjekker
Vaccine v.1.01	- Diskovervåker
VirusDetective v.2.0	- Virusindikator
Desinfectant v1.1	- Virusindikator/utrydder

Programmer for Amiga

VirusX v.3.2	- Virusindikator og virusutrydder

* To viktige spørsmål om virus/antivirus

Et interessant spørsmål angående virus er: 'Er det mulig å holde datamaskinen 100% unna alle virus?'. Svaret er 'Nei'. Det er ikke mulig å operere med et absolutt, 100% sikkert fravær av virus.

Selv om man holder en maskin helt adskilt fra andre datamaskiner, vil den ikke være 100% beskyttet. Så lenge man er avhengig av å hente operativsystem og program utenfra, er den ikke skikkelig isolert. Det har vært tilfeller der kommersielle programmer som er solgt over disk i dataforretninger har vært infisert med virus.

Et annet interessant spørsmål er 'Er det mulig å lage et antivirus som oppsporer absolutt alle virus?' Vi ser av og til firma og programmerere påstå dette, men svaret på spørsmålet er 'Nei'. To av grunnsetningene for virus/antivirus er:

Et antivirus kan finne og ødelegge ethvert kjent virus.

Et virus kan unngå ethvert kjent antivirus.

I praksis vil dette si at det går an å lage et antivirus som beskytter mot alle KJENTE virus, men det finnes ingen garanti for at det beskytter mot alle fremtidige virus. På samme måte kan et virus i teorien omgå alle kjente antivirus programmer.

På 'små' datamaskiner som PC, Mac og Amiga har et program som er startet full kontroll over alle datamaskinens ressurser, og såfremt det vet hvordan, kan det avvæpne alle antivirus-programmer.

* Hvordan oppdager du at maskinen din er smittet

Det er hovedsaklig tre måter du kan oppdage at datamaskinen din er smittet av et virus:

En virusindikator sier ifra. I så fall vil du allerede ha klassifisert viruset, og kan uskadeliggjøre det med en virusutrydder for dette viruset. Ofte vil en virusindikator være kombinert med en virusutrydder, og da vil viruset bli drept med det samme det oppdages.

Du oppdager unormale ting på maskinen. I dette tilfellet har du en litt større jobb. For det første er det slett ikke sikkert at unormale ting ved datamaskinen din skyldes virus. Faktisk er det ytterst sjelden at unormal oppførsel ved en datamaskin skyldes virus.

Indikasjoner på at det er et virus er slike ting som at filer endrer klokkeslett og dato for forrige skriving, systemet går tregere, eller at lengden på enkelte filer endrer seg. For å klassifisere et eventuelt virus bør du lese gjennom rapporter og beskrivelser av virus som angriper din type datamaskin.

Viruset sier selv ifra om at du er infisert. I dette tilfellet kan du være nokså ille ute. Dersom det er et virkelig ondsinnet virus, kan f.eks. harddisken din allerede være formatert før du får sjanse til å reagere. Imidlertid er klassifiseringen av viruset enklere, og du burde ikke ha noe problem med å finne mer info om viruset, bl.a om hvordan du utrydder det.

Hvis du oppdager at datamaskinen din er smittet av datavirus, har du her noen råd for hvordan du bør reagere.

IKKE FÅ PANIKK. Det er det absolutt verste du kan gjøre i en slik situasjon, og det vil nesten helt sikkert føre til at du mister enda mer data.

Forsøk å klassifisere viruset. Let gjennom forskjellige informasjonskilder der forskjellige virus for din type datamaskin er beskrevet og prøv å finne ut hvilket virus du har.

Så snart du har klassifisert viruset bør du forsøke å samle mest mulig informasjon om det, slik at du vet hvordan det fungerer, hva det kan ha infisert, og hva som kreves for å fjerne det. Prøv også å skaffe deg et antivirus og en virusindikator som man vet fungerer mot dette viruset.

Så snart du vet at maskinen virkelig er infisert og at det ikke er en falsk alarm, må du gi beskjed til andre brukere av samme type datamaskin som du selv bruker, slik at også de kan ta sine forholdsregler. Det gjelder især de som du tror du kan ha blitt smittet av, eller som kan ha blitt smittet av deg.

