Sikkerhedsprocedurer og katastrofeplan

Udarbejdet af DBC's Edb-afdeling94.05.01

Indholdsfortegnelse

Sikkerhedsprocedurer og katastrofeplan

Projektnr.: 1994:8

Formål At beskrive de sikkerhedsmæssige forhold der skal kunne sikre den samlede driftstabilitet for edb-systemer afviklet i DBC.

En del af aktiviterne er taget op i forbindelse med ISO9000-projektet og indgår i procedure 8.3 samt tilhørende instruktioner. Dette gælder ikke mindst backup.

Sammenfatning

1. Datasikkerhed
omfatter funktioner, og opgaver, forebyggende eller genoprettende, som tjener til at forhindre tab af data (sikkerhedskopiering og reetablering af data).

Der er fastlagt instruktioner for back-up-procedurerherunder anvendelse af puljer, og opbevaring af data.

Der er etableret viruskontrol og tilhørende vejledning.

Det indstilles, at der
- for alle systemer forefindes en backup-versionuden for huset

2. Systemernes adgangs- og sikkerhedsforhold
omfatter funktioner og opgaver, som skal tjener til at forhindre uautoriseret brug af netværk og maskiner (fysisk sikkerhed, kontrol med adgang på net, viruskontrol)

Til dette område knytter sig en aktivitet:
4. Opfølgning på etableret netadgangskontrol

Den fysiske sikkerhed betragtes som tilstrækkelig. I forbindelse med projektet er det blevet indskærpet overfor regngøringspersonalet, at vinduer og døre skal forblive lukkede til edb-afdelingen.

Adgangskontrollen til DBC's maskiner foretages dels af UNI-C, dels af DBC.
Der er etableret en "sikkerhedsmaskine" som varetager netadgangskontrollen.
Der er fastlagt regler for anvendelse af pasord.
Modemforbindelser er forsynet med tilbagekaldsmodem.

Der indstilles, at der

- indledes en drøftelse med vores konsulent (UNI-C), om det definitive sikkerhedsniveau, vi ønsker at etablere. Den konkrete beslutning vil medføre yderligere instrukser / rutiner og evt. anskaffelse af teknisk udstyr og programmel.
- planlægges udskiftning af køleanlæg og brandsikring inden udgangen af 1996
- foretages en fordeling af funktionerne på den nuværende bromaskine på to maskiner.
- ændres på den automatiske lukning af døre til edb-afdelingentil kl.16

3. Tilgængelighed

omfatter funktioner og opgaver, som skal sikre stabil drift (overvågning af maskiner og netværk, planer for genetablering)

Til dette område knytter sig to aktiviteter:

1. Vurdering af overvågning på RC9000 (drift)
3. Undersøgelse af overvågningsprogrammel til UNIX-maskiner

Der er anskaffet maskinel og programmel, som gør det delvist muligt at foretage overvågning af maskiner og netfunktioner, ligesom der er foretaget programmering til de enkelte systemer.

Der er blevet etableret dublering af RC9000, som sikrer maskinal oppetid på inddateringssystemet og Artikelbasen (online).
Netværksovervågningen er blevet sat i værk med det indkøbte software.
Der er etableret overvågning af opkoblingerne til Artikelbasen.
Der er programmeret scripts, således at der automatisk rapporteres på skærm hos de driftsansvarlige om f.eks. resultatet af natjobs.
Reetablering vil kunne ske fra originalsoftware og/eller back-up.

Det indstilles, at

- NCC-maskinen, som sørger for, at PC'ernes netkort bootes, dubleres.
- udbygningen af overvågning af elementerne i RC-kat-miljøet fortsættes.
- overvejelserne om anskaffelse af standard overvågningssystem henlægges indtil videre

4. Katastrofeplan

Til dette område knytter sig en aktivitet:

2. Vurdering af reetablering af maskiner

Sikkerheden vurderes som ganske stor i forbindelse med nedbrud /beskadigelse af enkelte maskiner, fordi der er gennemført en dublering af de fleste af maskinerne.

Der mangler

- tilbagemelding fra maskinleverandørerne på, hvor hurtigt man ville kunne reetablere maskiner eller medvirke til nøddrift. Denne forventes primo maj.

Indledning

Hvad er edb-sikkerhed?

God edb-sikkerhed varetager tre behov:

- *Tilgængelighed*. Man skal til stdighed kunne benytte og have adgang til alle edb-registerede informationer
- *Pålidelighed*. Sikkerhedssystemet sakl sikre, at edb-systemet fungerer uden fejl, og at data hele tiden er korrekte
- *Fortrolighed*. Adangen til informationerne i edb-systemerne skal kunne differentieres, så fortrolige oplysninger ikke kommer i uvedkommendes hænder.

Hvor kommer truslerne fra?

I praksis kommer de hyppigste anslag mod edb-sikkerheden fra "uskyldige" foreteelser som tekniske svigt og utilsigtede menneskelige fejl. Det kan være strømsvigt, programmerings- og driftsfejl, banale fejltastninger eller brand.

På den anden side er der også de forsætlige menneskelige handlinger: hackere, virus, databedrageri.

I DBC har vi prøvet at dække os ind, så vi kan imødegå de umiddelbare trusler.

Sikkerhedsaspektet er et væsentligt element i en udadvendt virksomhed. Selv om 100% sikkerhed ikke findes, er der stadig områder, der kan tages op og justeres. Kvalitetsstyringssystemet vil medvirke til en løbende revision af området.

Denne beskrivelse fortæller, hvorledes vi i begyndelsen af 1994 har grebet tingene an.

1. Datasikkerhed

omfatter funktioner, og opgaver, forebyggende eller genoprettende, som tjener til at forhindre tab af data (sikkerhedskopiering og reetablering af data).

Data er værdier for virksomheden og skal behandles som sådan. Firmaets revisorer har faktisk pligt til at sikre sig, at firmaer behandler data som værdier. Derfor er sikring af data ikke et personligt ansvar, men et ledelsesansvar. Ledelsen skal derfor opstille retningslinier for sikring af data og kommunikere dem ud i virksomheden.
Men at ansvaret formelt ligger hos ledelsen betyder kun, at ansvaret forplanter sig ud i alle led, således at det følger det organisatoriske ansvar i øvrigt.

Der er etableret faste back-up-rutiner af data, således at alle systemer vil kunne genskabes med minimalt tab af data (dagens arbejde).
Back-up tages i puljer i en bestemt rytme, så man kan gå flere "generationer" igennem.

Alle sikkerhedskopier og original software opbevares i brandskabe.
Nationalbibliografiske data opbevares desuden i en kopi udenfor huset.

