OPERATOR
CONSULT ApS

SECURE-WARE

- om edb-sikkerhed,
  data-sikkerhed og data-sikring

Skribent:

Poul Badura

Indholdsfortegnelse:

Indholdsfortegnelse:

Indledning:

Hvorfor data-sikkerhed ?

Det kan feks. besvares med et par mod-spørgsmål:

Hvorfor tegne forsikringer mod indbrud, hærværk, invaliditet og død ? Hvorfor indføre sikkerhedsseler, ABS-bremser og oppustelige puder i biler, og hvorfor medbringe redningsvest når man skal ud at lystsejle eller surfe ?

Sikkerhed, eller en bedre betegnelse: Sikring, er værnet mod risici - altså alle de mange ting der kan gå galt for os, med eller uden egen skyld - hændelser vi absolut helst havde været foruden.

Murphy's Computerlove siger feks.

Alt hvad der kan gå galt,
vil gå galt
- især på din PC !

Udgangspunktet for sikkerhed/sikring er altså at man tager omhyggeligt stilling til, hvilke uheldige hændelser der med rimelighed kan forekomme hos os, hvordan de kan opstå, hvem eller hvad der kan tænkes at være årsagen dertil, for derefter at tage stilling til, hvordan kan man bedst sikre os mod dem.

Og her er det vigtigt at betænke, at ikke alt behøver at være sikret 100%. Måske er sandsynligheden for et uheld meget lavt, eller uheld og tab på området vil kun have meget begrænsede effekter for arbejdet eller økonomien.

Når sikkerheds- og sikringsniveauet er fastlagt for de forskellige nøgleområder, lokaler, maskiner, systemer, data, kommer

valget af værktøjer og produkter som bedst og billigst kan opfylde behovene.

Det skal også nævnes, at sikkerhed og sikring ikke er en statisk tilstand, men en proces, som løbende skal evalueres, justeres og udbygges i takt med virksomhedens ændrede behov.

Indledning:

PC'en står efterhånden i alle kontorer solgt under betegnelsen Personal Computer.

Salgsmæssigt er det genialt (bemærk udbredelsen) men sikkerhedsmæssigt er det nærmest en katastrofe !

Efter forfatterens bedste overbevisning kan en maskine (en PC) på en arbejdsplads aldrig være personlig; det er virksomhedens maskine, det er virksomhedens data, det er virksomhedens arbejdstid, og det er virksomheden der betaler den pågældende for at benytte PC'en i virksomhedens tjeneste.

Derfor bør forkortelsen omskrives til at betyde

Production Computer

eller som det allerede har været benyttet, specielt iforb., med PC'er opkoblet i netværk

Workstation

Dermed indikeres også, at data på maskinen er virksomhedens og at virksomheden derfor bestemmer hvordan de skal opbygges, håndteres og gemmes.

* **Det er virksomhedens PC**
* **Det er virksomhedens data**
* **Det er virksomhedens arbejdstid**

Ved enhver form for uheld, ulykke eller kriminalitet omkring maskiner, systemer eller data er det

* **Virksomheden der skades**
* **Virksomheden der kommer i avisen**
* **Virksomheden der mister kunder og omsætning**
* **Virksomheden der skal betale omkostningerne**

Indledning:

Som så meget andet er det i sidste ende ledelsen der er ansvarlig for sikkerhed og dermed også EDB-sikkerhed, Data-sikkerhed og Data-sikring.

Top-ledelsen skal udstikke de nødvendige retningslinier, dvs. etablere en sikkerhedspolitik for virksomheden.

Det vil en politik som naturligt også omfatter de almindelige adgangsregler til virksomhedens forskellige afdelinger, produktionslokaler og lagre for både medarbejdere og gæster, brandsikring, varesikring mv..

Politikken vil typisk også omfatte grundlag for tegnelse af nødvendige forsikringer feks. for ansvar, produktansvar, drifttab mfl.

Man kan i princippet sikre sig mod alt, men i praksis vil der være mindst 2 ting der er med til at fastlægge niveauet:

Risikoen for en bestemt hændelse og dens arbejdsmæssige konsekvens, og økonomien for at sikre sig contra den økonomiske konsekvens af hændelsen.

Murphy's Computerlove siger feks.

I edb-verdenen slutter uheld aldrig, men overlapper hinanden i en stadig strøm !

Lad os i det følgende gennemgå en situation ad gangen -

- **hvad kan gå galt**
- **hvordan kan vi forhindre det**
- **hvad gør vi hvis det er gået galt**

Udgangspunktet er enkelt-bruger PC'ere, men de fleste forhold er også gældende for udstyr koblet op i større netværk.

Indledning:

Et par definitioner vi sikkert være på sin plads for at systematisere emnet en lille smule.

EDB-SIKKERHED:

Det at sikre driften af sit udstyr mod udfald og nedbrud, periodiske fejl, ustabilitet og andre tekniske problemer.

Eks.

Netop i nedbrudssituationer vil der være en potentiel fare for at data tabes med både tid- og økonomiske konsekvenser til følge.

DATA-SIKKERHED:

Det at sikre sine data's validitet (korrekthed) og integritet (adgang og anvendelse), samt at sikre gen-skabelse af data efter et uheld eller en katastrofe.

Eks.

Her er bla. Registerloven og Bogføringsloven relevante, men den almindelige sunde fornuft i at passe på sine data må heller ikke glemmes.

DATA-SIKRING:

At sikre sine data-medier mod fysisk skade under transport og opbevaring.

Eks.

Forsendelsesmedier indeholder i mange tilfælde personhenførbare data og ofte knyttet til store pengeværdier som skal overføres mellem forskellige parter.

Ødelagte, tabte eller forsinkede medier kan give direkte tab iforb. med forsinkede edb-kørsler, rentetab mv.

Sikkerhed generelt:

Som del af indledningen til denne bog finder vi det hensigtsmæssigt at omtale nogle generelle og overordnede principper omkring edb-sikkerhed og data-sikring.

Det er et samfundsmæssigt krav, at enhver virksomhed der anvender moderne informationsteknologi også lever op til et mindstekrav til datasikkerhed.

Dette krav kommer til udtryk igennem lovgivningen bla. i form af Registerloven og Bogføringsbekendtgørelsen; den sidste dog kun indirekte i kraft af "Bonus pater" betragtninger.

"Bonus pater" betragtninger er også udgangspunktet for de såkaldte "gode skikke", der inden for forskellige brancher er normdannende, feks som beskrevet i publikationen

"God EDB-skik - eller hvordan vi kan gøre tingene bedre"

fra FSR - Foreningen af Statsautoriserede Revisorer.

Ud over de motiver, der følger af de lovgivningsmæssige krav, er der også et forretningsmæssigt motiv for at etablere datasikkerhed, feks. understøttet af Markedsføringslovens regler om konkurrenceforhold og formidling af intern viden.

Motivet består i, at virksomheden har behov for at beskytte den investering, både i form af forbrugt arbejdstid og i form af direkte investeringer, som virksomheden har gjort.
Tillige er det væsentligt at fremhæve, at data i sig selv skal betragtes som immaterielle aktiver.

Det er med udgangspunkt i ovennævnte <u>et ledelsesmæssigt ansvar</u> at der er etableret nødvendig og tilstrækkelig datasikkerhed i virksomheden.

Datasikkerhed er en proces,

- ikke en tilstand -

Sikkerhed generelt:

Med udgangspunkt i at datasikkerhed er ledelsens ansvar, skal der formuleres en overordnet strategi og udarbejdes nogle politikker på området inden det praktiske sikkerhedsarbejde kan gennemføres effektivt.

Iforb. med politikken må man beslutte om sikkerhedstiltagene skal være RESTRICTIVE eller NON-RESTRICTIVE

RESTRICTIVE:

> *Ofte kaldt need-to-know.*
> *Adgang gives kun til de informationer og ressourcer den enkelte medarbejder har direkte behov for til udførelse af det daglige arbejde.*

NON-RESTRICTIVE:

> *Der gives forholdsvis fri adgang til systemets mange informationer og ressourcer.*
> *Begrænsninger opsættes kun til data eller ressourcer som er særlig kritiske for virksomheden eller som er underlagt lovmæssige forhold.*

I praksis vil løsningen oftest placere sig et fornuftigt sted midt imellem.

Sikkerhed må såvidt muligt ikke være til gene for medarbejderne i det daglige arbejde, men skal alligevel være så effektivt, at de nødvendige data, funktioner og maskiner, er beskyttet mod såvel egne medarbejderes fejlbetjening og mod at fremmede uretmæssigt får adgang.

Under alle omstændigheder skal sikkerhedsniveauet opfylde lovens krav.

Det er vigtigt at ledelsen informerer, helst skriftligt, til medarbejderne om med hvilken alvor man ser på sikkerhed og baggrunden for det valgte niveau.

Når teknikken tages i brug / Teknisk kontrol:

Det hele starter med købet af edb-udstyr, hvor man skal sikre sig at udstyret har den nødvendige tekniske kvalitet i forhold til hvad det skal bruges til.

Feks. skal en central server-maskine til et netværk være af betydelig højere kvalitet end PC'en som receptionen bruger til registrering af gæster, møder og fravær.

Kvalitet er noget relativt og mangel på kvalitet viser sig først langt senere - og altid på et uheldigt tidspunkt.

Som led i kontrol af kvaliteten kan der være idé i at indføre systematisk registrering af problemer og fejl på diverse udstyr i installationen for statistisk at kunne identificere typer og mærker, som giver flere problemer end andet tilsvarende.

Teknisk stabilitet og driftmæssig sikkerhed er grundlaget for enhver anden form for sikkerhed.

I det øjeblik der forekommer tekniske problemer stiger risikoen brat for, at det på en eller enden måde kan gå ud over vore data.

Folk er forvirrede, panikken breder sig og en række tiltag forsøges for at klare problemet med stigende risiko for, at data på den ene eller anden måde forvanskes, ødelægges eller helt forsvinder.

Så inden teknikken overhovedet tages i brug bør den gennemtestes og resultaterne gemmes til senere kontrol - også kontrol for, om lidt for fingernemme kolleger har 'pillet' ved udstyrets indmad, ændret set-up, skiftet kredsløbskort el. tilsv.

Når teknikken tages i brug / Teknisk kontrol:

Når udstyret kommer hjem (det handler om selve PC'en) er det rimeligt at foretage 2 slags test'er:

- **Specifikationskontrol**
- **Burn-in test**

Specifikationskontrollen skal sikre, at vi har fået det udstyr vi har bestilt !

Alt for tit ses maskiner med samme model-skilt på fronten, men med vidt forskellig indmad - den ene dobbelt så hurtig som den anden.

Årsagen skal søges i de mange slag-tilbud hos PC-forhandlerne; der er nok en grund til at PC'en er billigere end normalt !

Feks. er harddisken ofte af en langsommere type (men samme kapacitet), RAM-kredsene er lidt langsommere (gammelt lager) eller overførselskapaciteten til/fra diskette drevet er ekstremt langsomt.

Forskellige utility-programmer, som feks. Norton Utilities og PC Tools vil kunne klare disse tests.

Burn-in testen skal stress-teste udstyret og dermed afsløre, om der er løse forbindelser, svage strømforsyninger, følsomme komponenter eller andre fysiske defekter.

Chippene køres varme, disk- og diskette drev læser og skriver datablokke af variende længde og indhold. Drevene arbejder sig langsomt fra spor til spor for pludseligt at skulle springe til et yderspor og tilbage igen. Skærmen udsættes for konstante lys- og farveskift, skift af intensitet, blinkfunktioner, skrifttyper og figurer.

Når teknikken tages i brug / Teknisk kontrol:

Testprogrammerne kontrollerer alle dele af maskinen, incl. kommunikationsporte og bus'er, og aflæser de tekniske specifikationer på diverse kort- og chip-typer.

Disse aflæsninger resulterer i et certifikat for den enkelte maskine, dens teknik og stand, som lagret i en fil senere vil kunne bruges til sammenlignende kontrol af, om der er nogen der har pillet ved indmaden ?

Feks. kunne en sådan test udføres een gang om året, eller iforb. med software-installationer hvor maskinen er mere eller mindre ude af drift alligevel.

De samme test-programmer vil kunne anvendes til direkte problem- og fejlløsning hvis der opstår fejl i elektronikken.

Test-programmerne skal ikke nødvendigvis installeres på hver enkelt produktionsmaskine, men forefindes centralt i en 'værktøjskasse'.

Programmer som Check-It og QA Plus vil være velegnede til denne 'øvelse'.

Når teknikken tages i brug / Sikkerheds-disketter:

Der kan være mange årsager til at en PC pludselig ikke vil starte/boote, men typisk iforb. med forkerte ændringer i opsætningsfilerne AUTOEXEC.BAT og CONFIG.SYS.

Eneste måde at komme i forbindelse med sin harddisk er at kunne starte/boote sin PC fra en sikkerheds-diskette.

Skyldes problemet alvorligere fejl, feks på selve disken kunne det være rart med andre hjælpemidler, som også bør ligge på sikkerhedsdisketten.

Hver PC skal have sin egen sikkerhedsdiskette.

Det væsentligste er at disketten rummer DOS-styresystemet, hvilket gøre med kommandoen: FORMAT A: /S

Disketten skal yderligere indeholde simple udgaver af AUTOEXEC.-BAT og CONFIG.SYS, driver-programmer til keyboard, skærm og evt. mus, og evt. et program til udnyttelse af PC'ens interne lager (RAM).

I DOS 5.0 findes en IMAGE-kommando, som, i lighed med andre programmer, som feks Norton Utilities, sikrer en genskabelsesprocess ved at tage kopi af vigtige områder på harddisken.

Andre utility-programmer kan tage IMAGE-kopier af CMOS-data, dvs. PC'en hardwarekonfiguration, netop til brug for redning hvis den mistes.

Når teknikken tages i brug / Set-up standardisering:

Næste trin er at opsætte udstyret og konfigurere det til slut-brugeren.

Et godt sikkerhedsråd er, at standardisere sin directory-struktur, navngivning af filer mv. i videst mulig omfang.

Formålet er at forenkle, og evt. automatisere konfigureringen, lette den løbende assistance (aldrig tvivl om DIR's), lette back-up procedurerne og muliggøre en jævnlig kontrol af udstyr og indhold.

Lad programmerne ligge under de directory-navne de normalt placeres i under installationen, og opbyg nogle afdelings- eller firmastandarder for placering af data.

Opbyg samtidig nogle kontrollister du kan gå frem efter, så intet bliver glemt.

- **installation**
- **konfigurering**
- **produkttest (det nye produkt)**
- **systemtest (samspillet med øvrige produkter)**
- **tilretning af back-up procedurer**

Når teknikken tages i brug / Licens-kontrol:

Det er typisk iforb. med de ofte heftige installationer, hvor mange maskiner skal klargøres samtidig, at man glemmer licensreglerne.

Det er rent faktisk ulovligt at benytte flere programmer end man har betalt for - så enkelt er det !

Og der bliver helt sikkert ballade, når det bliver opdaget, feks. af revisoren som skal kunne sammenholde faktura'erne med det faktiske antal kørende systemer.

Når PC'erne er koblet i netværk og programmerne ligger på serveren er det noget lettere at kontrollere, at reglerne ikke overtrædes.

Feks. vil et produkt som SiteMeter blokere for yderligere programkald, når alle licenser er optaget. Først når en bruger frigiver sin brug af programmet fra serveren kan den næste gå i-gang.

Samtidig med licenskontrollen opnår man at kunne 'måle' sit licensbehov, da SiteMeter viser hvor mange der venter på hvilket tidspunkt.

Ved en lettere omprioritering af arbejdet i en afdeling vil man måske kunne spare licenser, i stedet for at indkøbe yderligere 5 eller 10 af slagsen.