Start systemet fra en skrivebeskyttet uinfisert diskett. Du må bruke kaldstart, dvs skru strømmen av og på igjen, ettersom noen virus kan overleve varmstart. Bruk den skrivebeskyttede originaldisketten for

DATAVIRUS forts.

operativsystemet som fulgte med maskinen da du kjøpte den.

Desinfiser alle disketter og programmer. Fremgangsmåten vil variere med virustype og maskintype, men dersom du vet hva slags virus det er snakk om, vil du kunne finne tilstrekkelig informasjon om dette i de kildene som er nevnt på slutten av denne artikkelen.

I størst mulig grad bør du forsøke å installere programmer fra skrivebeskyttede 'rene' disketter. Det gir størst grad av sikkerhet for at viruset ikke har ødelagt deler av programmet, og det vil gi deg størst visshet for at du har fått bort alle virusinfiserte programmer.

Til slutt bør du sørge for at en virusindikator for dette viruset alltid blir kjørt på maskinen din. Det vil hjelpe deg til å unngå nye virus av samme type.

Til slutt en gylden regel når du skal forsøke å desinfisere et system for et virus og du ikke er helt sikker på hva du skal gjøre: Forsøk å få tak i noen som kjenner mer til dette enn deg, f.eks hos RUNIT.

* Hvor reell er faren for å bli smittet ?

Datavirus er blitt funnet på datamaskiner i Norge - også på datamaskiner i Trondheim, så det er et problem du bør ta alvorlig.Det er funnet virus på Amiga og Mac her i universitetsmiljøet i Trondheim, men ikke på PC såvidt vi kjenner til.

Faren for at din datamaskin skal bli smittet er derfor tilstede. Faren øker jo større kontakt din datamaskin har med andre datamaskiner. Du kan redusere faren ved å isolere datamaskinen fra omverdenen. Men det vil i praksis bety tidkrevende og kompliserte rutiner som sterkt kan redusere nytteverdien av datamaskinen.

Dersom du satser på 100 % isolering, har du et stort problem straks du ønsker å bruke en skriver som er tilkoblet en annen maskin. Du vil heller ikke kunne få fordelene av å benytte et LAN (Local Area Network). Du vil også miste mange av fordelene ved kompatibilitet og standardisering av datamaskiner.

Et alternativ til fysisk isolering av datamaskinen er å kombinere bruken av antivirus-programmer, sjekksum-programmer, backup, og det aller viktigste våpen du har i kampen mot virus: informasjon. Ved å holde deg informert om de ulike virusene og deres måte å fungere på, samt å kjenne datamaskinens muligheter og begrensninger, står du svært sterkt rustet mot datavirus.

* Hvor kan du finne mer info om datavirus ?

Det finnes mange kilder for informasjon om datavirus, her er et utvalg som gir konsentert og saklig informasjon om virus.

Magasiner

Magasinet 'Computers & Security' som de siste 2-3 årene har hatt en stor prosentdel av stoff om datavirus. Seksjonsbiblioteket på elektro har alle de siste årgangene.

Elektronisk post (distribusjonslister)

Dersom du ønsker å melde deg på en av listene på EARN/BITNET (f.eks. VALERT-L@LEHIIBM1) gir du kommandoen:

TELL LISTSERV at LEHIIBM1 SUB VALERT-L Ditt Personlige Navn

Du kan også melde deg på en EARN/BITNET liste fra en adresse utenfor EARN/BITNET - f. eks. fra EAN. For påmelding til VALERT-L, send eletronisk post til: LISTSERV@LEHIIBM1.BITNET,
der brevet inneholder kun en linje:
SUB VALERT-L Ditt Personlige Navn

For å melde deg på Internet-listene sender du en forespørsel om å bli medlem til listeadressen, men i stedet for bare listenavnet bruker du <liste>-REQUEST, f.eks (for SECURITY):

SECURITY-REQUEST@PYRITE.RUTGERS.EDU

Lister

- VIRUS-L@LEHIIBM1 på EARN/BITNET som er en liste for diskusjon av datavirus. Her vil man finne mye relevant informasjon, flere sider hver dag. Dette er den beste måten å holde seg orientert om datavirus.

- VALERT-L@LEHIIBM1 på EARN/BITNET er en søster-liste til VIRUS-L, men inneholder kun korte og viktige advarsler om nye virus.