Centrale baser og systemer

RC9000.

Sikkerhedskopiering:
Der foretages følgende former for sikkerhedskopiering:

- disk-disk kopiering af basen. Foretages automatisk om natten. Først foretages en nedlukning af systemet på dbc9001, hvorefter der laves en kopi af de vitale statusfiler (ca. 15 minutter). Herefter kan database og søgeproces startes igen. Herefter foretages disk-disk kopi af basen fra dbc9001 til dbc9003. Kræver nedlukning af modtagesystemet i op til 1 time.
- magnetbåndskopi af basen. Efter disk-disk kopieringen startes automatisk kopiering af databasefiler, transaktionsfiler m.v. samt af kopierne af statusfilerne til magnetbånd. Varighed 60-120minutter. Herefter startes opdateringen startes.

Der benyttes
6 båndpuljer mærket med nummer (1-6)
4 puljer mærket med ugedag (Tir, ons, tor, fre)
Hver **mandag** benyttes en af båndpuljerne med nummer til såkaldt ugekopi, fordi den afslutter produktionsugen og samtidig har opdaterig af

data fra Kommunedata.

Der er en aftale med Indbindingscentralen, som har de bånd, der er 2 uger gamle. Disse udskiftes hver uge.

RC-kat-maskiner

(UNIX-maskiner: RC970, RC971, RC972, RC973 samt FELIX)

Backup:

De eneste data som ligger på dem (udover operativ-systemet), er temporære data, som folk henter over fra databaserne på RC9000. Her behandles de, og overføres igen til RC9000. Der kan dog godt ligge en rimelig datamængde, der først behandles dagen efter, så der tages backup af disse maskiner hver nat. Da det sagtens kan være på et bånd, tager vi backup af **alt** hvad der er på maskinerne. Vi har så et backup-bånd til hver dag. Det ligger i et automatisk job (i crontab), at backuppen skal startes klokken 23.00.

Der anvendes 5 bånd i 1 pulje.

MANUEL

(UNIX-maskine: DIMS'en)

Mandag aften starter MANUEL backup: rc990'erens fil-system afmonteres, og der tages backup af alle filer i systemet. Herefter tages en totalbackup af hele databasen, inklusive TK-basen. Dette er normalt færdig til midnat.

Output fra denne backup afleveres i root's mail, som kontrolleres tirsdag morgen, samtidig med at båndet placeres i brandskab.

Der anvendes 5 bånd i én pulje

Det overvejes at ændre backup til daglig sikkerhedskopiering af BASIS-kopi og Lokaliseringsregister. Det ville muliggøre en hurtigere etablering på en anden maskine i nødstilfælde.

Danbib-maskiner

(AIX-maskiner: Harpo, Chipo)

Kommunedata har i følge kontrakt ansvar for sikkerhedskopiering og retablering af data. forpligtelsen til at sørge for, at der foretages sikkerhedskopiering af disse to maskiner.

Der er i kontrakten angivet fejlsituationer, imødegåelse og retableringsmuligheder.

Det foretages dagligt automatisk på tape. Det er aftalt, at DBC udskifter båndene dagligt.

NOVELL-server

Vi har to NOVELL-servere(dbc og dbc2) på nettet, hvoraf den ene er af backup-hensyn,hvor brugerne under normale forhold ikke har adgang.

Novell-serverensharddisk er delt op i 3 volumes: 'USER:', 'PROGRAM:' og 'SYS:'.

Backup:

Der kan skiftes til reserve-serveren(dbc), hvis vores "rigtige" skulle gå i stykker i løbet af dagen. Hver nat overfører vi alle data fra USER: og PROGRAM:. Dette giver os stor sikkerhed for, at vi hurtigt er kørende igen, hvis uheldet skulle være ude. Kun de data som er lavet i løbet af dagen ville være utilgængelige.
Vores administrative system, eller vores on-line databaser ville ikke berøres af dette skift.
Udover dette tager vi også backup på streamer-tapehver nat. Da der kun kan være 525 Mb på et bånd, er proceduren som følger:
Mandag og onsdag tages backup af USER:.
Tirsdag og torsdag tages backup af PROGRAM:.
Fredag tages backup af SYS: og binderi (NOVELL database over brugere og printere med tilkyttede rettigheder).

Puljer:

For USER: og PROGRAM: arbejdes der med 5 puljer, hvoraf den ene kun bruges den første backup-dag i måneden.
For SYS: er der 4 puljer.
Back-up'en opbevares i brandskab.

NCC

NCC (Network Control Center) er den maskine, som booter netkortet på en PC, når den tændes. NCC'en skal altid være tændt, og stå i 'boot-mode'. Hvis ikke den gør det, kan PC'en ikke kobles op hverken med TCP/IP eller IPX.
For at kunne boote PC'erne indeholder NCC'en en database over alle PC'ere på nettet.
Backup af databasen foretages hver fredag eftermiddag og tager ca 5 minutter. En PC kan ikke boote imens.
Da maskinen er en almindelig PC, der ikke bruges til andet, er en backup af selve databasen nok, da alt andet kan genskabes udfra original-disketter.

Bromaskine

(UNIX-maskine: DBC)
Backup:
Udover at denne maskine bruges som omstilling til vores data-baser og til Kommunedata, bruger edb-afdelingen den som produktionsmaskine i forbindelse med dataleverancer/medieudlægning mm.
Det kan godt dreje sig om store datamængder, der skal ligge længe.
Der skal derfor tages backup om natten af en disk, der er større end det, der kan være på 1 bånd.
Vi har delt det op således:
- Mandag: Backup af systemfilerne (/).
- Tirsdag: Backup af '/usr'.
- Onsdag: Backup af '/usr2'.

Der køres med 3 backup-puljer. Det betyder, at der tages backup 1 gang om ugen af hvert sit område. Det lyder måske af lidt, men man skal tænke på at data på denne maskine ikke ændres meget, og ydermere kan data genskabes udfra RC9000.

Andre systemer

CHIP:

Backup:
Der tages backup af databasen hver nat
Fredag tages der yderligere backup af resten.
Der køres med 3 puljer.

DAN:

Backup:
Der tages backup hver dag.
Der anvendes 5 bånd i 1 pulje.

Decentrale systemer og data

Alle vores PC'ere kører DOS. Sikkerhedsniveauet i det operativsystem er jo ikke kendt for at være højt. Alle har derfor adgang til en PC, da der ikke er pasord ved opstart, og harddisken ikke er krypteret.
Ansvaret for at vitale data ikke kommer ud, er lagt ud på brugeren. Dvs vitale data bør ligge på netværket på brugerens eget område, hvorved der samtidig sikres automatisk sikkerhedskopiering.
Data vil kunne krypteres, enten i WordPerfect eller PlanPerfect, hvis brugeren mener, det er nødvendigt.