Brugeren som risiko / Orden og systematik:

Det lyder banalt, men at holde orden omkring sig - og i denne sammenhæng på sin PC - mindsker risikoen for at noget går galt.

Jo mere orden og systematik, jo bedre overblik - og dermed sikkerhed - giver det den enkelte bruger.

Systematik behøver ikke at være hverken besværligt eller kedeligt, men kan være nogle fornuftige rammer indenfor hvilke man selv kan opbygge og disponere.

Det vil være rimeligt om man indenfor en enkelt afdeling, hvor alle beskæftiger sig mere eller mindre med det samme arbejde, eller hvor man i det mindste har behov for tværgående informationsgange, har organiseret sine PC'ere nogenlunde ensartet:

- **Samme udgave af styresystemet**
- **Samme grundlæggende opsætning af maskinerne i filerne: AUTOEXEC.BAT og CONFIG.SYS**
- **Samme programmer (og samme udgaver)**
- **Samme DIR-navne for samme directories**
- **Samme menu-system og menu-punkter**
- **Samme makroer i samme taste-kombinationer**
- **Samme vedligeholdelsesprocedurer omkring PC'erne**
- **osv.**

Men naturligvis skal der også være plads til individuelle programmer og directories i det omfang arbejdet kræver det.

Ekstern mærkning af disketter (udvendig håndskreven etiket) er en anden vigtig ting, så man undgår fejlagtig formatering/sletning af indholdet med data- og arbejdstab til følge.

Brugeren som risiko / Disciplin:

Det kræver desværre en del personlig disciplin at arbejde med edb, uanset om man er teknikorienteret eller om man er slut-bruger.

HVAD ER DIN PERSONLIGE MTBF ?

Sælgernes: "De skal blot trykke på knappen, fru Jensen, så ordner det hele sig selv" - den holder ikke.

Den største sikkerhedsrisiko

kommer fra os selv - brugeren !

Disciplinen går bla. på at slukke for PC'en når man går hjem, at tage sine sikerhedskopier jævnligt, at låse kopierne inde i brandsikkerkt skab, at være opmærksom på uregelmæssigheder i-forb. med brug af maskinen, og at være opmærksom på 'underlige' resultater fra systemerne.

De fleste fejl er heldigvis banale og kræver højst en smule tid at rette op på de skader fejlen har forvoldt, men visse bruger-fejl kan være årsag til omfattende konsekvenser med data-tab og store omkostninger til følge.

Som bruger burde man kræve, at blive beskyttet mod at kunne begå fejl, feks. at kunne slette eller ændre data, under systemer hvor man normalt intet har at gøre.

Så længe man har mulighederne og rettighederne har man også ansvaret, et ansvar som ofte vil være urimeligt at skulle bære, da det næppe er understøttet af den fornødne tekniske uddannelse.

Der findes feks. en lang række sikkerhedsprogrammer, som kan begrænse enhver brugers adgang til programmer og data, hvor den pågældende normalt intet har at gøre.

Brugen af programmerne giver sikkerhed for fremmedes indtrængen i virksomhedernes systemer, og beskytter samtidig medarbejderne mod fejl opstået ved uheld.

Brugeren som risiko / Datafejl i Registre:

Få ting er så vanskeligt som at holde styr på et omfattende kunderegister med firmanavn, personnavne og adresser.

Fejl i disse oplysninger fører dels til ekstra tryksags- og porto-omkostninger ved udsendelse af brochurer og salgsbreve, og dels til irritation hos modtageren, som ikke får stavet sit navn korrekt, ikke har den anførte titel, eller ikke har det produkt som sælgeren refererer til i sit salgsbrev.

Direct Mailing og lignende former for markedsføring er stærkt opreklameret for tiden med udgangspunkt i firmaets edb-kartotek men der er grund til at advare, også selvom man køber oplysninger fra et adressebureau. Heller ikke de kan følge med i alt.

Navne: Er det den samme person / firma ?

Hr. H Hansen	?	Hr. H. Hansen
Hr. Hans Hansen	?	Hr. H. P. Hansen
De forenede A/S	?	A/S De forenede

Arbejder Hr. Hansen overhovedet der mere ?

Titler: Er der forskel på at være leder eller chef ?

Nogen bliver fornærmede hvis man benytter forkert titel, nu hvor de har arbejdet sig op i systemet og fået status !

Adr. : Bor firmaet stadig på adressen, har de filialer, hvor arbejder att.personen, osv.

United Bluffs		United Bluffs
Skolegade 14	?	Lærestræde 41
Att. Jensen	?	Att. Jensen

Tekst : Har kunden den maskine eller .... ?

Under henvisning til Deres maskine af mærket:
SuperDuper XL-12 kan vi tilbyde Dem .....

Det understregede er naturligvis udfyldt automatisk fra kunderegistret under udskrift ! Men er det rigtigt ?

Hvordan vil du selv reagere på et brev med forkerte oplysninger og påstande ?

Brugeren som risiko / Datafejl i Registre:

Netop fordi det er svært at holde styr på alfabetiske data tildeler vi hinanden numre, feks. kundenumre, kontonumre og personnumre - på samme måde som vi bruger varenumre, reservedelsnumre o.lign.

Selvfølgelig kan der også ske fejl under indtastning og registrering af numeriske data; feks. kan man komme til at byte om på 2 cifre eller at læse et 3-tal for et 8-tal (eller omvendt).
Der er altså massevis af muligheder.

Statistisk kan det bevises, hvilke tal der oftest læses forkert eller ombyttes på grund af den måde tallene er placeret på tastaturene.

For at undgå at månedslønnen sættes ind på den forkerte konto er alle kontonumre sikret ved hjælp af en modulus-kontrol, på præcis samme måde som vore CPR-numre er sikret.

I begge tilfælde er det sidste ciffer et KONTROL-CIFFER som ikke indgår i selve nummeret, men som beregnes og sammenlignes i alle edb-processor, hvor det er nødvendigt for at sikre data-integriteten.

CPR-numrene er sikret med en såkaldt modulus-11 kontrol.

Brugeren som risiko / Datafejl i Registre:

Eksempel:

P. Nummermann - født d. 17. Marts 1943

CPR-nr.: 170343-1bnK feks. 170343-047K

hvor lbn er et fortløbende løbenummer tildelt alle som blev født på denne dato, og hvor K er det beregnede kontrolciffer.

Modulus-11 kontrollen beregnes med vægtene 432765432 således:

CPR-nr	**170343-047_**
Vægte	**432765-432**

De enkelte cifre i CPR-nummeret multipliceres med tilhørende vægt(tal) og alle resultaterne lægges sammen.

1x7=7 + 7x3=21 + 0x2=0 + 3x7=21 + 4x6=24 + 3x5=15 +
0x4=0 + 4x3=12 + 7x2=14 alt-i-alt er summen: 114.

Tallet 114 divideres med 11, hvilket giver 10 med 4 i rest.

Resten 4 trækkes nu fra modulus-tallet 11 - og vupti -

KONTROLCIFFERET = 7

CPR-nr 170343-0477

Hvis man taster forkert - og bytter om på 3 og 4 giver det et helt andet kontrolciffer:

CPR-nr 170433-0475

Og på grund af at det tidligere beregnede kontrolciffer (det korrekte) ikke stemmer med det aktuelt beregnede (på grund af en fumlefejl) vil edb-programmet afvise den påbegyndte transaktion.

Brugeren som risiko / Datafejl i Registre:

Det var i denne beregning helt tilfældigt, at kontrolcifferet blev et ulige tal, som 'beviser' at P. Nummermann er en mand !

I virkelighedens verden skyldes fordelingen af CPR-numre til mænd og kvinder/drenge og piger, at de uddeles MANUELT ud fra en edb-genereret liste, som krydses af !

Da der normalt fødes mere end eet barn i døgnet i Danmark, og sjældent kender deres køn før i sidste øjeblik, må man nødvendigvis være klar med et antal CPR-numre, som kan tildeles den nyfødte.

Brugeren som risiko / Datafejl i Registre:

Eksempel:

Med P. Nummermann's fødselsdato som udgangspunkt kan vi 'generere' et antal CPR-numre til almindelig uddeling:

CPR-nr 170343-046_

CPR-nr 170343-0477

CPR-nr 170343-048_
CPR-nr 170343-049_
CPR-nr 170343-050_
CPR-nr 170343-051_
CPR-nr 170343-052_
CPR-nr 170343-053_
CPR-nr 170343-054_
CPR-nr 170343-055_
CPR-nr 170343-056_

Beregnet på samme måde som P. Nummermann's kontrol-ciffer kommer man frem til følgende CPR-numre:

CPR-nr 170343-0469 Ulige - det tildeles en **MAND**

CPR-nr 170343-0477 - - P. Nummermann - MAND !

CPR-nr 170343-0485 - - - -
CPR-nr 170343-0493 - - - -
CPR-nr 170343-0507 - - - -
CPR-nr 170343-0515 - - - -
CPR-nr 170343-0523 - - - -
CPR-nr 170343-0531 - - - -
CPR-nr 170343-054. rest 10 - udgår
CPR-nr 170343-0558 Lige - det tildeles en **KVINDE**
CPR-nr 170343-0566 - - - -

Brugeren som risiko / Datafejl i Regneark:

Ingen tvivl om at regneark er smart, praktisk og effektivt hvis altså regnereglerne er korrekte !

Ikke så få virksomheder har været ude i økonomiske problemer, fordi man stolede blindt på bundlinie-tallene i chefens eget regneark, som desværre regnede forkert.

Dvs. ... regnearket regnede rigtigt nok - men de bagved liggende regneregler var ikke korrekte. Måske var der blot en enkelt smutter med en kommafejl, en forkert momssats, forkert procent-udregning el. tilsv. !

Som bruger kan det være vanskeligt at opbygge og overskue, især hvis arket fylder mere end et enkelt skærmbillede, så det er nødvendigt at rulle billedet i alle retninger. Lettere bliver det vel næppe hvis det deles op i mange vinduer som mere eller mindre overlægger hinanden på skærmen !

At opbygge regneark kan sammenlignes med programmering, og de færreste som arbejder med regneark kan programmere !

De fleste regneark handler om firmaets økonomi, budgetter, likviditet, regnskaber mv., men flertallet af de som arbejder med disse regneark er regnskabsuddannede !

Det engelske revisionsfirma Coopers & Lybrand har i en engelsk undersøgelse konstaterer, at 21 ud af 23 kontrollerede regneark indeholdt fejl, som var væsentligt afgørende for resultatet !

De bedste råd til at opbygge korrekte regneark er:

- *Hold regnearket i en fornuftig størrelse*
- *Opbyg det evt. i flere dimensioner*
- *Lad det sammentælle kolonner og rækker som krydskontrol*
- *Lad evt. optællingen foregå som mellemresultater*
- *Er regnearket statisk kan man benytte nonsens-kontroller*
- *Lad ikke andre ændre i regnereglerne/lås indholdet*
- *Lad andre teste og kontrollere regnearket (på regnemaskine)*
- *Brug også god gammeldags overslagsregning*

Bemærk de mange udråbstegn ! - Regneark kan være farlige !

... men også aldeles gode og effektive.

Brugeren som risiko / Forkert fil slettet:

Det er let at 'komme til' at slette en fil, feks. et vigtigt dokument i tekstbehandlingssystemet, ved en fejltagelse.
Det går stærkt og man 'troede' at markøren/bjælken stod over et andet fil-navn !

Har man skrevet dokumentet umiddelbart før den uheldige sletning, er der sjældent andet at gøre end at begynde forfra !

Er dokumentet en ældre sag skulle der være en chance for at genfinde det på en tidligere sikkerhedskopi/back-up, så der kun mistes tid, men ikke den eksakte formulering af skrivelsen.

Se senere om sikkerhedskopier, hvordan man tager disse og hvordan man kan fremfinde sin gamle dokumenter igen.

Visse programprodukter leverer automatisk sikkerhedskopi, af det dokument eller regneark man netop arbejder med.

Dvs. at i det øjeblik man indlæser (eller lagrer) et dokument eller regneark fra disken tager programmet automatisk en kopi og giver den tilnavnet .BAK (backup) .BSW (backup worksheet) el.-lign.; så hvis det går galt under redigeringen af originalen kan man på få sekunder indlæse kopien i stedet og må altså kun genskabe netop udført arbejde.

Problemet med denne form for sikkerhedskopiering er, at den kun gælder til man igen indlæser (eller lagrer) samme fil:

Indlæs -> Sikkerhedskopi -> Rediger orig ->
Gem/Lagre -> Ud af systemet -> Ind igen senere ->
Indlæs -> **Sikkerhedskopi** -> Rediger orig -> osv.

Vi ser, at der igen tages en sikkerhedskopi, hvorved den tidligere er blevet overskrevet.

Dvs.: Denne form for sikkerhedskopiering er udelukkende til sikring mod 'fumlefejl', hvor man ved fejl-tryk eller misforståelse får slettet det man lige har opbygget.

Brugeren som risiko / Forkert fil slettet:

Det kan (næsten !) altid betale sig at gemme/lagre/save sine filer jævnligt, mens man arbejder med dem, feks. hvert kvarter eller når man har afsluttet et særligt kompliceret tekststykke eller avancerede regnearksformler.

Murphy's Computerlove siger feks.

En computer går kun ned, hvis det er længe siden, du sidst har gemt din tekst.

Det kan anbefales at man ved større skrive/regneopgaver selv opretter en sikkerhedskopi, dvs. gemmer teksten under 2 filnavne hver gang man har foretaget et vist omfang af ændringer, feks.

VIGTDOK1.DOK <=> VIGTDOK2.DOK

Det sikrer samtidig at man ikke mister hele sin fil, hvis der skulle opstå en sporadisk fejl på disketten eller disken. Med stor sandsynlighed vil man i stedet kunne læse det andet eksemplar af filen.

Regnearket SuperCalc har feks. 2 former for gemme-kommandoer; den ene gemmer uden at tage sikkerhedskopi, den anden gemmer med sikkerhedskopi, dvs. at forskellen mellem de 2 filer svarer til omfanget af arbejde siden seneste gem-kommando.

Årsagen til: (næsten !) i første linie skyldes, at man alligevel ikke altid er 100% sikret med back-up'er.

En bestemt udgave af WordPerfect kan feks. ikke altid holde styr på redigering og især flytning af tekstblokke indenfor meget store dokumenter (feks. 150 sider). Uden at give nogen form for advarsler gemmes filen på disken - men .. når den igen skal indlæses nægter WordPerfect pure med den lakoniske bemærkning: Filen kan ikke indlæses !

Her hjælper jævnlig brug af gem-kommandoer ikke meget, og ej heller brug af ekstra filer; i værste fald kan flere dages produktion gå tabt - og man må tilbage til seneste store back-up.

Brugeren som risiko / Forkert fil slettet.

Eksempel....

Torsdag:	Total back-up
Fredag :	Teksteredigering - alt ok
Mandag :	Teksteredigering - alt ok
Tirsdag:	Teksteredigering - alt ok
Onsdag :	Teksteredigering - alt ok
Torsdag:	Filen kan ikke indlæses !

Al produktion - fra fredag til torsdag incl. er mistet.
Back-up fra torsdag skal RESTOREs og arbejdet gen-skabes derfra.

Har man benyttet sine applikationsprogrammer til at slette data-filer er der ikke altid de store muligheder for at genskabe data uden at skulle tilbage til seneste sikkerhedskopi.

Anderledes forholder det sig, hvis man har brugt DOS-kommandoen: **DELETE** .

Fortryder man sletningen inden man har overskrevet arealet med nyere data vil filen kunne gen-skabes med en UNDELETE-kommando.