- SECURITY@PYRITE.RUTGERS.EDU er en liste for generell diskusjon av sikkerhet. Særlig sikkerhet rundt datamaskiner, men også sikkerhet generelt (låser, vakthunder, alarmer etc). Denne lista kan også nås via LISTSERV på EARN/BITNET som SECURITY@FINHUTC

- RISKS@KL.SRI.COM er en liste for diskusjon av risikoen ved bruk av data maskiner. Lista kommer endel innom datavirus. På EARN/BITNET kan denne lista nås som RISKS@FINHUTC

Listene VIRUS-L og RISKS er tilgjengelig på RUNIT's EARN maskin vha. INFO programmet. Programmet startes ved å skrive INFO -fra menysystemet skriver en CMS INFO. For EARN-brukere er det derfor ikke nødvendig å abonnere på disse listene.

Informasjon som kan hentes via anonymous ftp på Internet

- Du kan også hente forskjellige antivirusprogrammer fra forskjellige databaser rundt om i verden via anonymous ftp. Katalogen

  PD:<MSDOS.TROJAN-PRO>
  på serveren SIMTEL20 har endel antiprogrammer for PC'er. Disse kan hentes fra adressen WSMR-SIMTEL20.ARMY.MIL.

- Du kan hente gamle nummer av VIRUS-L lista via anonymous ftp fra filtjenerne IBM1.CC.LEHIGH.EDU og LLL-WINKEN.LLNL.GOV. Disse filtjenerne vil dessuten ha endel antivirusprogrammer som også kan hentes ned.

Informasjon som kan hentes fra LISTSERV på BITNET

- Du kan hente gamle nummer av VIRUS-L fra LISTSERV at LEHIIBM1. Denne serveren vil dessuten også ha endel antivirusprogrammer. Det er katalogisert under fil-lista VIRUS-L FILELIST Gamle innlegg fra VIRUS-L blir dessuten lagret andre steder i LISTSERV-systemet, se videre info fra LISTSERV selv.

- BITNET serveren SCFVM har en pakke med antivirusprogrammer for Mac, som kan hentes fra fil-lista VIRUSREM FILELIST

RUNIT-D har på sin VAX 8600 liggende dokumentasjon om virus og antivirusprogrammer for PC, Amiga og Mac. Du finner disse under katalogen

DISK3:<PC.VIRUS>.

Her vil du blant annet finne beskrivelser av endel virus, f.eks symtomer, evt. skader de gjør, og hvordan du blir kvitt dem. De viktigste programmene nevnt over kan hentes herfra.

Anders Christensen, RUNIT's orakeltjeneste

"The book I'm writing is titled *Transistors, Volume 1.*"

RUNIT-D Teknisk Gruppe
KUNDESERVICE

RUNIT-D Teknisk Gruppe har helt siden etableringen i slutten av 70-åra, utviklet seg til å bli et kompetansesenter for SINTEF/NTH-miljøet innenfor fagfeltene maskinvare og datakommunikasjon.

RUNIT-D har gjennom en stor og variert maskinpark vært avhengig av selv å sitte på nødvendig maskinvare- og programvarekompetanse. Dette er en kompetanse som har vært vanskelig - om ikke umulig - å skaffe fra eksternt hold.

Det hører med til historien at NORSK DATA's avdelingskontor for Trondheim ble startet med utgangspunkt i RUNIT-D's Teknisk Gruppe. Samarbeidet med ND's avdelingskontor har derfor fungert meget godt, slik at Teknisk Gruppe har kunnet tilby vedlikehold på ND-utstyr på lik linje med NORSK DATA selv, til en pris langt lavere enn markedspris.

RUNIT-D har også fungert som en avansert referanseinstallasjon i forholdet til ny maskinvare og nye versjoner av programvare. Dette har ikke alltid vært like heldig for sluttbrukerne, men likevel en stor utviklingsfordel for miljøet totalt.

Totalt sett har Teknisk Gruppe bygget opp en kompetanse som spenner over hele utstyrsspekteret fra brukeren i den ene ende til maskinressursen i den andre. Dette gir en klar gevinst i forholdet til problemsituasjoner som oppstår "et eller annet sted" mellom brukeren og maskinressursen.

Samtidig har den store variasjon av utstyrstyper som "skal snakke sammen", gitt oss en unik basis innen grunnleggende datakommunikasjon.