Brugeren bestemmer selv, om data skal ligge på netværket, en lokal harddisk eller en diskette. Hvis data ikke ligger på netværket, er det også

brugerens ansvar at tage backup.
Brugeren kan dog bestille en total-backup af harddisken, og edb-afdelingen tager så backup af data over nettet.

Hvis data slettes ved en fejl, kan man kontakte edb-afdelingen, der så prøver at finde data igen. Dette kan gøres med NOVELLs 'salvage', DOSs 'undelete' eller NORTON's Utilities.

2. Systemernes adgangs- og sikkerhedsforhold

a. Fysisk sikkerhed

Adgang til maskinstuen:
Der er kun en uaflåst dør i DBCs åbningstid, og det er hovedindgangen, hvor der sidder en receptionist og tager imod gæster. Hvis der er besøg til nogle i drift-afdelingen,ringes der efter personen.
Porten til vareindleveringen vil være åben i forbindelse med varelevering, og folk vil kunne komme ind ad denne vej. Problemet er dog ikke så stort, da der kun er 1 uaflåst indgang til maskinstuen (der er ingen vinduer i dette lokale). I kontoret inden maskinstuen sidder der 5 medarbejdere, og lokalet eller maskinstuen er bemandet kl.8-16aht helpdesk-funktionen.
De aflåste døre er sikret med en kortlæser, hvor man uden for normal arbejdstid (man-fre 8-17) udover at indsætte kortet i læseren, også skal indtaste en 4-cifret kode. Den ene dør, som er åben mellem 8-17 låses automatisk, og koden skal derefter indtastes.
Udover dem som arbejder i edb-afdelingen, er der kun nogle få andre personer, der på deres kort har rettigheder til at kunne åbne dørene i edb-afdelingen.

Det er indskærpet overfor rengøringspersonalet, at man ikke om morgnen må efterlade rummene med åbne døre og vinduer.

Brandsikring:
Rundt om i huset er der installeret røgdetektorer, og en alarm går igang, som gerne også skulle tilkalde brandvæsnet. Yderligere er der opsat skumslukkere forskellige steder i huset.

Selve maskinstuen er beskyttet med halonanlæg. Ved udløsning vil halonen kvæle ilden, uden at forvolde skade på komponenter.
Anlægget skal konverteres til et INERGEN (ER470)-anlæg,da halon ikke længere produceres, og anlæg senest skal være nedtaget med udgangen af 1998. Pris ca kr. 275.000.

Til opbevaring af programmer og back-up anvendes brandskabe.

Køling:
Som sikring mod varme, er der i maskinstuen et køleanlæg. Det holder en temperatur på max 24 grader. Da dette anlæg indeholder et stof, som er på listen over dem, der skal "afskaffes", skal dette udskiftes inden for de nærmeste år.

Strøm:
EDB-installationerneer jordet selvstændigt.

Nødstrømsanlæg (UPS) fungerer som store batterier, dvs at de sørger for, at systemerne holdes i luften eller lukkes "pænt" ned, hvis de bliver udsat for strømsvigt. De er derfor betryggende at have tilsluttet systemer, hvor genetablering vil kunne tage lang tid eller data ikke vil kunne genskabes. Der er nødstrømsanlæg på alle systemer med undtagelse af

- gateway-forbindelser. Dette er ikke nødvendigt, da de jo bare er en viderestilling til vores RC9000.
- RC9000-maskinerne. Da spørgsmålet var til behandling i ledelsen besluttedes det at undlade dette, da strømafbrydelser er sjældne og følgerne relativt begrænsede. Maskinen vil i heldigste fald komme i luften af sig selv efter en strømafbrydelse.
  Hvis databaserne ikke er under opdatering, vil disse også startes op. Hvis de var under opdatering, er basen ødelagt, og man må skifte til backup-maskinen (Rc9003).

Indbrud
Vinduer er sikret med stanniolalarm, og ved afbrydelse startes alarmsirene, ligesom der er aftale med Securitas. Det betyder naturligvis ikke, at der ikke kan foretages indbrud og at maskiner vil kunne fjernes eller ødelægges, inden Securitas kommer frem, men det anses for mest sandsynligt, at man vil koncentrere sig om at tage de maskiner, der står først for, dvs PC'ere umiddelbart inden for vinduerne.
Maskinerne er ikke fastgjort eller mærket fysisk, men der findes en central registrant over hele maskinparken.
Tilsvarende findes der en registrant over anskaffet software.

b. Adgangskontrol til systemer og data

Pasord
Der har været afholdt gå-hjem-møde om sikkerhedsproblematikker, herunder specielt betydningen af pasord.
Det har resulteret i større opmærksomhed og accept af pasord, og der er udarbejdet en beskrivelse om valg af gode kodeord. Denne vejledning er tilgængelig på nettet.

Pasord til servere i maskinstuen er kendt af de medarbejdere, der arbejder med de pågældende systemer. Desuden er pasord for maskine og evt. programmel registereret i lukkede kuverter, som opbevares i brandskab, således at man i nødstilfælde kan hente oplysningerne her.

Med jævne mellemrum køres en pasordskontrol med en pasord-cracker (COPS). Hvis disse pasord gættes af denne cracker, for brugeren besked på at ændre sit pasord. Det tager ca 1 dag for COPS at køre pasord-filen igennem.

En ny version vil muligvis kunne sætte nogle bedre gæt op, og programmet kun checke de logins, som har fået nye pasord i siden sidste kørsel.

RC9000.

Adgangsrettigheder:

Almindelige brugere har kun ret til at starte søge-databaserneop. Hvis de prøver alt andet, smides de straks af maskinen.

Kun nogle få medarbejdere i edb-afdelingen har ret til alt fra deres skærm, fordi de er koblet direkte til maskinen, og kan derfor køre som hovedkonsol.

Der foretages logning, som på Artikelbasen også kan bruges til at gå tilbage hvis en bruger undres over regningens størrelse. Brugeren betaler for hver søgning, de foretager, og der logges derfor, hvornår en bruger er inde, og hvor mange søgninger, der er foretaget.

Legalisering:

Til selve RC9000 findes der ingen login-procedure, men når man har koblet sig op til en database, skal man taste login og pasord. Dette pasord udløber aldrig. Dvs at det er op til brugeren selv at ringe og bede om et nyt pasord. Og det er så os der laver et nyt til dem, men brugerne har også selv mulighed for at gøre det.