Grunden til at det kan lykkes er, at diskettens data ikke fysisk er blevet slettet/overskrevet, kun i indholdsfortegnelsen er filen blevet slettet.

Da DOS 5.0 gemmer oplysninger fra indholdsfortegnelsen netop for filer slettet med DELETE med henvisninger præcis til de steder på disketten, hvor data stadig ligger fysisk - kan filen 'gen-skabes' ved at gen-oprette den i indholdsfortegnelsen.

Det giver så omvendt en sikkerhedsrisiko, hvis man låner eller forærer disketter væk, som er slettet på denne måde - andre vil kunne genskabe indholdet, så længe mediet ikke er overskrevet med alt for mange nye filer

- så pas på hvad du gør ! -

Det er jo ikke kun dine, men også i høj grad firmaets, oplysninger du måske kommer til at udlevere.

Brugeren som risiko / Forkert formatering.

Naturligvis kan man komme til at formatere en diskette, som indeholdt vigtige filer - men det er yderst uheldigt, da der næppe findes back-up af den.

DOS-systemet giver dog en mild advarsel inden den påbegynder formateringen, så man har en chance.

Noget tilsvarende kunne ske med harddisken, men sker det vil det være efter at 'kommandøren' har forceret en kraftig advarsel fra DOS-systemet om, hvad der var i vente.

WARNING. ALL DATA ON NON-REMOVEABLE DISK
DRIVE C: WILL BE LOST !
Proceed with Format (Y/N)?_

Har man svaret Y (YES) til dette vil der normalt ikke være nogen chancer for at genskabe informationerne; kun hvis man benytter DOS 5.0 eller har investeret i lidt ekstra programmel, feks. NORTON Utilities, har man en fair chance.

Disse benytter specielle formateringskommandoer, som indleder med at tage en kopi af diskettens indholdsfortegnelse med angivelse af på hvilke sporadresser de enkelte filer befinder sig på disketten - gemmer oplysningerne i komprimeret form på disketten - og foretager først herefter formateringen.

Fortryder man inden man er begyndt at lagre nye filer på mediet kan man udføre en UNFORMAT, som 100% genskaber det oprindelige indhold.

Er man begyndt at skrive på disketten eller disken vil de nye data i princippet lægge sig oven i hvor de tidligere data lå, og så vil gamle data fra netop dette område ikke kunne genskabes.

100% genskabte filer findes under det oprindelige navn, mens delvis genskabte filer samles under systemvalgte navne eller gives et særligt prefix.

Sikkerhedsmæssigt betyder det, at disketter som man tror er slettet med FORMAT-kommandoen faktisk er lette at gen-skabe, hvorved de kan udgøre en sikkerhedsrisiko.

- så pas på hvad du gør ! -

Det skal naturligvis også nævnes at der findes sikre metoder til formatering af disketter, så den almindelige bruger ikke kan genskabe tidligere indhold, feks. NORTON WIPE-funktion.

Brugeren som risiko / Sikkerhedskopiering:

Som det er nævnt et par gange, er det yderst vigtigt at tage sikkerhedskopier af sine data, tabeller og lignende.

Det kræver en vis **selv-disciplin** at overholde dette, da det altid er nemmest at springe over, hvor sikkerheden er lavest.

Først når dagen kommer, hvor et eller andet går galt, opdager man, hvor vigtigt det er at have sikkerhedskopier af sine data.

Hvor ofte skal man tage sikkerhedskopier ?

Så ofte som muligt !

Så ofte som muligt under behørig hensyntagen til data's værdi for arbejdet/virksomheden og ikke mindst til de konsekvenser det vil få, hvis data mistes af den ene eller anden grund.

Der kan også tages hensyn til i hvilket omfang det er muligt at genskabe data feks. ud fra noget bilagsmateriale eller andet, eller om det er komplet umuligt, fordi dataændringer er sket direkte og på grundlag af telefonsamtaler.

Hvis man arbejder med data, som sjældent ændres, er en ugentlig backup nok, men samtidig må det nok betragtes som absolut minimum - man vil ellers erfare, at man ændrer væsentlig flere data dagligt end man umiddelbart tror.

Arbejdes der derimod med data, som ændres fra dag til dag, bør der foretages mindst en daglig backup. Derved vil, i allerværste fald, kun een dags arbejde gå tabt. Men det kan da også være slemt nok !

Selv om der foretages daglig backup af de hyppigst anvendte data, bør man også tage en ugentlig backup af samtlige data, som derefter gemmes bort i brandsikre skabe eller i kælderen længst muligt væk fra originaludgaven.

Brugeren som risiko / Sikkerhedskopiering:

Der findes programmer som automatisk tager back-up, feks for hver 30 minutter eller hvad man nu vælger, enten som indbygget funktion i et større programkompleks eller som hjælpeprogram.

Back-up'en tages enten på samme medie (typisk harddisken) eller dirigeres til en separat diskette, som skal være permanent isat under arbejdet med PC'en. En udemærket ide, hvis man ikke benytter diskettedrevet alt for ofte.

De egentlige back-up rutiner bør køre efter et af følgende mønstre, og her forudsættes at sikkerhedskopierne skrives ud på disketter.

- **Fast ugentlig back-up dag: TORSDAG**
- **Fredagen kan bruges som sidste mulighed, hvis torsdag glipper.**
- **Ingen reel undskyldning for ikke at tage sikkerhedskopi.**
- **Sikkerhedskopien skal væk fra kontoret og helst fra huset.**
- **Sikkerhedskopier skal arbejde i cylclus'er.**

A. Total Back-up / Ugentlig

Datamængden er ikke større end at det kan betale sig, tidsmæssigt, at tage total back-up hver gang. Back-up'en fylder max. 10 disketter svarende til max. 1/2 times sikkerhedskopiering.

Samme back-up frekvens hvis der normalt ikke sker de store data-ændringer i løbet af arbejdsugen.

Uge-disketterne skal arbejde i cyclus på min. 3 sæt og gerne 5.

B. Daglig del back-up + Total back-up / ugentlig

Hvis der forekommer meget store data-ændringer henover den enkelte arbejdsdag, bør man tage daglig back-up, men kun af de filer, som er blevet berørt af ændringerne.
På engelsk/amerikansk kaldes det: Incremental Back-up

Daglig back-up fylder 1-3 disketter, som skal arbejde i cyclus på 5, dvs. et sæt pr. ugedag.

Uge-disketterne skal arbejde i cyclus på min. 3 sæt og gerne 5.

C. Ugentlig del back-up + Total back-up / månedlig

Samme model som B, men bruges ved færre dataændringer.

Brugeren som risiko / Sikkerhedskopiering:

Det er trygt og godt at vide at der er taget back-up, og at disketterne er anbragt forsvarligt i boks el.lign. ...

.... indtil det viser sig at man ikke kan læse dem igen, eller at man alligevel ikke har fået taget back-up af alt, fordi man har fået et nyt program og glemt at tilrette back-up proceduren!

Stikprøvevis bør man forsøge at lægge data tilbage igen, det der hedder en RESTORE, eller at RESTORE (nu dansk !).

Afslutningsvis skal det nævnes, at til back-up af meget store diske (rummelighed > 100 mb) bør man anskaffe en TAPE-STREAMER, og bruge denne i stedet for disketter.

Der medfølger specialsoftware, med varierende funktioner, til den enkelte type og fabrikat tape-streamer.

Men husk: Back-up principperne er præcis de samme !

Murphy's Computerlove siger feks.

1. **Til en back-up kræves altid én diskette mere end du har.**
2. **Et back-up program svigter præcis på det tidspunkt, hvor du har brug for det.**

Første afledning:
Når back-up programmet svigter, vil det overskrive den eneste eksisterende sikkerhedskopi.

Anden afledning:
Når du vil genetablere et program ved hjælp af sikkerhedskopien, finder du ud af, at den eneste version af RESTORE var på den disk, som du lige har formateret.

Brugeren som risiko / Sikkerhedskopiering:

Til brug for back-up arbejdet kan man vælge mellem følgende DOS kommandoer:

COPY, DISKCOPY, XCOPY og BACKUP,

samt kommandoen

RESTORE,

som tilbagekopierer filer, som er kopieret ud med BACKUP-kommandoen.

COPY-kommandoen kopierer, efter ønske, på kryds og tværs mellem medierne.
Kopierede data kan umiddelbart kopieres tilbage igen med samme kommando.

DISKCOPY kopierer alt fra en diskette over på en anden diskette formateret på samme måde som den første, incl. evt. free-space. DISKCOPY benyttes kun når man ønsker at sikkerhedskopiere data mellem disketter.
Kopierede data kan umiddelbart kopieres tilbage igen med COPY-kommandoen.

XCOPY kopierer alt fra en diskette over på en anden diskette, men pakker det effektivt og udelader free-space. XCOPY kan benyttes til sikkerhedskopiering mellem disketter af forskellige formater og/eller til kopiering mellem harddisk og disketter.
Kopierede data kan umiddelbart kopieres tilbage igen med COPY- eller XCOPY-kommandoen.

BACKUP kommandoen siger sig selv, nemlig at sikkerhedskopiere. BACKUP benyttes når man sikkerhedskopierer fra harddisk, men den kan ligeså godt benyttes til sikkerhedskopiering fra disketter.
Kopierede data kan ikke umiddelbart kopieres tilbage med COPY; man skal i stedet benytte **RESTORE-kommandoen.**

Alternativt kan man benytte en lang række specialprodukter, som gør tingene lidt anderledes - og ofte lidt mere !

Brugeren som risiko / Sikkerheds-opbevaring:

Et er at tage sikkerheds-kopier/backup, noget andet er at opbevare denne kopi af virksomhedens mest følsomme data et fornuftigt sted.

Sikringen skal reelt opfylde 2 formål:

- **tyveri-sikring**

- **brand-sikring**

og det er desværre ikke altid at disse områder er samfaldende i de lokaler, bokse, skabe og kasser man opbevarer sine datamedier i.

Tyverisikringen bør bestå af indelukker med dirkefri låse, SKA-FOR-godkendte, og med behørig sikring mod ved simple ødelæggelse, at nogen kan få adgang til datamedierne.

Bortset fra den evt. følsomhed i forsvundne data, vil arbejdspladsen fortsat kunne operere da data i øvrigt vil være intakte på de enkelte maskiner.

Brandsikringen skal sikre mod ødelæggelse af data i en situation, hvor data i øvrigt er ødelagt på de enkelte maskiner pga. brand, sammenstyrtning eller vandskader.

Data bør opbevares i bokse specielt godkendt til formålet, hvilket vil sige at det skal have gennemgået feks. en Braunschweig-test, hvor boks-skabet har været udsat for brand i et antal timer, været tabt fra 3.sals højde, brændt igen og derefter stillet til afkøling.

Data-medierne skal naturligvis være intakte og kunne læses efter denne behandling.

Den kritiske temperatur for magnetmedier ligger omkring 60 C^{o}.

Klassificeringen for netop Dataskabe hedder henholdsvis:

S 60DIS & S120DIS

hvor tallet refererer til det antal minutter skabet kan tåle at være udsat for direkte ild- og varmepåvirkning uden at det går ud over datamedierne inde i skabet.

Brugeren som risiko / Datatransport og -udveksling:

Der udveksles dagligt hundredevis af datamedier mellem virksomhederne, feks. lønindberetninger til pengeinstitutterne, betalingstilladelser til PBS, indbetalinger til ATP og til Told & Skat, indberetninger til Danmarks Statistik, køb og salg til Værdipapircentralen, pensions- og børnepengeoverførsler fra det offentlige og meget meget andet.

På magnetbånd, disketter og cassetter af enhver art og oprindelse.

Hvordan ?

Med posten i mere eller mindre almindelige kuverter, med taxa og andre bil-transporter emballeret i brunt indpakningspapir, med cykelbude og hvad der ellers måtte være til rådighed af transportformer.

Yderst følsomme data med konto-numre, navne, CPR-numre, store beløb osv. flyder 'uhæmmet' rundt i vore gader - uden nogen form for effektiv beskyttelse mod fysiske skader, mod tyveri og mod evt. kopiering !

Det mindste man kan gøre for sine egne data-medier (og værdier) er at emballere dem forsvarligt i en æske/box/kasse og lukke den med en eller anden form for segl eller plumbering.

Er seglet brudt ved man at data-integriteten er brudt - og man kan tage sine forholdsregler. Hvis man ikke ved det, og det alligevel er sket, har man ikke en chance for at forebygge eventuelle konsekvenser.

Er data-mediet overhovedet nået frem til modtageren ? Eller kører det sigth-seeing med en taxa som var heldig med en tur 'fra gaden' ?

Hvorfor ikke informere modtageren, feks. pr. fax, at nu afsendes båndet med taxe (Navn & nummer) og forventes at være fremme om ca. x minutter ?

Og hvorfor ikke bede modtageren kvittere for modtagelse med en følgeseddel eller en contra-fax ?

Er vores data i virkeligheden så ligegyldige - eller er det os selv der er det ?

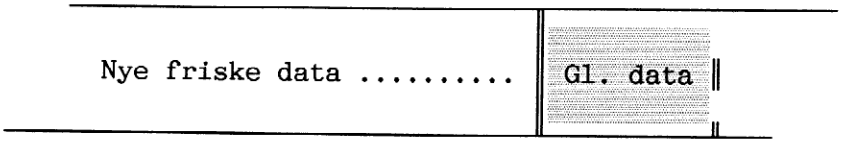
Brugeren som risiko / Datatransport og -udveksling:

Ligger de følsomme informationer i klar-tekst på mediet, så nogle der vil det onde kan kopiere dem - og sende dem videre - uden at vi ved at data er kopieret ?

Er data-indholdet tilpas følsomt vil det være rimeligt at fremsende dem i crypteret form, dvs. scramblet eller 'forvirret' på en måde som kun den rigtige modtager kan de-cryptere - og læse.

Normalt returneres medierne til afsenderen efter brug, og indgår almindeligvis i en fast cyclus.

Når mediet sendes næste gang er det ikke sikkert at de nyeste data fylder, og derved overskriver, mere end hvad der var på mediet fra sidste gang.



Dvs. at man reelt kan gen-læse de overskydende informationer, UNFORMAT'e dem med DOS, gen-skabe dem med andre værktøjer og i værste fald få dem indlæst 'dobbelt'.

Forsendelse- og udvekslingsmedier bør, for alle eventualiteters skyld, være slettet grundigt inden de gen-indspilles.

Grundig sletning kan feks. gøre med DOS'en FORMAT /U -kommando, som sletter fuldstændigt, så en UNFORMAT-kommando ikke giver resultater.

En anden metode hedder de-gaussing - afmagnetisering - som foregår med en meget kraftig elektromagnet. De-gauss maskiner findes i flere udgaver med tilpasnings-kit til stort set enhver medietype.

Og iøvrigt bør man kun bruge helt fejlfri medier til udveksling. Dårlige medier kan være årsag til fejl-læsning, om-levering og drift-forsinkelser hos modtageren - som arbejder videre med

VORES DATA !

Når mange har adgang / Fysisk sikring af PC'en:

Tyveri af en PC er en alvorlig sag - måske ikke så meget pga. PC'ens værdi som pga. af de følgevirkninger det ofte vil have for både arbejdet og ikke mindst pga. de mistede data, specielt hvis 'hele firmaet' ligger på maskinens harddisk.

Vi formoder her, at alle nødvendige tiltag til sikring af lokaler mv. mod ulovlig indtrængen er taget, men alligevel kan både indbrud og tyveri ske.

Altså må PC'en sikres særskilt.

Der findes både fysiske og logiske låsemekanismer.