Grunnlaget for hele vår virksomhet har basis i at vi selv utfører teknisk vedlikehold på de utstyrstyper RUNIT-D disponerer. Dette gjelder ikke bare maskinvare/periferiutstyr, men også avanserte nettkomponenter innenfor datakommunikasjon. Teknisk Gruppe får gjennom sitt tekniske vedlikehold tilgang til informasjoner/spesialkompetanse som den enkelte leverandør kanskje er alene om ellers.

RUNIT-D sitter også med egen systemdriftskompetanse, og samspillet mellom denne og Teknisk Gruppe har vist seg svært nyttig i feilsituasjoner der selv leverandøren får problemer.

Mange eksterne leverandører har klart signalisert at de ser store fordeler med en organisasjon som Teknisk Gruppe som kan fungere som en forlenget arm i feilsituasjoner der kravet til bl.a. responstid er høyt. RUNIT-D Teknisk Gruppe har derfor prioritert å opprette gode samarbeidsavtaler med de aktuelle leverandørene. Dette kommer i neste rekke hele SINTEF- og NTH-miljøet tilgode.

Etter ønske fra NTH har RUNIT-D etablert seg som autorisert forhandler for IBM PS/2 og MACINTOSH. Dette har medført at Teknisk gruppe også har etablert vedlikeholdsressurser for disse produktene.

Datakommunikasjon er et satsningsområde i tiden, og er også blitt et hovedområde for Teknisk Gruppe. RUNIT-D har ansvaret for store deler av stamnett og forbindelser mot utenomverdenen fra NTH-miljøet, samt et meget stort og sammensatt eget nett. Vår nettkompetanse gjør at vi også benyttes ved utarbeidelse av nettløsninger lokalt i miljøet.

Store maskin- og nettinstallasjoner stiller sterke krav til kraft, ventilasjon og overvåkning. RUNIT-D Teknisk Gruppe har også bygget opp høy kompetanse innenfor disse spesialfeltene.

I forrige nummer av RUN-NYTT presenterte vi et ekstrakt av de tjenester Teknisk Gruppe kan tilby innenfor SINTEF/NTH, og det er en klar forutsetning for vår videre utvikling at vi benyttes av miljøet rundt oss.

Henvendelse : RUNIT-D's ekspedisjon,SBII 2.etg.
Tlf. (59)3028/2978

RUNIT-D´s KUNDESERVICE

Runit yter blant annet brukerstøtte på følgende områder :

(Tjenesten er enten A, B, eller C, og det vises nedenfor hvilke tjenestetyper som tilbys for de ulike grupper).

MIKROMASKINER/ ARBEIDSSTASJONER

. IBM PS/2 og Apple (C)
  . Utpakking og konfigurering
  . Innlegging av system-programvare og tilleggsprogram

. PS/2, PC, PC/AT, APPLE (A)

. SUN, APOLLO (A)
  (avtaler under forhandling)

MINIMASKINER

. Norsk Data (ND) (A, B, C)

TERMINALER - SKRIVERE

. ND, DEC, Tandberg, FACIT, IBM, Apple m. fl. (A, C)
  . Timebasert vedlikehold og feilretting

DATANETT

. 3-COM/BRIDGE-produkter (A, B, C)
  . broer, TCP/IP-servere, multiportrepeatere

. Vitalink (B, C)
  . broer for 64 kbit/s og 2 Mbit/s leide linjer

. NOVELL (maskiner/nett) (A, B, C)
  . Konfigurering og uttesting

KONSULENT-TJENESTER

. Mikromaskiner/arbeidsstasjoner, minimaskiner, terminaler, skrivere og datanett

A. Servicekontrakt, fastpris pr. år

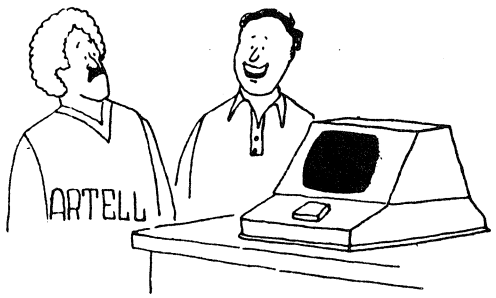
B. Servicekontrakt/systemdrift, fastpris pr. år

C. Timebaserte tjenester etter avtale

Forannevnte tjenester er en del av RUNITs KUNDESERVICE.