Sådan er systemet, men man skal tænke på, at det er kun et søgestyem, der kan ikke slettes eller ændres noget.

UNIX-maskinerne.

Generelt

Disse maskiner er de sikkerhedsmæssigt mest sårbare, da de kører en standardiseret protokol, og sidder på Internettet. Der er derfor vigtigt med en høj sikkerhed her. Det bør derfor overvejes om kontoen ikke skal låses hvis et forkert pasord tastes 3 gange (hvis dette kan lade sig gøre).

Vi kører allerede nu på nogle maskiner en test på, om en konto jævnligt bruges. Hvis den ikke bruges i en måned, låses den.

Maskinerne følger C2 (orange book), dvs vi kører med 'etc/shadow'.

Pasord til "root" giver adgang til alle funktioner. Derfor er det væsentligt at opretholde stor sikkerhed og justists omkring dem.

RC-kat-maskiner

Rent sikkerhedsmæssigt behandles disse 4 maskiner fuldstændigt ens, og vil derfor blive behandlet under et.

Adgangsrettigheder:

Hver bruger har deres eget område, hvor de må alt. Når de logger ind på

maskinerne, startes automatisk et program op, der sætter dem i forbindelse med databaserne på RC9000. Dvs de kan ikke andet på maskinerne end køre dette program, og skrive data ned på deres eget område.

Legalisering:
Brugeren skal ændre sit pasord hver sjette måned, og får en advarsel en uge i forvejen. Pasordet skal være på mindst 8 tegn.
Der køres med log af, hvem der har logget ind og hvorfra.

Manuel

Kun få maskiner kan etablere netforbindelse til Manuel.
Udover driftsmedarbejderne har databasebestyrerne adgang til DIMS, og de involverede medarbejdere til adgang til Trykte-kort-systemet.

Danbib-maskiner

(AIX-maskiner: Harpo, Chipo)
Kommunedata har i følge kontrakt ansvar overvågning af driftssystemernes tilgængelighed: opkobling via net og øvrige tilkoblingsmuligheder, UNIX-kernes og basisprogrammets tjenstlighed (herunder databaseprogrammellet).

Andre systemer

NOVELL-server

I forbindelse med projekt "ledelsesPC" vil der blive etableret modemadgang til Novell-serveren. Der vil blive anvendt lokalnummer i forsøgsperioden. Hvis denne resulterer i fortsat forbindelse, bør der være tilbagekaldsmodem svarende til de andre modemopkoblinger.

Normalt kobler medarbejderne sig på UNIX-maskinernefra Novell-nettet. Dette sker af praktiske grunde (bl.a. aht WP-Office). Man kan dog godt komme direkte til UNIX-maskinerne, og denne "nødprocedure" er beskrevet i "Råd og vink".

Adgangsrettigheder:
På **USER:** har brugerne kun rettighed til følgende:
- Sit eget brugerområde, hvor alt er tilladt.
- Backup-området for WordPerfect, hvor alt også er tilladt. Her kunne man overveje at fjerne slette-rettighederne, men vi har ment at brugeren selv skal have mulighed for at slette sin backup-fil igen.
- Et fællesområde for alle brugerne, hvor de kan ligge de filer, som alle skal kunne se/rette i. Her er alt selvfølgelig også tilladt, da de selv skal rydde op på dette område.

På **PROGRAM:** er rettighederne lidt forskellige fra bruger til bruger. Brugerne er medlemmer af forskellige grupper, der gør at de har forskellige adgangsrettigheder. Nogle har læserettigheder i forskellige kataloger, mens andre også har ret til at skrive og slette.
Alle programmer og system-filerer dog **read-only**, så en bruger ikke får slettet noget forkert ved en fejl.

På **SYS:** har alle brugere kun læse-rettigheder.Dette er nok, da det er her vor alle utilities i NOVELL ligger. Det er også her, vi lagt lagt vores egne små utilities. Større utilities/programpakker ligger på PROGRAM:. Selve brugernes mail-kataogerligger på SYS:, hvor man selvfølgelig har Create-mulighed.

De fleste brugere har kun ret til at optage sammenlagt 5 Mb på USER:. Dette har vi indført, da vi er 130 brugere, der skal dele ca 700 Mb og de kan jo altid ligge data enten på disketter eller på deres lokale harddisk. Det samme har vi gjort på PROGRAM:.

Legalisering:
Brugerne er defineret med et unikt bruger-id og et pasord, som er obligatorisk. Pasordet skal være på mindst 4 tegn, og brugeren bliver tvunget til at skifte det hvert halve år.
Når en bruger bliver opfordret til at udskifte pasordet, kan man svare nej til dette 6 gange (hvis det ikke lige passer at skifte på det pågældende tidspunkt). Derefter vil kontoen blive låst, og kun supervisor kan låse den op. Man kan ikke bruge det samme pasord igen.
Når en bruger vil koble sig på nettet, tastes først login-id.Selv om dette ikke findes, promptes man også for et pasord.
Hvis login-id findes, men pasord tastes forkert 3 gange, låses kontoen i et kvarter. Dette burde besværliggøre det for udefra kommende personer som hurtigt vil prøve at snige sig ind. Pasord skal forhindre udefra kommende i at snuse, og interne brugere, som er interesserede i ting, som ikke vedkommer dem.
Når vi giver modemadgang til Novell-serveren vil det være nødvendigt at tage pasord-reglerne op til fornyet overvejelse.

Bromaskine

Denne maskine bruges dels til at omstille eksterne brugere til vores databaser, dels til produktionsformål.
Dobbeltfunktionen betyder, at det sker, at maskinen bliver så belastet, at den ophører med at fungere.
Der arbejdes derfor på at få brofunktionen lagt på en selvstændig maskine.

Modem-tilslutning:
Der sidder et modem på denne maskine. Den er sikret med et call-back system, hvor kun nogle få medarbejdere i edb-afdelingen, og nogle få

kunder er lagt ind. Der arbejdes med en 4-cifret kode som er forskellig for hver bruger. Hvis koden er der, ringes der tilbage til det nummer, som systemet er sat op til. Vi har dog for en sikkerheds skyld lagt et pass-through nummer (gennemstillingsnummer) i, så vi kan komme ind på maskinen fra et nummer som ikke er lagt ind i systemet. Da vi arbejder med 4 cifre, og bruger et lokalnummer (gennemstillingsnummer), er det ikke en større risiko. Call-back systemet ringer tilbage på samme linie, men selv om man kommer igennem her, skal man jo stadigvæk taste login/pasord.