Fysisk kan PC'en (centralenheden) låses fast til bordpladen (forudsætter naturligvis en bordmodel) med forskellige låsesystemer, som kræver mere eller mindre permanent installation.

Det kniber mere med sikring af gulvmodellerne. Til gengæld kan man så sige at de er både tungere og mere besværlige at fjerne i en fart !

I teorien kunne maskinerne (centralenhederne) låses inde i et sikret skab eller aflåseligt lokale, men både betjening, ventilation og kabellængder taler indtil videre mod dette.

Så længe PC'en er PERSONLIG må vi acceptere dens nærhed.

Bedste bud på fysisk sikring mod tyveri og hærværk er, at sikre lokalerne bedst muligt med låse, adgangssystemer, tyverialarmer og hvad der ellers hører til.

Fysisk sikring mod brug af maskinen, hvor den nu står, består først og fremmest af maskinens egen lås, som dog ikke er mere avanceret end, at det nok skulle være muligt at finde en nøgle som passer til.

Til daglig forhindrer den dog at 'tilfældige' kolleger, eller gæster, kan starte din maskine, og måske komme til at slette noget eller se noget, de ikke skulle have set.

Evt. kan power-switchen sikres med forskellige former for låsemekanismer.

Der findes forskellige former for låse-sikring af diskettedrevet, således at det ikke uønsket kan benyttes til at kopiere data ud fra harddisken.

Når mange har adgang / Fysisk diskette-beskyttelse:

Disketter er et yderst fleksibelt medie, som derfor bruges til hurtige dataudvekslinger mellem mange mennesker og PC'ere.

Disketten er billig (5 - 25 kr/stk), så det er ikke noget man passer specielt godt på. De ligger mere eller mindre og flyder på borde, i skuffer, i vindueskarme eller andre uautoriserede steder.

Og det burde absolut ikke være tilfældet.

For i virkeligheden drejer det sig jo slet ikke om selve mediet, men om de data mediet aktuelt indeholder og konsekvensen af at miste disse !

Medierne er præcisionsmedier og kan som sådan ikke tåle enhver form for behandling (=mishandling) - derfor:

- **Opbevar disketter i lukkede plastbokse**
- **Læg dem aldrig hvor der er støvet**
- **Pas på med tobak og aske**
- **Rør aldrig ved magnetbelægningen**
- **Læg dem aldrig i vindueskarme**
- **Pas på fugt, kulde og varme**
- **Må ikke bøjes eller trykkes**

En klassiker i diskette-ødelæggelse er, at skrive disketteidentifikation med kuglepen på en etiket, som allerede er klistret på disketten ! Der skal ikke meget til før der trykkes for hårdt og magnetbelægningen er skadet.

Skriv etiketten men den ligger på bordet - og sæt den så på !

5 1/4"-disketter:

Er sårbare overfor bøjning og trykning i det bløde etui.

Er sårbare mod fedtfingre på magnetbelægningen i området hvor læse/skrivehovedet skal kunne arbejde.

3 1/2"-disketterne

Er noget mere stabile i kraft af det mindre og stivere etui.

Til gengæld skal man passe på ikke at beskadige lukkepladen; den skal kunne skubbes til side let og frit.

Når mange har adgang / Fysisk disk-beskyttelse:

I PC'er med indbygget harddisk er der en risiko for, at læse/-skrive-hovederne, eller disken, kan blive ødelagt, hvis maskinen bliver udsat for et kraftigt stød.

Normalt rører læse/skrivehovederne ikke diskoverfladen, men ved stød kan de risikere at ramme den roterende disk med alvorlige fysiske skader til følge.

For at hindre ødelæggelse har de fleste maskiner en kommando som sørger for, at læse/skrivehovederne bliver trukket tilbage fra de magnetiske plader i en parkeringsposition, hvor de fastlåses til maskinen tændes næste gang.

Kommandoerne kan variere lidt blandt leverandørerne, men for alle gælder at det er en kommando man skriver som det sidste, inden der slukkes før strømmen.

Eksempler....

```
C:\>SHIP

Please turn off power now. Read/Write head moved.


C:\>PARK

Please turn off power now. Read/Write head parked.


C:\>DISKPARK

DISKPARK - HARDDISK HEAD PARK PROGRAM VER 1.7
COPYRIGHT ONTRACK COMPUTER SYSTEMS 1988

This program will move the heads on your SEAGATE
ST213, ST225, ST238R.. disks to their landing zone
This process is recommended prior to ANY physical
relocation of the computer or removal of the hard disk
drives for any reason.

You should TURN OFF the computer after running this
program.

Do you wish to proceed? (y/n): y

DISK HEADS ARE NOW PARKED
YOU SHOULD NOW TURN THE POWER OFF
```

Når mange har adgang / Fysisk disk-beskyttelse

Hvis man periodisk flytter sin ellers stationære PC'er fra et sted til et andet, er det naturligvis en god ide at sikre sig, at intet kommer til skade under transporten, og flyttes den ofte er det en god ide at gemme originalemballagen og anvende den som beskyttelse.

De bærbare PC-typer er konstrueret anderledes, men alligevel skal man passe godt på dem og primært undgå kraftige slag og stød, men vær også opmærksom på meget høje/meget lave temperaturer og kraftige temperatursvingninger.

Bær-bar eller ej;
kommer maskinen fra stærk kulde ind i varmen skal den aklimatiseres før den startes for at undgå kondensdannelser på disk-fladerne.

Når mange har adgang / Logisk sikring af PC'en:

Der findes forskellige program-produkter til logisk sikring af adgang til PC'en.

Dvs. at selvom man rent fysisk kan tænde den og at styresystemet indlæses, er det umuligt at komme længere hvis man ikke kender et bestemt adgangsord/password.

DOS-systemet i sig selv yder ingen eller kun ringe beskyttelse, hvorfor man må investere i supplerende sikkerhedsprogrammel fra uafhængige leverandører.

Et system som feks. Lock-It arbejder med skjulte filer og præsenterer et flot adgangsbillede, som kræver: Password.

Det betyder også at man ikke kan benytte DOS-kommandoer, og derved kopiere data ud af maskinen.

Med et produkt som AllSafe, kan man feks. begrænse adgangen til bestemte filer og/eller til, at der skrives i dem både via DOS-kommandoer og fra andre programmer, ligesom man kan forhindre utilsigtet formatering af disketter og/eller disk.

AllSafe kan yderligere kryptere/kode data, så de kun kan læses efter en de-kryptering/de-kodning med brug af et kode-ord.

Når mange har adgang / Passwords og PIN-koder:

Password, nøgle eller kode, dækker den hemmelige adgangskode som skal indtastes for at få adgang til et program eller nogle bestemte data.

Password er personlige og skal ændres, hvis de af en eller anden legal årsag har været udleveret til en der normalt ikke skal have denne adgang.

Password kan være svære at huske, specielt for de som anvender mange edb-systemer, så derfor bruger man typisk sine fødselsdata, bilens nummer, hundens navn, børnenes navne eller tilsvarende let gættelige koder !

For at være effektivt bør password'et være på mindst 5-6 tegn og helst flere, og samtidig helst en blanding af bogstaver, tal og tegn, hvis det sidste er muligt (tilladt af password-systemet).

Eksempler:....

HAN44SEN SE6ERGÅT FM90,2MH

Hvis man ikke kan huske det så.... kan man jo notere det på en seddel i skuffen, en etiket på skrivebordslampen el.lign !!!!

De fleste adgangssikringssystemer kan sættes op til at kontrollere brugen af passwords.

Feks. skal password'et være på min. 6 karakterer.

Feks. skal password'et ændres efter 35 dage eller efter 75 ganges brug.

Feks. må det samme password ikke genbruges før efter min. 3 perioder.

Feks. må password'et ikke indeholde samfaldende tegne med det tidligere password; man kan ikke udskifte OLE122 med OLE894.

... samt et par andre muligheder for at undgå sammenfald med tidligere anvendte password.

Når mange har adgang / Passwords og PIN-koder:

Det bliver ikke lettere når man samtidig skal holde styr på et antal PIN-koder (Personligt Identifikations Nummer) på sit DAN-KORT, DINERS, STATOIL, JETBENZIN og FRIDA-kort, eller hvad de nu hedder, plus adgangskortet til arbejdspladsen.

4 cifre - det er da til at huske, men hvilke 4 cifre, og i hvilken rækkefølge, og til hvilket kort ?

Hvis man ikke kan huske det så.... kan man jo notere det på en seddel som ligger i tegnebogen sammen med kortene !!!!

Når mange har adgang / Passwords og PIN-koder:

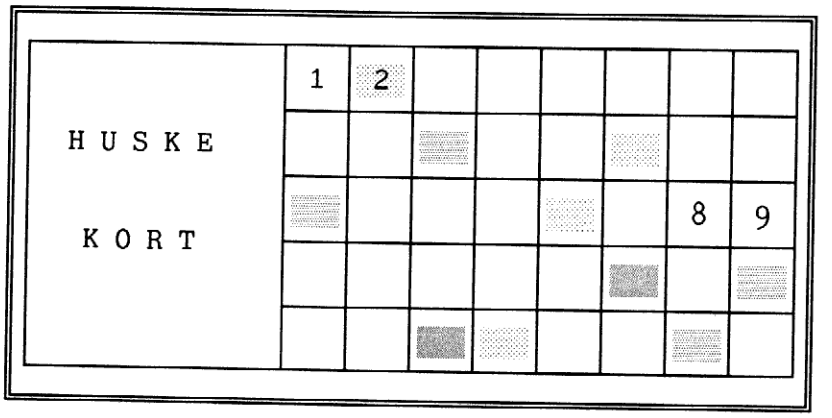
Der er dog hjælp på vej med en lige så effektiv som sikker løsning på PIN-kodens forglemmelse:

ET HUSKEKORT (uden PIN-kode)

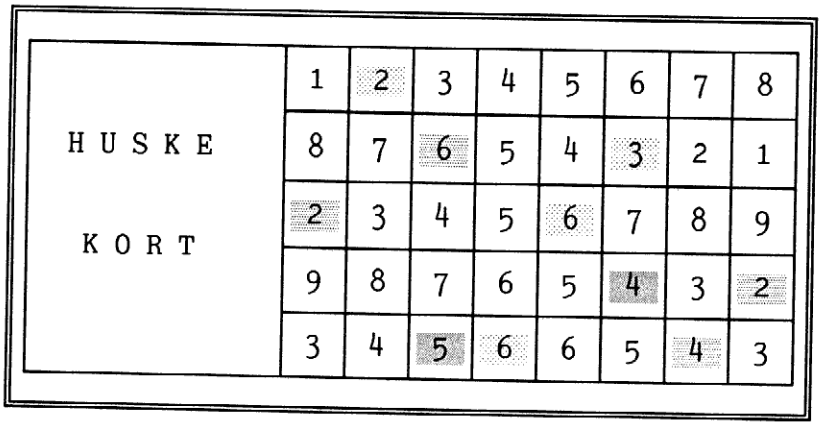
Det er udviklet af PBS (Pengeinstitutternes Betalings Service) og består i alt sin enkelhed af et kort med kvadratiske felter i forskellige farver.

På kortet kan man placere talkoden i en visuel kombination, som vore hjerner beviseligt er bedre til at huske.

Først udfyldes det med PIN-koden ....



..... som derefter camoufleres med andre tal



Enkelt, simpelt og sikkert.

Når mange har adgang / Passwords og PIN-koder:

Pengeinstitutterne (her Bikuben oktober 1993) udgiver gode råd om, hvordan man bruger sit kort på den sikreste måde:

1. **OPBEVAR DIT KORT FORSVARLIGT**

   Kortet er lige så personligt som pas, kørekort, sygesikringsbevis og lignende.

2. **KUN DU MÅ KENDE DIN PIN-KODE**

   Koden er din elektroniske underskrift. Fortæl den ikke til andre og brug den ikke i andre sammenhænge, hvor du selv kan vælge en kode.

3. **BRUG DIN PIN-KODE TIT - SÅ HUSKER DU DEN.**

   PIN-koden må aldrig opbevares sammen med eller noteres på kundekortet. Har du alligevel behov for at notere din PIN-kode, så bed (Bikuben) om en PIN-kode Husker.

4. **BRUG DIN PIN-KODE, MEN GØR DET DISKRET.**

   Stil dig tæt op af terminalen eller pengeautomaten og dæk tasterne med den frie hånd, mens du taster PIN-koden ind.

5. **UDFYLD ALTID ALLE FELTER NÅR DU UNDERSKRIVER EN NOTA**

   Sæt en vandret streg eller krydser foran beløbet således, at det ikke efterfølgende kan forøges.

6. **HUSK AT FØRE REGNSKAB**

   Gem kvitteringen og sammenhold den med din kontoudskrift fra (Bikuben).

7. **OPBEVAR IKKE DIT KUNDEKORT TÆT PÅ MAGNETISKE FELTER**

   Opbevar aldrig dit kundekort i nærheden af magneter - f.eks. magnetlåse på tasker. Det kan medføre, at informationerne i kortets magnetstribe ødelægges.

8. **HVIS DIT KORT FORSVINDER ELLER BLIVER STJÅLET SÅ MELD DET STRAKS.**

   Kontakt straks (Bikuben) eller - uden for (Bikubens) åbningstid - PBS på telefon: 44 89 29 29.

Når mange har adgang / Datasikkerhed med cryptering:

Ønskes data sikret på en sådan måde, at en stjålen kopi ikke må kunne læses, er datacryptering måden.

Datacryptering betyder at data via en hemmelig kode/nøgle omsættes til en serie uforståelig tal, tegn og bogstaver, som kun kan føres tilbage i læsbar form ved brug af den rette kode/nøgle.

Kopieres data ud på diskette fra harddisken eller tages hele disken ud og isættes en anden PC vil det fortsat være umuligt at læse data uden kendskab til koden/nøglen.

Cryptering kan udføres hardwaremæssigt via specielle kredsløbskort eller softwaremæssigt via forskellige specialprogrammer.

Af andre sikkerhedsgrunde bør en sådan kode/nøgle opbevares i forseglet kuvert i en eller anden boks, eller være kendt af 2 personer, så firmaet kan få adgang til sine data hvis en medarbejderen skulle blive indisponeret pga. sygdom, ulykke eller fyring.

Teknikken svigter:

En PC arbejder upåklageligt i lange perioder, måske i årevis.

Så, pludseligt går et eller andet frygtelig galt, og det er ikke gennemskueligt, hvorfor der er fejl - den opfører sig simpelthen underligt !

Kan det være:

- **Et simpelt hardware problem ?**
- **En uventet fejl i softwaren ?**

Eller kan det være noget mere alvorligt:

- **En tidsindstillet bombe ?**
- **En logisk bombe ?**
- **En trojansk hest ?**

Mest sandsynligt skyldes fejlen:

- **En hardware fejl.**
- **En software fejl.**
- **En menneskelig operativ fejl.**

Den mest almindelige årsag til massive tab af data, er det lejlighedsvis glimt af idioti, vi alle lider af.

Især **DEL *.*** -kommandoen brugt i et forkert bibliotek eller drev, og altid hvor der er filer, der ikke desværre ikke er taget backup af.

Eller, i den sene nattetime, hvor **FORMAT** bruges på netop den diskette, hvor flere ugers arbejde er gemt, og det er den eneste kopi, man har !!

Husk muligheden for UNDELETE og UNFORMAT.

Teknikken svigter / El-problemer og fejl:

Har man edb-udstyr i hjemmet vil det være en god ide, at få installeret en separat sikringsgruppe udelukkende til dette, og helst med 3-benet jordforbindelse.

Så undgåes at feks. start af en støvsuger, en større maskine eller andet el-krævende udstyr får strømmen til 'at dykke', hvilket kan få en følsom PC'ere til at slukke med evt. komponentskader til følge.