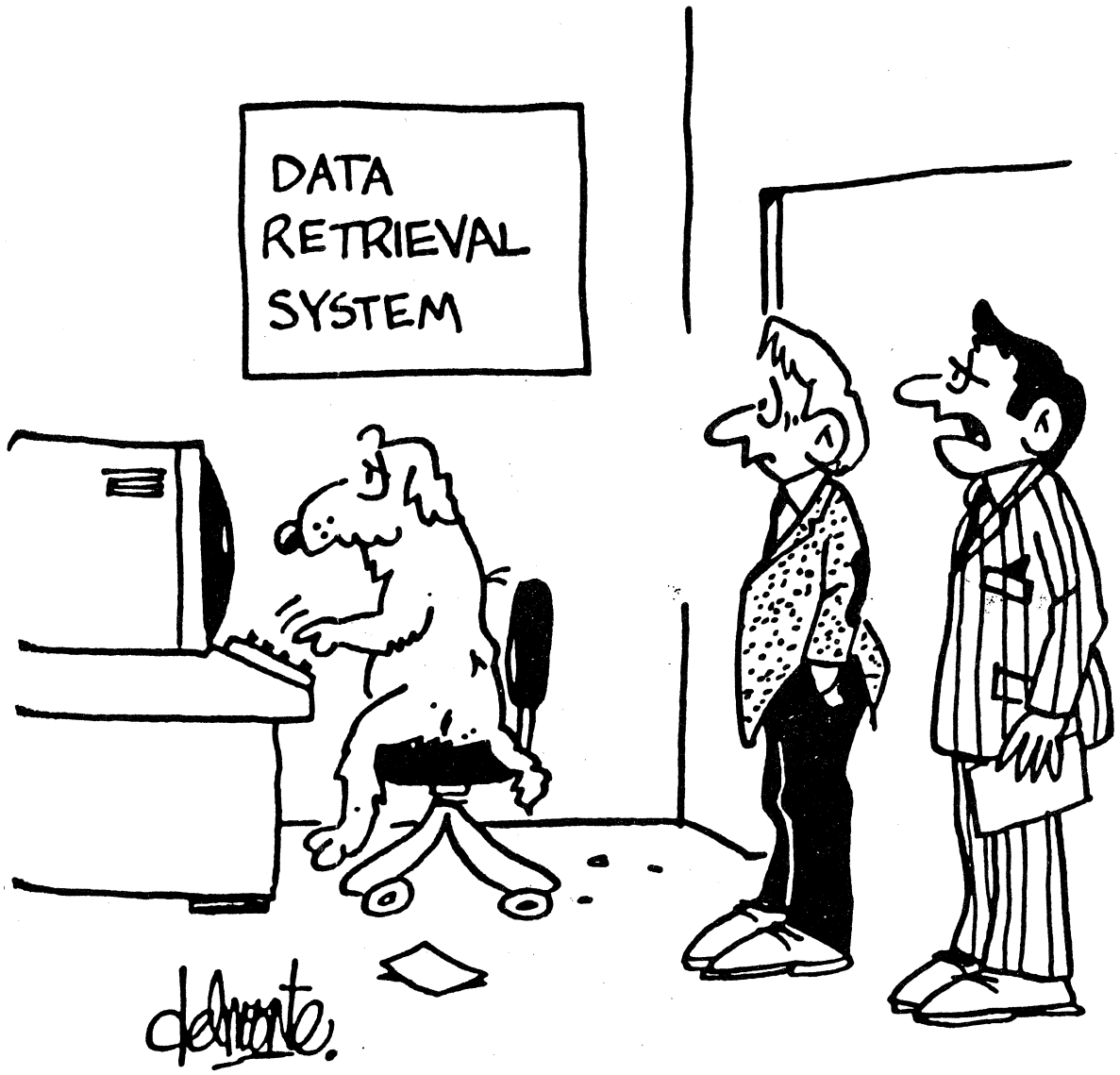
Henvendelse:

RUNITs ekspedisjon
SBII, 2.etg.
Tlf. (59) 3028/2978



" I got a Real Deal on the Keyboard "

Returadresse:
RUNIT-D
7034 Trondheim



" I know he´s a retriever, but this is ridiculous ".