Adgangsrettigheder:
Brugerne har kun læse-rettighed i området, hvor '.profile' ligger, som viderestiller dem til RC9000.

Legalisering:
Folk logger ind med deres eget bruger-idog pasord, hvis de er specielle. Det mest almindelige er, at der logges ind med et standard login (som bruges af mange brugere), som uden at spørge om pasord, omstiller til en af RC9000s databaser.

CHIP:

Man kan ikke udefra komme i forbindelse med CHIP, idet den ikke svarer.

Adgangsrettigheder:
Når man logger ind på CHIP får man en indgangsmenu, som viser hvilke systemer, man har adgang til (pt. Pro:Mis og Tidsstyringssystem)
I Pro:Mis får brugeren via menuopsætning adgang til de dele af systemet, som man skal have adgang til.
Det er herefter ORACLE-databasen, der bestemmer hvilken bruger der må se hvilke data, og hvilke bruger der også har skriverettigheder. Det eneste som ikke er læseligt for alle i databasen er lønoplysningerne.

Legalisering:
Hver 3 måned skal pasordet ændres (advarsel 1 uge i forvejen). Mindst 8 tegn langt. Der køres med log, og spærring på at det kun er maskiner fra et kendt domain, der kan logge ind.

DAN:

Adgangsrettigheder:
Da denne maskine udover at være nameserver, også varetager mail-funktionen, skal alle i DBC principielt have adgang til denne maskine. På maskinen har de så kun adgang til deres eget brugerområde, og kan modtage/sende post.

Legalisering:
Denne maskine har kontakt med omverdnen.

Decentrale systemer

Bortset fra de bærbare PC'ere er der ikke adgangskontrol på vores PC'ere.

Det ses ofte af folk går fra deres PC (i kortere eller længere tid), mens de stadigvæk er logget ind på nettet. Da de fleste kører Windows, vil dette kunne løses ved at sætte pause-skærmen op med pasord. Dette er ikke implementeret.

Alle vores PC'ere kører med virus-check,der ligger resident når PC'en er tændt. Der checkes for virus i boot-sector og memory.
Disketter kan checkes selv, ved at brugeren tager en 'dir' på dem, eller bruger indeks-funktionen i Word/PlanPerfect. Hele harddisken kontrolleres en gang om måneden, når vi alligevel kopierer ny version af virus-checkprogrammet (Dr. Solomon) ned over nettet. Hver nat checkes endvidere NOVELL-serverens harddisk for virus.
I "Råd og vink"-kataloget på nettet findes vejledning vedrørende viruscheck.

3. Adgangskontrol

Oprindelig aktivitetsbeskrivelse
Netadgang/overvågning

Navn	Opfølgning på etableret netadgangskontrol
Formål	At få udnyttet eksisterende programmel til alarmering ved unormal aktivitet på nettet
Kritiske succesparametre	Opfølgning og daglig rutine fungerer
Riscici	At funktionen drukner i andre rutiner At der ikke er den fornødne viden om programmellets funktionalitet
Slutprodukt	Beskrivelse af fordelingen af analysemulighederne

DBC's net
Selve netværket består af 6 segmenter:

- 3 stk IMC-segmenter, 1Mbps. Her sidder nogle få Partnere (Seddelfortegnelsessystemet)
- 1 stk IMC-segment, 10 Mbps. Her sidder vores RC9000'ere på nettet, samt de maskiner som fungerer som gateway til TCP/IP-verdenen. RC9000 kan kun køre IMC (en gammel RC-protokol).
- 2 stk 10 Mbps segmenter, hvor der kører TCP/IP-og IPX-trafik.

Internet router:
Denne kasse gør at vi er tilkoblet det verdensomspændende Internet. På denne måde kommer mange biblioteker ind og benytte vores bibliotekssystemer.

Internet MAC bridge:
Her sidder en fast opkoblet linie til Kommunedata (64 Kbps), hvor SNA-kunder (DATEX) til KMD kan omstille sig til vores databaser. Da vi snakker om faste linier, er det eneste problem stort set, at den skal være kørende.

BC, BC970, BC971, BC972 og Felix
Disse UNIX-maskiner er vores gateway-maskiner, som kan nås fra Internettet. På BC sidder yderligere et modem, så man også kan komme ind over DATEL.

DAN:
Denne UNIX-maskine er vores **nameserver** til (Inter)nettet, dvs den maskine, der omsætter mellem navn og IP-nummer,så man ikke bever at skulle huske nummeret, men kan connecte sig til et navn.
Udover dette, varetager den også mail til og fra Internettet.

NCC:
Står for Network Control Center. Er den maskine som booter vores Dataco-netkort.Dvs når en PC tændes, bootes dens netkort fra NCC'en. Herfra får den også sit IP-nummer.

Overvågning af lokalnettet

Der er etableret en særlig maskine (server) med netværksovervågningsprogrammel (*Comtest LA*).
Maskinen overvåger det ene segment, men vil hurtigt kunne flyttes til det andet segment ved at flytte kablet fra et transceiverstik til et andet.

Programmet hedder *Comtest LA*, som blev valgt i 1993 efter evaluering af et antal produkter.
Programmet anvender et specielt kort med egen 32-bit-processorog 4 Mb RAM. som gør programmet uafhængigt af PC'ens egen processor. Det betyder, at falder selve serveren af, vil hele forløbet være registreret.
Programmet har reel multitasking, idet det samtidigt kan fange trafikken (100%), analysere samt gemme og vise oplysningerne. Der kan opsamles data fra alle 7 lag i OSI-standarden.
Data kan filtreres vha avancerede selektionskriterier, og opsamlede data kan genspilles og data kan overføres til regneark.

Alle PC'ere, NOVELL-servere og UNIX-bokse er indtegnet i overvågningssystemet. Derved kan man med det samme se for hver maskine, hvor meget trafik de laver, hvornår frames sendes (og hvor store de er) og om den genererer nogle fejl.

Systemet er sat op til at alarmere, hvis en af serverne "går død". Dette kan umiddelbart lade sig gøre for NOVELL-serverneog NCR-maskinerne (UNIX), men nok ikke for ICL-maskinerne. Det undersøges pt, om der kan købes en speciel driver, for at det kan lade sig gøre.
For IMC-maskinernekan en sådan overvågning IKKE lade sig gøre.

Alarm fremkommer desuden, hvis
- netbelastningen kommer over 30%, eller at
- antal frames pr sekund er over 400.