De fleste PC'ere leveres med 3 ben på net-stikket - og det vil være en fordel om dette kan bevares aht. fejlspændinger mv.

Er man privat afhængig af sin PC eller befinder arbejdspladsen sig i et område, hvor der ofte er problemer med den offentlige strømforsyning, det være sig svigt eller spændingsdyk, kan det anbefales at investere i et UPS-anlæg.
UPS står for: Un-interuptable Power Supply

Dels sikres edb-udstyret mod de spændingsvariationer (transienter), som altid kan forekomme i et el-net og dels fungerer UPS-'en som nødstrømsforsyning, hvis by-strømmen svigter helt.

Investeringen vil i bedste fald kunne tjenes ind ved at PC'erne ikke ødelægges, samt ved den tid der spares til re-konstruktion af tabte data mv.

Arbejder man med meget store edb-installationer kan det være en god ide at sikre 2 uafhængige strømtilførsler til bygningen, således at et evt. overrevet kabel (gravemaskiner !) ikke er ensbetydende med totalt strømsvigt.

De store edb-virksomheder supplerer under alle omstændigheder med egen nødstrømsforsyning, UPS-anlæg, batterier og evt. nød-dieselgeneratorer.

Teknikken svigter / El-problemer og -fejl:

Tæt på 90% af de edb-fejl som opstår via spændingsforsyningen stammer fra transienter.

Transienter på netspændingen stammer typisk fra støjkilder som lynnedslag, variation i netspænding, fejlforbindelser o.lign.

Arbejder edb-udstyret i netværker, dvs. med kabelforbindelser mellem en lang række PC'ere højt og lavt og dybt i huset er der grund til at sikre, at datakablerne ikke ligger parallelt med og for tæt på spændingskabler når de ligger i samme kabelbakke.

Om ikke andet må man benytte særligt skærmede datakabler.

Datanettet påvirkes typisk af støjkilder som: Elektrostatiske udladninger, elektromagnetisk interferens, forskelle i jordpotentiale og fra fejlspændinger ved uheld.

Der findes grundige beskrivelser af disse støjforhold og modforhold i IEEE 802.2 i afsnittet om sikkerhedskrav til LAN (Local Area Networks).

Problemerne kan undgås hvis man:

- adskiller data- og spændingskabler
- indkobler transientbeskyttere

- benytter skærmede datakabler
- udlægger lysleder/fiberoptiske kabler

De første pinde kan anvendes i eksisterende installationer; de sidste 2 er at anbefale til alle ny-installationer.

Teknikken svigter / El-problemer og -fejl - UPS-anlæg:

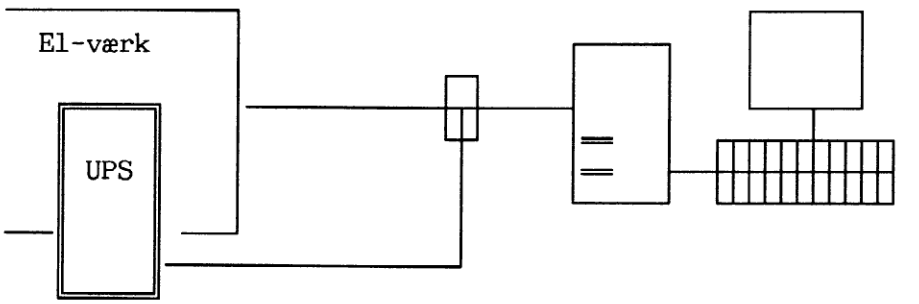
Med en **UPS-enhed** kan det centrale edb-udstyr sikres både mod transienter (varierende netspændinger) og direkte strømsvigt. **UPS-enheden** leverer fortsat strøm længe nok til, at data kan gemmes og alle igangværende programmer lukkes kontrolleret ned.

UPS-enheder fra leveres som 2 typer:

OFF-LINE HOT STAND-BY

ON-LINE

OFF-LINE HOT-STAND-BY betyder, at strømforsyningen til edb-udstyret normalt fødes direkte fra by-strømmen med UPS'en i klarposition til at overtage, hvis by-strømmen svigter.



Der skal altså foretages et skift som foregår glidende på mindre end 4 ms, hvilket er hurtigt nok til, at edb-udstyret fortsætter sin drift.

Overgangen til UPS'en betyder at man nu har et begrænset antal minutter til rådighed så alle igangværende aktiviteter kan afsluttes efter forskrifterne.

Det er ikke meningen at man skal fortsætte sin drift på strøm fra UPS'ens batterier - der er kun en forholdsvis begrænset kapacitet.

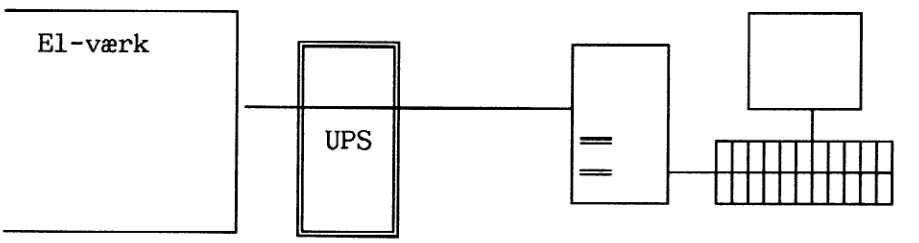
Teknikken svigter / El-problemer og -fejl - UPS-anlæg:

ON-LINE UPS betyder at edb-udstyret konstant modtager sin strøm via UPS'en, som igen konstant oplades fra by-strømmen.

Svigter by-strømmen vil der ikke være nogen omskiftning; edb-udstyret arbejder videre indenfor de tidsmæssige begrænsninger batterierne tillader.

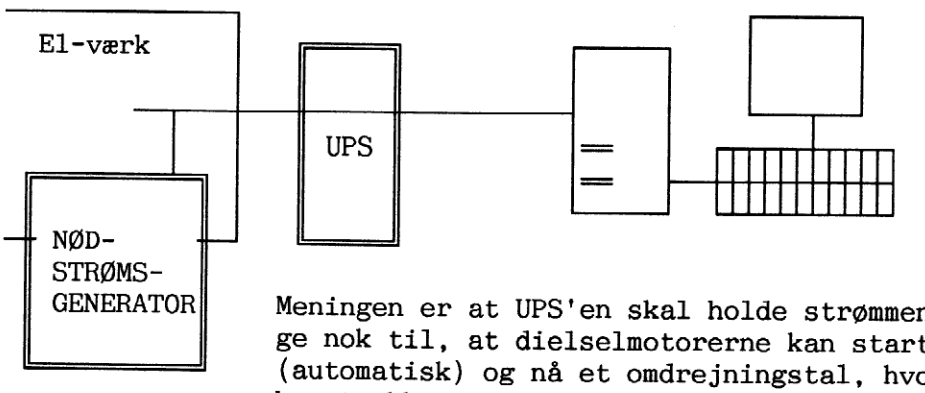
UPS'enheder er specificeret med en VA-angivelse (VoltAmpere), som i grove træk svarer til det Watt-forbrug der skal kunne trækkes fra dem. VA er ca. 20% højere end Watt. VA x 0,7 = Watt, som i UPS-terminologi udtrykkes som Power Factor (PF).

Ved dimensionering (og køb) skal man være opmærksom på hvilket omregningsfaktor den enkelte leverandør benytter.



Normalt har man kun UPS-sikret de væserntligste maskiner, feks. servere og særligt udvalgte PC'er; der er normalt ingen grund til at have sikret printere, scannere, plottere el. lign.

Har man behov for at kunne fortsætte driften efter overgang til UPS-strøm, må man nødvendigvis supplere med et egentligt NØDSTRØMSANLÆG feks. med dielselgeneratorer.



Meningen er at UPS'en skal holde strømmen længe nok til, at dielselmotorerne kan startes (automatisk) og nå et omdrejningstal, hvor de kan trække generatorerne.

Teknikken svigter / Maskinfejl og diskfejl:

Naturligvis kan der ske maskinfejl, som feks. bevirker at maskinen 'går død' midt i en arbejdsprocess.

Almindeligvis vil data, som er lagrede/gemt før problemets opståen være intakte; kun de data, som var direkte under behandling vil være tabt.

Dog skal det tilføjes, at de fleste moderne database-produkter også er istand til at genskabe disse, så snart maskinen er køreklar igen.

Hvorfor og hvordan fejlen egentlig opstod, om det var maskinen, programmet, en uheldig kombination af begge, en eller anden form for 'misforståelse', eller om brugeren ramte en 'forkert' tast det vides sjældent eller aldrig.

Men det vigtigste her (for brugeren) er dog også, at data er intakte og at kun de sidste indtastninger skal gentages.

Alvorligere ser det ud, hvis der pludselig opstår fejl iforb. med maskinens indbyggede harddisk, enten ved at man ikke kan komme i forbindelse med den (fejl i kontrol-elektronikken) eller at data ikke kan læses/skrives pga. af fysiske skader på diskens magnetiske overflade.

Fejl i elektronikken kan oftest repareres, men man vil ikke kunne komme til sine data i en længere periode; maskinen skal til reparation.

Er der opstået fysiske fejl på diskens pladeoverflader kan i uheldigste fald kan mange timers arbejde være spildt; det vil ofte være umuligt at gen-skabe data som lå netop på det ødelagte sted, men størstedelen af data vil typisk kunne reddes ved brug af et særligt Utility-program til formålet.

Er data ekstremt vigtige er sidste udvej at sende disken til et laboratorium, som med yderst avancerede metoder vil kunne genskabe tæt på 100% af diskens indhold, feks. også efter en brand.

Skal man undvære sin maskine incl. adgang til data i længere tid uden mulighed for at gen-etablere sit edb-miljø kan det blive en alvorlig affære for forretningsgangen og virksomhedens evne til fortsat at kunne betjene sine kunder.

Kun de færreste udarbejder et sæt manuelle arbejdsprocedurer så arbejdet vil kunne udføres uden anvendelse af edb - men det giver da stof til eftertanke !

Teknikken svigter / Maskinfejl og diskfejl:

Specielt er harddiskene på netværksservere brugsmæssigt sårbare, da de rummer både programmer, administration og data for et større eller mindre antal brugere.

For at sikre den konstante adgang til diskene kan man vælge disk-systemer af RAID-typen.

RAID står for:

Redundant Array of Inexpensive Disks.

RAID-diske findes i 6 sikkerhedsniveauer:

RAID 0 - Striping
RAID 1 - Spejling
RAID 2 - Disk med checksum
RAID 3 - Striping (en diskarm) og checksum
RAID 4 - Striping (flere diskarme) og checksum
RAID 5 - Striping (flere diskarme) og striping af checksum

Med RAID 5 niveau'et kan kun brand, vand og fysisk vold forhindre fortsat adgang til data.

Det skal nævnes, at RAID 4 og 5 også vil kunne implementeres som en software-løsning op mod både fysiske og logiske volumes.

Men også stabiliteten i maskinellets øvrige komponenter og kredsløbskort bør indgå i en bredere sikkerheds-, drifts- og risiko-vurdering

Specielt i netværk gælder det gamle ord om, at kæden ikke er stærkere end det svageste led.

Problemet er, at identificere dette led !

Følgende sider beskriver mere detaljeret teknikken på de forskellige RAID-niveauer.

Teknikken svigter / Maskinfejl og diskfejl:

Da PC'en, som så meget andet, kan køre død, hvad gør man så ?

Nemt nok - man sender den til reparation !

..... men STOP !

Hos mindre og mellemstore virksomheder vil 'HELE FIRMAET' ligge på maskinens harddisk !

Tør man sende den afsted og satse på, at der ikke er nogen der, når maskinen virker igen, 'lige skal se hvad der mon ligger på disken' ? Maskinen skal trods alt afprøves inden vi får den tilbage, ellers er det jo også galt!

Som stor-kunde med service-aftale bør kontrakten indeholde garantier for, at der ikke foretages kopiering, garantier for hemmeligholdelse mv. samt noget om retslige skridt hvis aftalen overtrædes.

For den lille bruger, feks. enkelt-mandsvirksomheden, som netop har alt på een PC, skrives der ikke kontrakter, blot fordi han indleverer maskinen på værksted, men han er dog beskyttet af markedsføringsloven mfl. hvis der sker uretmæssig brug af data fra maskinen.

Nogle virksomheder anlægger den politik, at ingen maskiner sendes på værksted med en harddisk monteret. Man udtager selv harddisken og gen-monterer den, hvis det ikke er den der er problemet.

Er disken/kontrolenheden defekt destrueres disken.

Da det samtidig kan være en billigere løsning end reparation er det helt fint. Priserne på harddiske falder konstant.

Det kræver blot, at eet enkelt forhold er i orden:

****

S I K K E R H E D S K O P I E R

****

Teknikken svigter / Reparation og salg:

Når en PC gå istå med teknisk fejl er det helt naturligt at sende den på værksted incl. harddisken, som kan rumme mange følsomme firmadata.

Tænk sikkerhed:

- **Har De garanti for at Deres data ikke misbruges ?**
- **Hvordan har værkstedet sikret sig mod indbrud ?**
- **Har teknikerne underskrevet tavshedserklæringer ?**
- **Er Deres data sikret under transport efter rep. ?**

Skal PC'erne sælges skal der ryddes op på disken inden, hvilket betyder at alt skal slettes - ikke kun firmadata men også programmer for ikke at overtræde licensregler mm.

En formatering er ikke nok. Data kan så let som ingenting genskabes med simple kommandoer eller lidt mere avancerede hjælpeprogrammer. Sletning skal foretages enten med direkte overskrivninger med ligegyldig information eller ved hjælp af særlige slette funktioner i de samme programmer som kan genskabe data.

For nylig erhvervede en af vore egne konsulenter en defekt PC fra en kunde.

Vi fik maskinen gjort køreklar - og vupti - var der fri adgang til firmaregnskaber, korrespondance, rykkerbreve, incassosager mv.

Eneste løsning på den slags er altid at fjerne harddisken fra en defekt PC før den sælges eller kasseres. Den fjernede harddisk skal derefter destrueres fysisk.

Teknikken svigter / Programfejl og softwarefejl:

Jo mere kompleks et stykke software er, jo større mulighed er der for fejl i softwaren.

Murphy's Computerlove siger feks.

1. **Komplekse systemer frembringer komplekse fejl.**

2. **Enkle systemer, derimod, frembringer komplekse fejl.**

Første tilføjelse:
Nye systemer producerer nye fejl

Anden tilføjelse:
Nye systemer gentager deres nye fejl

Tredje tilføjelse:
Gamle systemer producerer nye og gamle fejl.

Nogle af dem kan medføre et bemærkelsesværdige tab af data, feks. hvis der er programmeringsfejl i regnskabsprogrammer o.lign.

Selvom et program er testet og afprøvet i alle ender og kanter vil der kunne opstå sammenfald af omstændigheder, som ingen nogensinde havde kunnet forestille sig, og netop kombinationen af disse omstændigheder bevirker, at programmet måske adderer et beløb, hvor det burde have subtraheret beløbet - og af uforklarlige årsager stemmer alle saldi og opgørelser !

Indkøber man regnskabsprogrammer eller tilsvarende, vil det være god politik i en periode på måske op til 6 måneder at fortsat at bogføre parallelt på den 'gammeldags' maner.

Man vil jo i samme periode have sine indlæringsproblemer at kæmpe med, hvilket yderligere udgør en risiko for fejl.

Alle bilag og transaktioner skal gemmes i sin fysiske form, således at det hele, i uheldigste fald, kan rekonstrueres.