Hver morgen checkes systemets alarmlog for at se om der er alarmer, og der tages stilling til, om og hvorledes der skal gribes ind.
Hvis nogle maskiner er faldet af, vil også det stå der (kun dem der er sat op til det).

Hver aften klokken 21 udskriver systemet en log (i en fil) over, hvor meget nettet har været brugt, og af hvilke maskiner.

Der logges
- antal sendte bytes,
- frames,
- collisions og
- genererede fejl registreres.

Loggen opbevares på nettet.

Hver mandag udskrives en log (igen i en fil) over netbelastningen (og antal collisions) i løbet af ugen. Denne opbevares ligeledes på nettet. Log-filernekan bruges til at danne sig et generelt overblik over, hvordan vores net "ser ud", når det "kører". Når det så ikke fungerer, som det skal, kan man ud fra de gamle logs se, hvordan de varierer i forhold til de "fejlramte" logs, og måske udfra det kan gennemskue, hvad der er galt.

Hver måned, vil systemets filer blive resat. Dette gøres både for at kunne bevare overblikket (få slettet gamle data, som vi jo nu har som backup), men også for at undgå at filerne pludselig bliver fyldt op, når vi har mest brug for systemet.

"Sikkerhedsmaskinen" (Petbin)

Den eneste maskine, der kan kommunikere ind til PETBIN er DAN.

I forbindelse med vores sikkerhedsaktiviteter har vi udpeget Peter Binderup som den, der i praksis tager sig af sikkerhedsspørgsmål.

Til brug for denne funktion er der installeret en software-pakke (*TCPWRAPPER*) på UNIX-maskinerne(ekskl. AIX og LINUX).
Det er et public domain program, som gør det muligt at sætte regler op for, hvem må komme ind hvor. Det fungerer på den måde, at det sættes op på de standardiserede porte på UNIX-maskineni stedet for de normale programmer (Telnet, FTP osv). Reglerne ligger så i nogle filer. Reglerne bestemmer, hvad der skal testes for. Hvis testen er OK, kalder wrapperen så det normale program, og der kan fortsættes.

Alt hvad wrapperen modtager, logges på en sikkerhedsmaskinen. Det giver for det første et godt overblik over, hvem der har forsøgt at logge ind hvorfra, samtidig med at vi kun får dem ind, vi vil have ind. Navn og IP-nummerpå indloggende maskiner, slår wrapperen op i nameserveren.

Funktionen er, at når nogen åbner en forbindelse fra deres maskine til vores, kommer de først i forbindelse med wrapper-softwaren, som lige laver nogle kontroller, og derefter stiller om til den "rigtige" maskine.

Disse kontroller kan konfigureres meget fleksibelt.

Der foretages en logning af alle, der forsøger at logge ind.
Når wrapper-softwaren åbner en indkommende forbindelse, logger den denne begivenhed vha "*syslog*" (standard UNIX-facilitet).syslog kan man igen konfigurere til at gøre forskellige ting alt efter, hvad det er for en hændelse, der registreres. Konkret sender UNIX-maskinerneoplysninger-ne til "sikkerhedsmaskinen" (Petbin).
For at man kan vide sig sikker, skal man sørge for, at det er meget vanskeligt at fjerne en sådan logning igen. Derfor er wrapper-softwaren på "sikkerhedsmaskinen" sat op til at nægte adgang for næsten alt, da hackere ellers bare kunne gå ind og fjerne sine spor.

Syslog bruges også til at det en wrapper-logninger. Vi er begyndt at indbygge i de forskellige systemer, at de kalder *syslog*, hvis der er noget galt. Hvis f.eks. DIMS'en går ned logges hændelsen. Meddelelsen kan sendes ud til bestemte personer, så man kan gribe ind.
Når DIMS'en genstartes logges dette også.

Den type overvågning er indført på / for
- CHIP natjob
- Sikkerhedskopiering af Artikelbasen
- DIMS
- Overførsel af TK-kunderegister(TK-adm-system)

Der er planlagt udvidelse til at tilsvarende løsninger skal etableres for
- artikelbasens oppetid
- RC-katsystemet

Internettet.

Vi er tilkoblet det verdensomspændende Internet på en 2Mbps-forbindelse.
Hele driftsansvaret ligger hos UNI-C,og den eneste interesse vi har i det (udover at vi kan bruge nettet), er, at vi ved hvem, der har lov til at komme ind på vores net. Der er derfor opsat nogle filtre i routeren, der gør, at ikke alle kan komme i forbindelse med vores net.

Disse filtre er ikke så nødvendige mere, som de var før i tiden. Det skyldes, at vi med *TCP-wrapperen* har fået et stærkt stykke værktøj mth log og rettigheder. Men vi kan lige så godt stoppe trafikken der, så uvedkommende får endnu sværere ved at komme ind på vores net.
Vores router forbinder også Depotbiblioteket, men de kommer aldrig ind på vores net, da routeren sender dem forbi, og ud på selve Internettet. Grunden til at det er lavet på denne måde, er jo at UNI-Cskal have selve nettet til at hænge sammen.

Overvågningsprogrammel til UNIX

Oprindelig aktivitetsbeskrivelse

Formål	At få klarlagt funktionalitet og priser på udstyr, der kan sikre overvågning i UNIX-miljø - helst alle maskiner
Kritiske succesparametre	Demonstration af funnktionalitet Pris modsvarer besparelser ved tilsvarende manuel indsats
Riscici	At produkterne er maskinspecifikke At prisniveauet er prohibitivt
Slutprodukt	Indstilling om evt. anskaffelse

Den oprindelige tanke med denne aktivitet var at skaffe et overblik over standardprogrammel til UNIX, som ville muliggøre maskinovervågning og jobafvikling på samme måde som man kender det fra main-frame-området.

Følgende produkter er der indhentet materiale om:

CA-UNICENTER

CA-UNICENTERer udviklet af Computer Associates.
Programmet dækker følgende områder

- Sikkerhed - adgangskontrol og rapportering
- Konsol og meddelelseshåndtering
  Opfanger meddelelser og reagerer på disse efter definerede regler. Driftsautomatisering
- Problemhåndtering og 'helpdesk'
  Lagrer problemer i database. Bruges til opfølgning og erfaringsbase
- Planlægning af batchjobs
- Printhåndtering
- Rapportdistribuering
- automatisk arkivering og backup
- statistik
- overvågning (performance)

Programmet installeres på den enkelte platform. CA-UNICENTER kan bl.a. leveres til NCR SVR4. Imidlertid koster systemet ca kr. 400.000 og er som sagt bundet til den enkelte maskine (man skal helt ned i unix-kernen).

SISoft X-Mon

XMon er software beregnet til driftsafvikling og overvågning og performance i et distribueret miljø.

XMon kan bl.a. overvåge:

- ressourcer
- performance
- sikkerhed
- databaser
- applikationer

Problemer eller overskridelse af grænser medfører alarm/advarsel.
Alle målinger registreres og kan anvendes som driftsdokumentation og analyse.
Der kan leveres overvågningsmodul til ORACLE.
Netværksovervågning er integreret.

BMC Patrol

Dækker samme funktioner som ovennævnte XMon.

Vi har som det fremgår selv lavet flere programmer (scripts), som langt hen ad vejen vil kunne løse vores behov, - og ikke mindst kunne skræddersyes til vores formål.
Det er derfor vores vurdering, at der vil være for mange omkostninger ved at anskaffe et færdigt program. Dels er der selve anskaffelsen, men også det at sætte sig ind i programmets funktioner og virkemåde (og vedligeholde denne viden) vil være ressourcekrævende.
Med en mindre indsats mener vi, at vi ville kunne komme meget langt med de standardværktøjer, der findes i UNIX (og ORACLE).

RAID

En helt anden form for sikkerhed ville kunne etableres med RAID.

RAID er en teknologi, som kan reducere problemer i forbindelse med hardware nedbrud.
RAID betyder Redundant array of independent discs, og det indebærer en øget sikkerhed og forbedret peformance. Der findes RAID-klasser fra 0 til 5.

I RAID indgår følgende begreber:

1. fysiske drev
2. logiske drev (modsat fysiske) bestående af blokke
3. "streams", som består af blokke, og som kan komme fra forskellige fysiske drev
4. blokke (dele af den fysiske disk) som består af "stripe blocks"
5. "stripe blocks" vedrører den logiske disk og er af variabel længde

6. sektor, som adresseres af CPU'en. En sektor er 512 bytes.

Vi ville kunne drage fordel af RAID 5, som benytter "stripe blocks". Metoden betyder, at maskinen kan læse og skrive samtidigt (hurtig), og fejlkorrektion er spredt på diskene (stor sikkerhed).
Ca. 20% af diskkapaciteten anvendes til fejlkorrektion.
RAID sikrer, at man kan køre videre, selv om en disk skulle falde ud: data gendannes på tilbageværende disk(e). En disk vil kunne udskiftes med en anden, mens maskinen kører.
NCR-3450 kan i givet fald køre med forskellige RAID samtidig.
Der kan etableres RAID til NCR og IBM fabrikaterne.

NCR har desuden en softwarepakke, *LifeKeeper*, som kan administrere flere maskiner af 3000-serien, og som garanterer en samlet oppetid på 99.99%. Det er baseret på, at koble flere maskiner sammen, således at den ene kan overtage den andens funktioner, hvis det skulle blive nødvendigt.

4. Reetablering

Oprindelig aktivitetsbeskrivelse:
Vurdering af reetablering af maskiner

Formål	At finde ud af, hvor hurtigt der kan genskabes produktion på andre maskiner
Kritiske succesparametre	At maskiner kan findes indenfor 7 dage (dvs. tab af én arbejdsuge)
Riscici	At reetablering ikke kan ske indenfor 7 dage At omkostningerne ved det nødvendige beredskab er for høje
Slutprodukt	Delrapport med indstilling (skal vi?, og hvis ja, hvem)

Der er i de sidste par år gennemført en maskindublering på en række nøglemaskiner bl.a. med henblik på at øge fleksibiliteten og driftssikkerheden.

Systemer
RC-kat
RC-kat programmellet er placeret på maskinerne 970, 971, 972 og 973 (primært DBC brug) samt Felix (primært til "felix-bibliotekerne", som katalogiserer til Danbib). Brugerne kan selv vælge maskine.
Disse UNIX-maskiner er i princippet standardmaskiner, som vil kunne genanskaffes ved almindeligt køb. Den egentlige forskel ligger i et specielt netkort, som kan håndtere to protokoller.

RC-lib
RC-lib-programmellet er placeret på DBC9001, DBC9002 og DBC9003. Disse maskiner er RC8000-kompatible aht til RC-lib-programmet. Maskinerne kan stadig leveres, men med leveringstid.

Bl.a. til validering af data, der sendes mellem RC-kat og RC-lib er der indskudt Manuel (DIMS) På denne maskine er desuden installeret Oracle. Denne maskine er en kraftig server.
Falder maskinen ud kan man standse opdateringen. Ved længerevarende nedbrud omgå valideringen og som sidste udvej flytte programmel og data.
DIMS-programmet kan køre på alle NCR-maskinerne (forudsat at der er diskplads mm), og er dermed flytbart inden for 1-2 døgn.

DanBib
Driftsansvaret for DanBib ligger hos Kommunedata, men det er DBC, der har indkøbt maskinerne, og som er ansvarlige for deres vedligeholdelse. Der er tale om IBM Risc-maskiner med AIX-operativsystem (en IBM UNIX). Harpo er databasemaskine med Oracle, og Chico er søgemaskine.

Bromaskine
En unix-maskine, som fungerer som bro til 970'erne / 9000'erne.

Netværk
Der anvendes en standard dos-maskine som server til netværket.
På denne maskine ligger desuden alle fælles programpakker (WP-familien mm).
Denne maskine er dubleret, således at daglig drift foregår på dbc2, mens dbc er backupmaskine, og kan anvendes til undervisning af nye programpakker inden de tages i anvendelse.

Hvis Novell-serveren falder fra kan man ikke arbejde med kontorprogrammerne, hvorimod der er alternative adgangsveje til både RC-kat og Pro:Mis.

NCC.
NCC (Network Control Center) er den maskine, som booter netkortet på en PC, når den tændes.
Hvis NCC'en skulle gå i stykker, har vi tilkaldetid på 3 timer. Vi burde selv kunne genskabe en NCC, hvis det bare er selve PC'en, der går i stykker. Hvis selve NCC-kortet ryger, går der op til 3 timer, inden vi får en tekniker ud.
Falder NCC'en fra kan vi med andre ord risikere, at samtlige medarbejdere ikke kan benytte nettet i 3-4 timer.
Derfor bør der etableres løsning for en reserve-NCC, som kunne sættes ind i stedet, hvis uheldet er ude.
Der er indhentet tilbud på en sådan løsning. Prisen er ca kr. 40.000.

Pro:Mis
Det administrative system er placeret på en UNIX-maskine (Chip). Programmet er baseret på Oracle.