Teknikken svigter / Programsammenstød - Clashes

Opstår der mistanke om fejl i retning af systemfejl/programfejl, er det uhyre vigtigt at forsøge at finde systematikken i fejlens opståen, dvs. systematisk at gentage og/eller gennemprøve arbejdsgangene i systemet og at registrere resultater og mellemresultater for hvert skridt.

Et stort arbejde - ja - men trods alt bedre end blot at køre videre for langt senere at konstatere fundamentale fejl i systemet eller systematiske brugsfejl.

Den lidt mere avancerede PC-bruger vil ofte råde over en række forskellige værktøjer til diskvedligeholdelse, administration, fejlfinding, datakomprimering mv., og ofte programmer, som arbejder på det man kalder low level niveau, dvs. så tæt på maskinens teknik som det er muligt.

Feks. overtager programmerne periodisk kontrollen, fremfor at det er styresystemet, DOS'en, der har kontrollen.

De mere kraftfulde low-level værktøjer kan kollidere rent fysisk ved deres brug af samme eller overlappende områder i maskinens interne lager, eller på den måde de feks. arbejder med maskinens harddisk på.

Teknologien har udviklet sig meget hurtigt, og der er i dag flere varianter af harddiske, end man kan forestille sig.

Til nogle af dem anvender man ikke-standard partition-tabeller, så når et low-level værktøj møder en sådan harddisk, giver dette ofte problemer.

Der er ligeledes problemer med disk cache software, programmer til administration af store diske, disk organizers, datakompressorer og andre programmer, der arbejder lavere end DOS-niveau.

Normalt er det sådan, at de programmer, der bryder DOS-reglerne, fungerer korrekt hver for sig, men når man anvender dem to eller flere sammen, kan det føre til tekniske og evt. datamæssige katastrofer.

Man skal undgå et bruge low-level værktøjer sammen med RAM-residente programmer (TSR-programmer/Terminate Stay Resident)

Fremmedes indtrængen / Adgangssikring af lokaler:

Feks. kunne man skrive følgende i sine sikkerhedsforskrifter:

- Døre, låse, vinduer

Alle bygningens yderdøre skal være forsynet med SKAFOR-godkendte låse, og karme og karmtræ skal være af tilstrækkelig høj kvalitet til at modstå fysisk indtrængen i minimum ___ min.

Alle vinduer i bygningen skal være forsynet med indbrudsalarmer, feks. sølvtape, alternativt skal rummene være behørigt alarmsikret med .....

Virksomhedens døre bør alle være adgangs- og alarmsikret. Kun een dør bør benyttes til alle ind- og udgange. Øvrige døre markeres som flugtveje.

Fra hallen bør adgang til ikke-offentlige gangarealer lukkes med en dør, som samtidig skal fungere som adskillelse mellem brandceller.

- Personkontrol

Generelt bør alle medarbejdere bære et synligt ID-kort, som samtidig fungerer som nøgle til virksomhedens sikrede døre.

Generelt skal alle gæster, incl. håndværkere og teknikere, forsynes med et GÆSTEKORT eller TEKNIKERKORT, som skal bæres synligt og returneres ved udgangen.

Kortene administreres og udleveres i receptionen.

- Vægterrundering

Der skal være vægterrundering ____ gange pr. aften/nat samt ____ på Lørdage, Søndage og Helligdage.

Maskin-rum, edb-rum og telefon-central skal have særlig opmærksomhed.

Noget tilsvarende burde naturligvis skrives rettet direkte mod edb-afdelingen og øvrige edb-maskinrum.

Fremmedes indtrængen / Adgang for konsulenter, sælgere mfl.:

Tillid er godt - kontrol er bedre, også når det gælder brug af eksterne konsulenter.

De fleste servicekontrakter indebærer at forskellige, og ikke altid lige bekendte, systemkonsulenter 'farer ud og ind af huset', og ofte betjener de selv både terminaler og centralenhed - en absolut uskik ! (Teknikere dog undtaget)

Kun virksomhedens egne medarbejdere kan være ansvarlige for driften - systemkonsulenterne er det i hvert fald ikke - og derfor bør de også kun røre maskinerne under behørig kontrol.

Tænk sikkerhed:

- **Ved De feks. hvornår konsulenterne kommer og går ?**
- **Har konsulenterne et standardpassword ?**
- **Hvem udleverer passwords til konsulenterne ?**
- **Hvordan kan 4 konsulenter huske samme password ?**
- **Kan konsulentvirksomheden kalde op via modem ?**
- **Bruger konsulenten samme password hos alle kunder ?**

Et andet problem kan opstå, hvor et softwarehus går fallit undervejs i et projekt som virksomheden allerede har postet flere hundrede tusinde kroner i.

Hvordan kommer projektet videre, hvor er programkoden og hvem har rettighederne.

Edb- og datasikkerhed handler derfor også om

- **stram projektstyring**
- **fornuftige leverandørkontrakter**
- **deponering af kildekode**

Fremmedes indtrængen / Hackere, crackere og andre tyveknægte:

Flere og flere benytter PC-netværk og kommunikationsmuligheder ud og ind af nettet. Med muligheden for at fremmede hacker sig ind opstår der et øget behov for sikring.

Som med virus er også hacking blevet et populært og opreklameret emne, som absolut ikke må ignoreres, men som skal behandles på linie med de øvrige risici og sikkerhedsaspekter.

Sikring mod hacking drejer sig ikke kun om fysisk og logisk sikring af kommunikationslinier, men også om sikring mod naivitet.

Iflg. de ægte hackere er det utroligt let, med en lille opdigtet historie, at lokke folk til at opgive telefonnumre og password i telefonen. Også skraldespande og affaldscontainere er ren guf i hackernes forsøg på at finde navne, numre og koder.

Den bedste sikring af eksterne linier opnås feks. ved

- **kun at tænde modem'et når det skal bruges**
- **brug af fast opkoblede linier**
- **brug af modem's med call-back facilitet**
- **brug af modem's med crypteringsmuligheder**
- **brug af opkaldsfaciliteter med elektronisk id**

Interne netværk sikres primært som stand-alone PC'er mod fremmed adgang, virus mv..

Men samtidig stiger behovet for driftstabilitet, som i relation til edb- og datasikkerhed, skal sættes højt. Problemer og fejl skaber panik og kaos - panik og kaos skaber nye fejl som måske fører til tab af data.

Derfor kan man yderligere sikre sig feks. således:

- **nødstrømsforsyning til serveren (UPS)**
- **sikring af server diske (mirror teknik)**
- **sikring af server diske (RAID teknik)**
- **fysisk sikring af udstyret (lokale/adgang/brand)**
- **etablering og afprøvning af nødprocedurer**
- **etablering af katastrofeplaner (back-up center)**
- **driftovervågning/vagttilkald/serviceaftaler**

EDB-virus / Trojanske heste og logiske bomber:

Programmer, der med fuldt overlæg ødelægger ens data på disk kaldes Trojans, eller Trojanske heste, fordi de gemmer sig og først viser sig under forud bestemte omstændigheder.

Trojans er logiske bomber som feks. udløses af en tidsfaktor, på en bestemt dato, feks. fredag den 13.10.89, hvor de måske formaterer harddisken.

Logikbomber udløses, når bestemte betingelser er opfyldt.
Feks. når et bestemt antal filer på disken er opnået, eller når man skriver en bestemt kombination af bogstaver feks. CHKDSK C:, eller hvad konstruktøren (det syge menneske) nu kan finde på

Grunden til at denne type "virus" har fået tilnavnet Trojanske heste er, at de ligger skjult indtil betingelserne er opfyldt, og så 'myldrer' de frem.

Som regel udfører et eller andet flot, uventet grafisk show på skærmen, for at bortlede den stakkels brugers opmærksomhed fra, at kontrollampen blinker hidsigt og lystigt, i programmets vellykkede bestræbelser på at formatere harddisken eller vende op og ned på det hele.

Det er dog ikke alle Trojanske heste, der er så ondsindede;
nogle nøjes med det grafiske show som en lille velment hilsen.

EDB-virus / Trojanske heste og logiske bomber:

Man beskytter sig feks. både mod Trojanske heste og mod edb-virus angreb på følgende måder:

1) **Ved at have og overholde en god backup-procedure.**

2) **Ved kun benytte anerkendte produkter.**

3) **Ved kun at udveksle data-disketter med kendte kontakter**

4) **Ved aldrig at have spil på produktionsmaskiner**

5) **Ved at have kendskab og viden om mulige risici**

6) **Ved rutinemæssig kontrol af maskiner og software.**

7) **Ved særlig sikring af vigtige programmer og data**

8) **Ved at undgå panik hvis der opstår mistanke om virus**

Murphy's Computerlove siger feks.

En computer-virus udbredes principielt via "garanteret virusfri" program- og systemdisketter.

Din computer får virus nøjagtig på det tidspunkt, hvor du er sikker på, at du ikke har nogen.

Den virus, som overfalder din computer, rammer kun de filer, som du ikke har back-up af.

EDB-virus / Vira:

En edb-virus er defineret, som et program, der er i stand til at kopiere sig selv - uden at brugeren ønsker det, og uden at de fleste brugere opdager det.

Den sproglige betegnelse (virus), der er brugt for denne type af programmer, knytter sig til den biologiske virus, som formerer (kopierer) sig selv.

For eksempel kan en virus "angribe" FORMAT-programmet, og blive udført hver gang der formateres en diskette, uden at brugeren er klar over det; alt fungerer tilsyneladende normalt. Men herved kan enten FORMAT-programmet vokse, og/eller virus kan overføres til den formaterede diskette.

Ligeledes kan virus sætte sig på COMMAND.COM eller en hvilken som helst anden eksekverbar fil.

Virus-koden udføres før det originale program, og først herefter overgives kontrollen til det ægte program. Der er flere måder en virus kan arbejde på, feks. som Jerusalem-virus (1813), der installerer sig selv i RAM-lagret og inficerer ethvert program, der herefter udføres.

Jerusalem-virus er kendt under mange navne, men angriber 'kun' COM og EXE-filer. COM-filer vokser med 1813 bytes, men kun én gang, hvorimod EXE-filer vokser med mellem 1792 og 1808 bytes, hver gang den udføres. Programfilen kan til sidst blive så stor, at den ikke kan loades ind i lagret.

Der afsløres flere og flere nye virus-typer, hvilket betyder at der også udvikles flere og flere - der er indtil videre afsløret mere en 1200 forskellige, hvor der tilsvarende er konstrueret forskellige former for værn imod.

Specielt hvis man udveksler mange disketter med kolleger, kunder, leverandører eller venner bør man ikke arbejde uden et Anti-Virus program.

I en virksomhed bør der stå en (gammel) billig PC udelukkende til at virus-teste indgående disketter før de benyttes i firmaets øvrige PC'ere, og naturligvis virus-teste alle udgående disketter, så man ikke ved en fejl er med til at sprede galskaben.

Konstaterer man virus på en modtaget diskette skal man omgående meddele afsenderen om sit fund, og derefter sikre at den ikke har haft mulighed for spredning i egen organisation.

EDB-virus / Vira:

Hovedproblemet, som en virus medfører, er de mange unormale sideeffekter, feks. indvirkningen af en virus i et netværk.

En virus er et RAM-resident program (TSR), som foretager ting med disken på low-level niveau. Et netværk er ligeledes et TSR-program, der også arbejder med disken på low-level niveau, ikke alene disken på den inficerede datamat, men følgelig også på Server-disken, og disken for alle de maskiner, der er koblet på netværket....

.....og dette netværk er måske koblet op mod en Mainframe,.... som er et enkelt domain i et større netværk..., og så er det at virus breder sig !

Eksempelvis er Jerusalem virus nogle gange tænkt til at være en pestilens kun når en fredag falder på den 13., hvor virus'en så sletter programmer som man prøver at udføre.

Men på et Novell netværk, vil Virus'en støde sammen med Novell Netware, og netværket vil ikke fungere korrekt.

Der er virus, der er uklare i deres sigte på skade. Virus'en Datacrime laver en low-level formatering af spor 0 på en harddisk, når den aktiveres, hvorefter disken ikke kan benyttes.

Virus kendes i flere forskellige former, og alt efter hvordan de optræder, har man inddelt dem i følgende typer:

- **Boot sektor virus (BSR)**
- **Partition sektor virus (PSV)**
- **Fil-virus:**
  - *** Direct Action (DAFV)**
  - *** Indirect Action (IAFV)**

EDB-virus / Vira:

Boot-sector virus:'

En boot sektor virus erstatter diskens boot sektor med sin egen kode og flytter den originale boot sektor til et andet sted på disken. Når der startes op fra disken, vil virusprogrammet først blive udført, og derefter vil den sædvanlige boot proces blive udført.

En boot sektor virus kommer ind i maskinen, før alt andet software, hvorfor beskyttelse med anti-virus programmer er noget vanskeligere.

Når en boot sektor virus én gang har sat sig fast i boot sektoren, vil virus blive udført hver gang, der bootes. Virus'en loader sig selv ind i RAM-lagret, og beskytter sig selv ved at markere hukommelsen som værende i brug.

Virus'en angriber nogle af PC'ens interrupts - typisk disk read/write interrupt, så hver gang der læses eller skrives på disken, vil Virus'en blive afviklet først.

Nogle boot sektor virus angriber kun disketter, andre angriber også harddisken. Hvis en boot sektor virus har angrebet en harddisk eller en DOS opstartsdiskette, vil der hurtigt kunne komme et stort antal af inficerede disketter i omløb.

Beskyttelse mod boot sektor virus:

Der er principielt to måder, man kan beskytte sig mod, at boot sektor virus kommer ind i maskinen.

Den første er, at lade boot sektor Virus'en tro, at den allerede er inde, og så vil den ikke prøve at komme ind igen.

Den anden måde at beskytte sig på, er at sørge for boot sektor Virus'en ikke kan komme sammen med hardware.

Der er flere produkter, som kan hjælpe med en sikring mod bootvira, bla. Dr. Solomon's Anti-Virus Toolkit program, McAfee, Safetynet's VirusNet mfl.

EDB-virus / Vira:

Partition sektor virus

Partition sektor virus ligner boot sektor virus; den angriber der imod harddiskens partition sektor - og ved disketter vil den angribe boot sektoren og virke som en boot sektor virus.

Partition sektor virus er sværere at finde fordi de fleste værktøjer ikke tillader, at man får lov til at se i partition sektoren. Koden i partition sektoren udføres før boot sektoren, så igen vil software, der afvikles under DOS, udføres under kontrol af Virus'en.

Stoned er den mest udbredte partition sektor virus.

Fil Vira

Fil virus kendes under to former, den ene arbejder i en direkte aktion, og den anden indirekte. Begge angriber filer så som COM-, EXE- og SYS-filer. Overlay-filer går heller ikke ram forbi, og så er det ligegyldigt, hvilken extention de har.

Fil Virus - Direct Action (DAFV)

Et DAFV udvider eller indsætter sig selv i en eksekverbar fil.

De fleste COM-filer har tre bytes i begyndelsen af programmet, som udpeger startadressen på det aktuelle program. Virus'en udvider sig selv til slutningen af filen og omdirigerer hoppet til startadressen, så der hoppes til viruskoden. Den sidste instruktion i viruskoden er så et hop til det oprindelige program. Herved vil programmet umiddelbart afvikles normalt, og brugeren får ingen mistanke om, at der er noget galt.

COM-fil virus er nemmere at udvikle end EXE-fil, fordi COM-filer har en simpel struktur, som bevirker, at de nemt kan angribes. EXE-fil virus er derfor mindre udbredt, men skal alligevel ikke ignoreres af den grund.