Vedligeholdelseskontrakter
Der er tegnet vedligeholdelseskontrakter på alle kerne-maskiner og netværksdelen. Fra tilkald til påbegyndt rettelse er tiden max. 4 timer. Aftalerne indeholder udbedring eller udskiftning med nye reservedele.

Maskinparken er relativ ny og moderne, og vil kunne erstattes af nyindkøbte maskiner.

Genetablering
Dubleringsstrategien betyder, at det skal være en ekstraordinær hændelse, der kan forårsage længerevarende nedbrud. Ved ekstraordinær hændelse tænkes her på brand eller hærværk, som kan sætte dubleringseffekten ud af kraft.

I såfald er der tre løsningsmodeller for genetablering:

1. Erstatningsmaskiner
Så længe der er tale om standardkonfigurerede maskiner, er problemerne til at overse, men nogle af maskinerne har specielle konfigurationer, og leverandørerne anvender ordrefabrikation for at undgå lageromkostninger. Det kan betyde, at de normale leveringstider er mere end en uge.

2. Lånemaskiner
For at få driften hurtigt igang, vil det kunne være nødvendigt i en periode at prøve at låne en maskine af tilsvarende konfiguration, som den, der er sat ud af spillet. Her gælder som ovenfor, at det er yderst begrænset, hvad de enkelte leverandører ligger inde med.

3. Andet driftsmiljø
DBC har flere kommunikationsveje, som muliggør at der kan gennemføres on-linedrift på eksterne installationer, forudsat at applikationer og data kan overføres.

ICL, NCR og IBM er blevet bedt om at fremkomme med forslag til, hvorledes de vil få vores systemer op at køre hurtigt, herunder et økonomisk overslag. Spørgsmålet har også været rejst overfor Kommunedata, som jo dels har RC udstyr i Ålborg og ellers anvender IBM.
Der forventes tilbagemelding primo maj 1994.

Hvis evt skade lader maskinstuen være intakt, og rammer arbejdspladser i huset, vil der kunne etableres opkoblinger, der gør det muligt for berørte medarbejdere at arbejde hjemmefra, hvis der ikke kan findes alternative placeringer i huset.

29. august 1994

Dansk Biblioteks-Center·as

Sikkerheden i DBCs on-line systemer: DANBIB, Artikelbasen m.m.

på teammøde i edb/produktudvikling vil vi tage sikkerheden omkring DBCs on-line systemer op til drøftelse. Vi tager udgangspunkt i de nuværende sikkerhedsforhold (ordnet kaos) og prøver at give vores bidrag til et sikkerhedssystem som kan leve op til forventningerne hos vore brugere.

Vi tager sikkerhedsforholdene op nu af flere grunde. En enkelt og tilstrækkelig grund er at det nuværende sikkerhedsnet i DANBIB er mangelfuldt. Det må være grund nok.

Vi kan bruge forløbet af den just overståede nedbrudsperiode fra to. d. 25. aug. kl. ca. 22:00 til søn. d. 28. aug. kl. ca. 22:15 som instruktivt eksempel (på hvordan vi ikke skal gøre ?).

Sikkerhedskravene i DANBIB indeholder elementer som vedrører:

1. (utilsigtet) nedbrud: forebyggelse og overvågning,
2. (hurtig) retablering af drifttilstand efter nedbrud,
3. (utilsigtet) adgang: forebyggelse og overvågning,
4. sikring af adgang til systemet for brugere,
5. sikring af adgang til systemet for medarbejdere (herunder "tjenesteydere"),
6. (utilsigtet) tab af data: forebyggelse og overvågning,
7. andet ?

Stikord til de enkelte punkter:

1: (utilsigtet) nedbrud: forebyggelse og overvågning

- Udvikling på udviklingsmaskiner,
- aftestning af programmel og maskinel før installering,
- overløb af data/filer,
- adgangsbegrænsning,
- automatisk overvågning fra uafhængig maskine,
- overvågning af tjenesteyder.

2: (hurtig) retablering af drifttilstand efter nedbrud

- automatisk tilkald af nøglepersoner,
- adgang til maskineri/maskinstue for nøglepersoner,
- "passepartout" og orientering til nøglepersoner,
- nøglepersoner hos tjenesteydere,
- dublering af nøglepersoner.

3. (utilsigtet) adgang: forebyggelse og overvågning

- adgangsbegrænsning gennem passwordkontrol,
- adgangsbegrænsning gennem router-låse,
- adgangsbegrænsning ved aftale,
- orientering til medarbejdere om "usikre områder",
- logning af aktiviteter på maskineri/net,
- adgangsbegrænsning til bygninger.

4. sikring af adgang til systemet for brugere

- åbne af adgangsveje,
- information til brugere om systemets tilstand,
- information til brugere om brugen af systemet,
- information til brugere om systemets åbningstider o.l.

5. sikring af adgang til systemet for medarbejdere (herunder "tjenesteydere")

- revision af UNIX-brugergrupper,
- etablering af netværk af nøglerpersoner (sikkerhedsgruppe ?)
- beskrivelse og evt. revision af ansvarsfordeling for maskineri og systemdele (incl. find-box),

6. (utilsigtet) tab af data: forebyggelse og overvågning

- gennemførelse af sikkerhedskopiering,
- retablering af tabte data,
- kørselslogning,
- advarsler og fejlmeddelelser til bruger (e-mail).

Eksempel fra det virkelige liv ...:

- Torsdag d. 25. aug. 1994 kl. ca. 22:00 konstateres driftstop på HARPO,
- drift søges genoprettet af DBC nøgleperson in situ, opgives fredag kl. ca. 4:00,
- driftstop rapporteres til DBC nøgleperson fredag kl. ca. 8:05,
- driftstop rapporteres til KMD umiddelbart efter,
- KMD møder op fredag kl. ca. 11:00 (?),
- Find-box lukkes for adgang til DANBIB med oplysning om genoptagelse af drift "mandag formiddag",
- KMD arbejder hele fradag uden held,
- KMD oplyser at: de mangler person med expertice (på ferie), at de derfor ikke vil møde frem før mandag, at de i øvrigt mangler adgangskort til DBC,
- Efter konference med foersatte indvilliger KMD i at møde op lørdag d. 27. aug. kl 10:00,
- adgangskort udleveres af DBC nøgleperson til KMD på medarbejders privatadresse,
- KMD melder HARPO driftklar lørdag kl. 14:00,
- DANBIB er utilgængelig lørdag og søndag grundet find-box,

- Find-box åbnes søndag kl. 22:00.

Find fem fejl ... eller flere !

m.v.h. ...

Dansk Biblioteks-Center·as