Der findes virus, som er i stand til at angribe både COM- og EXE-filer, og gør det ved at undersøge filtypen, for derefter at bestemme, hvilken handling, der skal udføres (feks DATACRIME II)

Da det er nemt at læse og ændre fil-attributten, kan man hverken på dato, tid eller read-only sikre sig eller opdage angrebene.

EDB-virus / Vira:

Fil Virus - Indirect Action (IAFV)

Et IAFV angriber COM og EXE-filer ved at Virus'en sætter sig i RAM-lagret, og vil sædvanligvis erstatte koden, DOS-interruptet, for "afslut program".

Men den kan også erstatte andre interrupts som benyttes ofte. Et godt interrupt at opsnappe, er interruptet for "Load and Execute program", der anvendes når DOS prøver at loade en EXE eller COM-fil, som jo netop er de filer, som Virus'en ønsker at angribe.

Det, at Virus'en sidder i RAM-lagret bevirker, at hver gang DOS gør noget som helst, har Virus'en kontrollen. Den gør, hvad den vil først, og derefter giver den kontrollen til DOS, der får lov til at udføre sine instrukser, enten i intakt eller (af Virus-'en) i en modificeret form.

Det betyder, at man kun behøver at udføre en IAFV én gang, hvorefter den vil angribe mange andre filer. Det betyder også, at en maskine, der kører under kontrol af Virus'en, er uforudsigelig.

EDB-virus / Anti-Virus programmer:

Der findes flere anti-virus programmer på markedet, nogle bedre end andre målt på deres evne til dels at identificere en given virus og dels på deres evne til at fjerne eller omgå den fundne virus.

Typiske anti-virus programmer benytter sig af en virus-scanner, som loades resident i RAM (TSR-rutine) iforb. med boot af PC'en. efter at RAM'en først for skjulte vira.

TSR-rutinen kontrollerer ethvert program som startes, og forhindrer eksekvering og dermed spredning, hvis der findes virus iforb. med .COM eller EXE.-koden.

Scanneren baserer sin kontrol på 'mønstergenkendelse' ud fra en tabel med mønstret på alle kendte PC-vira, en tabel som løbende opdateres af de førende producenter, typisk 4 gange om året.

Anti-virus programmerne tilbyder også en anden kontrol form baseret på, at registrere størrelsen på alle PC'ens program-filer og gemme informationerne i en kontrol-fil.

En periodisk kontrol, hvor filernes aktuelle størrelse kontrolleres op mod kontrol-filen vil afsløre, om der er sket ændringer i et program, og i hvilket.

Det betyder til gengæld også, at når programmer opdateres eller nye installeres skal man huske at skabe en ny kontrol-fil.

Moderne anti-virus programmer arbejder efter samme princip som virus-byggerne, dvs. at de følger virus-byggernes tankegang og søger efter vira de steder hvor de mest sandsynligt befinder sig - hvis de er der.

Moderne antiv-virus programmer leder også efter mutationer af kendte vira, samt holder øje med hvordan programmerne opfører sig i relation til brug af maskinens interrupts og hardware.

Hardware-kontrol baserer sig på ethvert programs opførsel i relation til at foretage sig ting, som normalt ikke er 'tilladt' i PC'en.

EDB-virus / Anti-Virus programmer:

Her betyder 'tilladt' feks. skrivning direkte til harddisken udenom den normale kontrol af styresystemet.

Denne form for sikring påstås at være fremtidssikret, da den ikke er baseret på nogen bestemt virus-type men i stedet på den generelle angrebsformen.

Men ikke nok med at anti-virus programmet skal kunne finde vira, det skal også kunne fjerne eller omgå dem.

Man vil i et vist omfang kunne vælge om det skal ske automatisk eller om man ønsker lidt mere kontrol med havde der foregår, og hvordan.

Nogle programmer vælger direkte at fjerne virus'en hvor den blev fundet, mens andre fletter den inficerede fil helt.

Under alle omstændigheder gives der en passende lejlighed til en mere omfattende kontrol, når PC'en er blevet inficeret.

Ud over de tidligere beskrevne måder at sikre sig mod virus på, kan man nævne et produkt som Dr. Solomon's RingFence, som baserer sig på at påføre disketter en intern firmakode.

Kodede disketter kan således kun anvendes på maskiner med RingFence installeret og kan ikke indføres i virksomheden før de er blevet virus-kontrolleret af Dr. Solomon Anti-Virus Toolkit og har fået påført en maskinel godkendelse.

RingFence koden sikrer samtidig mod pirat-kopiering af programmer og mod udlevering af firmadata til fremmede - disketterne kan simpelthen ikke læses.

Også indenfor et firma kan man etablere flere uafhængige RingFence-grupper, feks. een for udviklingsafdelingen, een for salgsafdelingen og een for administrationsafdelingen.

Det er dermed ikke muligt at overføre eller udveksle disketter på tværs af afdelingsgrænserne.

... og samtidig undgåes muligheden for inficering af PC-virus !

EDB-virus / Anti-Virus program-test's:

Andre ulykker / Katastrofer, brand, vandskade

Ordet katastrofe har en klang af noget voldsomt over sig, som feks. naturkatastrofer: oversvømmelser, stormskader, vulkanudbrud el. lign. eller omfattende ulykker som eksplosionsulykker, togsammenstød, flystyrt mv.

Naturligvis kan også mennesker skabe katastrofer feks. iforb. med sabotager, attentater eller sågar som følge af en stejke.

Om noget kan karakteriseres som en katastrofe eller ikke, i relation til edb-drift og evt. data-tab, er mere en angivelse af **konsekvensen** fremfor selve hændelsen.

Og konsekvens-vurderingen går primært på virksomhedens evne til at overleve hvis man pludselig ikke har adgang til sine styrings- og produktionsværktøjer, kunde- og leverandørregistre, bogholderi og finanssystemer, ordre- og produktionsstyringssystemer mv.

Kan virksomheden ikke levere varer, uanset årsagen, mistes sandsynligvis kunder til konkurrenterne, og ikke alle kunder kan påregnes at vende loyalt tilbage når vi atter kan levere.

Er ledelsen feks. bekendt med konsekvenserne ? Kender de svarene på følgende spørgsmål ?

- **Hvordan er virksomhedens afhængighed af forretningsinformation**
- **Kan virksomhedens forretningsprocedurer opretholdes i en krisesituation ?**
- **I hvor lang tid (minutter/timer/dage/uger) kan virksomheden være uden adgang til sine informationssystemer ?**
- **Hvor store tab kan påregnes ved en langvarig afbrydelse af virksomhedens forretninger ?**
- **Hvordan kan man sikre virksomhedens fortsatte drift i en krisesituation ?**

Andre ulykker / Katastrofer, brand, vandskade

Det er ikke nødvendigvis en katastrofe, at en edb-maskine er defekt, men det kan være en katastrofe, hvis virksomhedens fortsatte drift afhænger af netop denne maskinenes tilgængelighed.

Skulle det værste ske, en rigtig katastrofebrand, en alvorlig sammenstyrtning eller store vandskader, så dataudstyret udsættes for alvorlig påvirkning er der stadig en chance for, at ikke alt (alle data) er tabt.

Maskinerne er ikke nødvendigvis det store problem; specielt PC'ere og Servere vil kunne gen-anskaffes meget hurtigt og sættes i drift på relativ kort tid (1-2 dage), men skal vitale data, som er nødvendige for at kunne fortsætte virksomhedens drift kunne gen-etableres indenfor samme korte tid (eller endnu hurtigere) så er det helt nødvendigt, at man har haft en effektiv backup procedure og passet godt på sine medier.

Diske og disketter fra de ødelagte maskiner og lokaler kan med et vist held gen-skabes i laboratoriemiljø, hvis det skulle blive nødvendigt - men det tager tid.

I Norge findes det eneste laboratorie af sin art (ibas), som er i stand til at genskabe data fra datamedier som har været udsat for de meget store varmepåvirkninger fra brande og fra vandskader som måtte være en følge af brandbekæmpelsen eller have andre årsager.

Eneste forudsætning er, at medierne ikke har være forsøgt anvendt i nogen maskine efter skadepåvirkningen.

Brandalarmer og slukning:

Som mod andre risici er det bedre at forebygge end at helbrede, i dette tilfælde ved installation af feks. alarmer.

Normalt monteres brandalarmer (sensorerne) i loftet, hvor de påvirkes enten af varme (temperaturfølsomme) eller af røg.

I begge tilfælde vil branden have været igang et godt stykke tid inden alarmen lyder !

Andre ulykker / Katastrofer, brand, vandskade

Da elektronikbrand sjældent udvikler sig eksplosivt, men snarere snigende med start i et overophedet komponent, som står og ulmer inde i et kabinet. Varmen forplanter sig til ledninger og ledningsisolering som begynder at afgive dampe.

Hvorfor ikke fange branden allerede på dette tidspunkt ?

Der findes udstyr til direkte montage feks. på server-maskiner, hvor man indsætter luftslanger i hvert enkelt kabinet.
Slangerne fører til en røg-analysator, som ved den 'rette' påvirkning udløser en alarm.

Systemet kaldes Air Sampling Detection.

Systemet kan monteres så det er muligt præcist at identificere den server (eller anden maskine) som ulmer.

Uanset hvad der udløser brandalarmen, kan det forbindes til noget automatisk slukningsudstyr.

Normalt forbinder man ikke slukning af elektronikbrande med vand, men det er slet ikke så tosset endda, bla. fordi vand ikke på nogen måde indeholder stoffer, som er skadelige for elektronikken (feks. syrer) eller udvikler andre skadelige stoffer under selve slukningsprocessen.

Andre ulykker / Katastrofer, brand, vandskade

Større edb-rum blev tidligere sikret med Halon 1301, et stof som nu er totalt forbudt fra 1/1-1994. Halon'en skal tømmes af anlæggene og deponeres i en Halon-bank. Fremover må det kun benyttes i flyvemaskiner, hvor andre slukningsmidler er uegnede.

Halon'en fjerne kortvarigt ilten fra luften, lige længe nok til at ilden ikke kan næres.

For at der overhovedet kan næres en ild skal der være 3 elementer tilstede:

* **Brandbart materiale**
* **Høj temperatur**
* **Ilt**

Fjernes een af elementerne er der ingen ild !

Pr. 1. Februar 1992 indførte man skærpede regler for brug af Halon i Danamark. Forbudet omfatter:

* Alle anvendelser som ikke er nævnt nedenfor efter 1/1-1992.

* Produktion, salg og genopladning af håndslukkere efter 1/2-1992.

* Tilsigtede udslip iforb. med afprøvning efter 1/2-1992.

* Etablering af stationære slukningsanlæg efter 1/1-1993.

* Efterfyldning af stationære slukningsanlæg med ny Halon efter 1/1-1994.

* Efterfyldning af stationære slukingsanlæg med gen-vunden Halon (recirkuleret) efter 1/1-1999.

* Livsnødvendig anvendelse som bla. omfatter skibe, fly og forsvar er tilladt efter 1/1-1999 (indtil videre).

Andre ulykker / Katastrofer, brand, vandskade

Omkring brandsikring skal kabelkanaler og specielt kabelgennemføringer i murværk have et ord med på vejen.

Gennemføringer skal altid være fyldt ud med brandhæmmende materiale - ikke kun når arbejdet er færdiggjort - men hver eneste dag inden håndværkerne forlader etablissementet.

En åben kabelgennemføring vil i værste fald kunne virke som trækkanal for en opstået ild og forstærke dens spredning på samme måde som trappe-, elevator- og ventilationsskakte gør det.

Røg-sikring:

Røg fra egen brand eller røg fra nabo-virksomheders udslip kan i værste fald skabe periodiske fejl i edb-udstyret, hvis dette rammes af syreholdige røggasser.

Komponenter og forbindelser ætses langsomt med fejl til følge - en langsomt snigende katastrofe.

Det er næsten umuligt for teknikeren at finde frem til det defekte komponent, da det, i hvertfald kun i starten, giver periodiske fejl.

Når først fejlen er permanent vil mange andre dele i maskinen være tilsvarende skaset.

Netop faren for røggassser til edb-udstyret er en af grundene til, at diverse ventilationsspjæld skal lukke automatisk iforb. med en brandalarm.

Gemmer man sine datamedier i S60DIS eller S120DIS klassificerede brandskabe er medierne samtidig sikret mod røggasser med den særlige måde døre og karme mødes.

Fugt- og vandskader:

EDB-udstryr 'gemmes' typisk af vejen i en kælder, bla. ud fra betragtningen om, at den er bedre sikret mod både fremmed indtrængen og mod brand - hvilket lyder rigtigt !

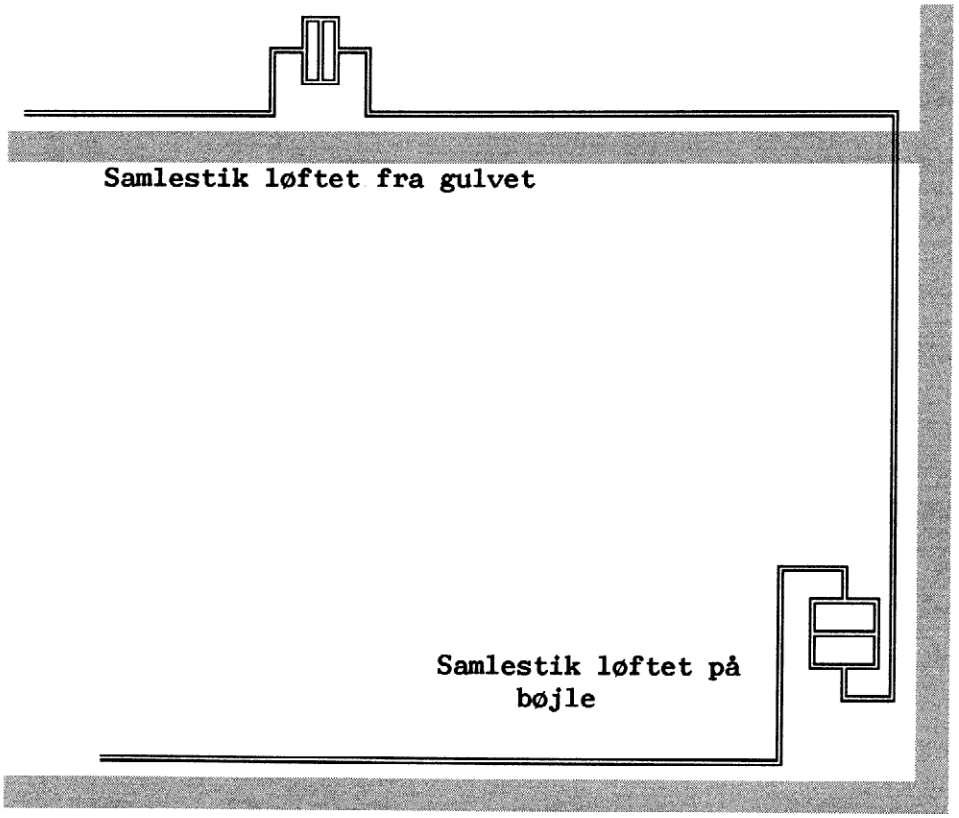
Til gengæld kan den blive udsat for fugt- og vandskader; sprungne vandrør, kondensproblemer, kloakker der løber over mm.

En fugt-alarm ville kunne gøre underværker - og at placere edb-udstyret i palle-reoler kunne være en anden løsning.

Andre ulykker / Katastrofer, brand, vandskade

Specielt kan kabelsamlinger være sårbare, hvis kablerne føres under dobbelt-gulv eller i kabelskakter på muren.

Det vil altid være god politik at hæve samlestikkene fra gulvet eller løfte dem op i en bøjle.



Føres kabelskakten uden på husmuren, bør skakten være kraftigt ventileret for at undgå kondensdannelser.

Andre ulykker / Katastrofeplan & -beredskab.

Også her drejer det sig i sidste ende om penge; det er dyrt at opretholde et meget omfattende katastrofeberedskab mod katastrofer, som kun med ganske lille sandsynlighed vil forekomme, så det gælder om at finde 'den gyldne middelvej' - et niveau som er både realistisk og økonomisk forsvarligt.

Beredskabsplanen skal dokumentere hvordan virksomheden har tænkt sig at overleve katastrofer (disse skal defineres), og planen skal fortælle alle parter i virksomheden hvordan de skal forholde sig i katastrofesituationen og hvilke maskiner, systemer og data der er nødvendige for den fortsatte drift af afdelingen/-virksomheden, og dermed minimere følgevirkningerne.

En beredskabsplan kan feks. indeholde følgende overskrifter: *)

- **Forudsætninger for planen**

- **Definition på katastrofer (virksomhedens def.)**

- **Definition på kritiske ressourcer (maskiner, systemer, data)**

- **Organisation og ansvarsfordeling**
  Tilkald, escalering mv.

- **Handlingsplan**
  Hvem beslutter planens igangsætning
  Hvem indgår i kontrolgruppen
  Hvem varetager brugerkontakten
  Hvem varetager leverandørkontakten
  Hvordan kommunikeres til omverdenen
  Hvordan opretholdes sikkerheden bla. i relation til revisionen og lovgivningen.

- **Re-etablering**
  Hvad, hvor og hvordan skal re-etableres
  Prioritering
  Hvem skal udføre hvilke opgaver (personale/konsulenter)
  Bruger- og leverandør-aftaler, midlertidigt/permanent
  Kontroller og test før igangsætning

- **Test af selve katastrofeberedskabsplanen**

*) Dette er kun et eksempel; litteraturen rummer en lang række opfattelser med flere eller færre detaljer.

Andre ulykker / Katastrofeplan & -beredskab.

Man skal være opmærksom på, at det i praksis vil være nogle relativt få af virksomhedens mange systemer, som reelt er umiddelbart kritiske i en katastrofesituation, og derfor skal gen-etableres omgående.

De øvrige systemer kan prioriteres og under gen-etableres under lidt mere rolige former de følgende timer/dage/uger.

Det er væsentligt at man har en detaljeret oversigt over systemerne, deres ejerforhold, anvendelse, grænseflader indadtil og udadtil, tilknyttede manuelle procedurer (også alternative), kendskab til data, deres opbygning og aktuelle status og meget mere.

Omkostninger ved at opretholde et realistisk beredskab skal afvejes mod konsekvensen, også de indirekte omkostninger som fremkommer ved forsinkede leverancer, negativ presseomtale, tab af troværdighed, dårligt image mv.

Selvom meget dækkes af forsikringerne, både de direkte tab som følge af katastrofen (maskiner, erstatningsudstyr, overarbejde, drifttab mv) dækker forsikringen ikke tabte markedsandele.

Andre ulykker / Kolde og varme back-up centre

Som led i en katastrofeplan og et katastrofeberedskab bør indgå en vurdering af behovet for back-up center aftaler.

De store danske hovedbanker har, efter deres fusioner, datacentre i henholdsvis Jylland og i København, og Kommunedata har tilsvarende centre i København, Odense og Ålborg, hvilket gør det muligt for dem, at arbejde med spejlede registre, spejlede maskinkonfigurationer og forskellige nød- og fall-back-procedurer, hvis et af centrene bliver 'ukampdygtig'.

For andre, som ikke indenfor firmaets egne rammer, har de muligheder, er der til gengæld mulighed for at lave aftaler med autoriserede back-up centre, feks. Dansk Back-up Center i København eller svenske Backup Centralen, som har etableret afdelinger i Stockholm og Oslo.

Back-up centre findes i 2 udgaver:

KOLDT BACK-UP CENTER:

Omfatter etablerede driftlokaler med dobbeltgulve, ventilation, luft- og vandkøleudstyr, el-tavler, generatorer, telekommunikationslinier og modemer mv.

I en nødsituation skal kunden selv sørge for via sine leverandører at fremskaffe det nødvendige udstyr, få det opstillet og re-etablere driften.

VARMT BACK-UP CENTER:

Omfatter store køreklare anlæg med alt nødvendigt IO-udstyr, kommunikationslinier, modemer mv.

I en nødsituation skal kunden selv sørge for at re-etablere driften.

Andre ulykker / Kolde og varme back-up centre

Dansk Back-up Center tilbyder begge løsninger.
Det kolde center er en del af Mærsk Data's tidligere edb-lokaler i Titangade i København; det varme drives af Mærsk/Datacentralen med en maskine som dagligt anvendes til udvikling og test. Når katastrofen meldes garanteres maskinen frigjort og klargjort indenfor 4 timer.

Centret drives som en forening/sammenslutning, hvor man fast indbetaler et fast abonnement for råderetten over et vist antal kvadratmeter (det kolde) og en vis maskinkapacitet (det varme).

Når alarmen lyder betales en væsentlig højere ydelse i det antal dage eller uger faciliteterne benyttes.

Dansk Back-Up Center kan prale med (Jan. 1993) ikke at have haft en eneste aktiv kunde i 10 år !

Svenske Backup Centralen udbyder varmt back-up center i Stockholm og koldt back-up center i Oslo.

Normal kan man kun være i det varme center en relativ kort periode, aht. muligheden for at andre skal bruge faciliteterne, men længe nok til at faciliteter kan etableres i alternative lokaler, feks. det kolde center's.

En speciel fordel ved det varme center er, at man periodisk, feks. een gang om året, kan afprøve sine nødprocedurer i 'real life miljø'.

Centrene er ikke kun for de store kendte datacentre, men kan anvendes af alle, som ønsker at sikre sig mod det værst tænkelige.

Ansvar og organisation / Hvem er ansvarlig for sikkerheden ?

Det overordnede ansvar for sikkerheden (og ikke kun edb) påhviler virksomhedens daglige leder, som må sørge for, at de sikkerhedsmæssige forhold bliver tilstrækkeligt klarlagt og analyseret og at de deraf nødvendige aktiviteter bliver igangsat.

Det påhviler ligeledes ledelsen at sørge for et tilstrækkeligt kvalifikationsniveau hos de som arbejder med sikkerhedsmæssige opgave, hvilket bla. indebærer at de sikres den nødvendige tid i hverdagen til at udføre arbejdet på tilfredsstillende måde.

At virksomheden evt. har udnævnt en sikkerhedsansvarlig, fritager det på ingen måde de øvrige medarbejdere for at varetage de sikkerhedsmæssige aspekter omkring adgang til og anvendelse af følsomme data.

Det er uden tvivl enhver chef og leders ansvar at sikkerheden varetages på behørig vis indenfor den enkeltes ansvarsområde.

Det må samtidig indebære, at lederen skal tilsikre den nødvendige motivation og uddannelse således, at sikkerheden ikke sættes over styr.

Der bør løbende foretages en vurdering af hvem der har adgang til hvad på hvilket niveau og med hvilke rettigheder, både ud fra et arbejdsmæssigt hensyn og ud fra en vurdering af den enkelte medarbejders habilitet.

Det kan i visse situationer være nødvendigt, at afkræve medarbejderen en ren straffe-attest, at kræve underskrift på særlige hemmeligholdelses- og tavshedserklæringer mv., feks. iforb. med følsomme udviklingsopgaver.

For visse medarbejdergrupper vil det være nødvendigt med et grundigt kendskab til den juridiske lovgivning på området, feks. markedsføringsloven, registerloven og bogføringsloven.

Virksomheden bør også have nogle klare forholdsregler om hvordan man håndterer situationen når en medarbejder slutter sin ansættelse, enten ved selv at have opsagt sin stilling eller pga. opsigelse fra virksomhedens side.

Skal medarbejderen øjeblikkeligt bortvises, omplaceres til mindre følsomme arbejdsområder, have frataget nøgler, sikkerhedskoder mv. eller ???

Ansvar og organisation / Husets arbejdsgange og sikkerheden:

Det vil altid være en god ide at have udarbejdet en sikkerhedsinstruks for håndtering og opbevaring af data, således at ingen er i tvivl.

Feks. kan retningslinierne indeholde punkter som:

- **Organisation/sikkerhedsansvarlig(e)**
- **Adgang til virksomheden, kontorer og maskinrum**
- **Kontrol af sikkerheden iforb. med programudviklingen**
- **Kontroller som skal indbygges i applikationer**
- **Kontrol af sikkerheden iforb. med driftafviklingen**
- **Dokumentklassifikation/håndtering/opbevaring**
- **Klassifikation af databærende medier**
- **Regler for tildeling, brug og udskiftning af kodeord**
- **Regler for sikring af, og kontrol af, dataintegritet**
- **Generelle kontrol- og revisionsrutiner.**
- **Rapportering og aktioner iforb. med sikkerhedsbrud**

.... og hvad hjælper så al den megen sikring af edb-udstyret og data, hvis 'hvem som helst' kan trænge ind og fjerne eller ødelægge udstyret ?

Se Appendix med oplæg til en SIKKERHEDSHÅNDBOG.

Selvom denne bog handler om edb-sikkerhed, data-sikkerhed og data-sikring må det erkendes, at

GENEREL ADGANGSSIKRING OG ALARMERING

trods alt også er grundlaget for effektiv edb-og data-sikring !

Ansvar og organisation / Revisoren og EDB-revisoren:

Nogle virksomhedsledere mener, at når revisoren har sagt god for sikkerheden, er alt ok.

Revisionsvirksomhederne kontrollerer om data behandles og beskyttes jvf. bogførings- og registerlovens forskrifter, og om de nødvendige transaktionsspor og revisionsspor er intakte.

Men derfra til at erklære, at edb- og datasikkerheden er ok kan der være meget langt !

De statsautoriserede revisorer arbejder ud fra 2 vejledninger:

Vejledning nr 14:

Vejledning om revision i virksomheder, som anvender edb.

Revisors undersøgelse af en virksomheds edb-anvendelse kan normalt opdeles i

- indledende vurdering af edb-anvendelsen
- gennemgang af generelle edb-kontroller
- gennemgang af kontroller i brugersystemer

hvor sidstnævnte er udmøntet i

Vejledning nr. 17:

Vejledning om revision af edb-baserede brugersystemer

Men der er næppe mange revisionsvirksomheder som har tilstrækkelig edb-mæssig ekspertise indenfor alle tekniske platforme med et samtidigt kendskab til markedets mange muligheder for, og produkter til, sikring af udstyr og data.

EDB-revisoren er ikke et alternativ, men et supplement til den statsautoriserede revisor.

Juridiske forhold / Piratkopiering:

Pirat-kopiering handler om Ophavsretslovens bestemmelser, hvor konsekvenserne ved overtrædelse kan blive ret omfattende med både bøder og erstatninger og evt. beslaglæggelse af edb-udstyr.

EDB-programmer er direkte nævnt i loven.

PC-programmer er en vare som så meget andet og må ikke kopieres og bruges uden at der er betalt for det.

Desværre er det alt for let at kopiere programmer for mindre formuer, og nogle lader sig bevidst friste, mens andre tænker for lidt over have de egentlig foretager sig.

Der opstår flere uheldige konsekvenser af ulovlig kopiering:

- **Leverandøren/udvikleren mister penge på det, penge som bla. skulle have været brugt til programmets fortsdatte uvedligeholdelse og udbygning.**

- **Den virksomhed som bliver taget i pirat-kopiering, fordi en lidt for smart medarbejder ville undgå bureukratiet og budgetterne, kommer på forsiden af Ekstrabladet !**

- **Virksomheden bliver pålagt en større bøde for ulovligheden og en pæn stor erstatning til udvikleren.**

Pirat-kopiering falder i alle tilfælde

tilbage på 'piraten'.

Ulovlig kopiering, tyveri af PC-programmer, er en kriminel aktivitet helt på linie med at stjæle fra cigaret-automaten eller i supermarkedet.

Juridiske forhold / Licensregler:

PC-programmer er normalt købt og beregnet til brug på een PC ad gangen. Dvs. at man nødvendigvis må af-installere og ny-installere på en anden PC, hvis det skal bruges mere end eet sted.

Den eneste kopiering der lovligt må foretages er, en sikkerhedskopi. Hvis programmet videresælges skal alle sikkerhedskopier følge med - eller slettes fuldstændigt.

Flere software-leverandører tillader dog at en medarbejder må lægge samme program på sin private PC, hvis det er også er nødvendigt at arbejde med firmaets opgaver derhjemme.

Licens-tilladelserne er givet ud fra den betragtning, at den samme person netop kun arbejder eet sted ad gangen.

Det er altså ikke tilladt, at lade familien hjemme benytte tekstbehandlingsprogrammet samtidig med at mor elle far bruger den tilsvarende licens inde på arbejdet !

HUSK !

Ulovlig kopiering, tyveri af PC-programmer, er kriminelt.

VIGTIGT !

Før kontrol, manuelt eller maskinelt, med firmaets licenser, og slå hårdt ned på de medarbejdere der overtræder licens-reglerne.

Juridiske forhold / Hvem ejer data ?

Både programmer og data skabt i virksomheden af den ansatte ejes af virksomheden, hvis ikke andet er aftalt.

Nogle egen-udviklede programmer har en vis handelsværdi, men den største handelsværdi ligger primært i data-registrene, feks.

* **Kunderegistre**
* **Strategiplaner**
* **Udviklingsresultater**
* **Kalkulationsmodeller**

Alt sammen information som konkurrerende virksomheder kan få stor gavn af at kende, og som kan påføre ejeren store tab hvis de forvanskes eller mistes.

Ikke kun de direkte omkostninger, men i høj grad de afledte til gen-skabelse, som i værste fald skal ske helt fra bunden af hvis det overhovedet er muligt.

Her er man underlagt "Markedsføringloven's" paragraffer om indsigt og videregivelse af fortrolige informationer. Og videregivelse eller misbrug er klart ulovligt.

Eksempelvis kørte der en sag medio 1993, hvor en medarbejder fik et nyt job hos konkurrenten - og tog kunderegistret med sig fra sin gamle arbejdsplads.

Det var et par kunder som slog alarm ! De undrede sig over, at den samme stavefejl i deres navn forekom på breve fra begge de konkurrerende firmaer.

Den pågældende medarbejder forsøgte sig med en undskyldning om, at de fleste kundeinformatiner var medtaget fra en endnu tidligere arbejdsplads ! Den ene ulovlighed undskyldt med en anden !

Af forskellig grunde endte sagen med en slags forlig, hvor de nyeste arbejdsgiver måtte slette nogle kundedata, men sagen kunne meget vel have endt med erstatningskrav fra begge tidligere arbejdsgivere.

Der er faldet dom i andre sager, hvor medarbejdere forlod en virksomhed med kopier af planer og konstruktioner, for at starte egen virksomhed op på tilsvarende produkter.

HUSK !

Det er lige ulovligt hvad enten informationerne befinder sig på et edb-medie eller som foto-kopier.

Juridiske forhold / Udvikling og kildekode:

Når en kunde lader et specialprogram udvikle i et såkaldt software-hus er det sjældent at kildekoden overlades til kunden, kildekoden er omfattet af Oprethavsloven som et kreativt skabt værk på linie med en bog, en sang og et musikstykke.

Nu skriver de fleste forfattere selv deres bøger og det får ikke de store konsekvenser for et orkester, hvis en komponist må opgive inden musikværket er færdigskrevet, men når det gælder udvikling af specialsoftware står der ofte store summer på spil, hvis software-huset går konkurs.

Først er de penge tabt, som evt. er indbetalt løbende for et program som hverken er helt eller halvt færdigt, og dels de udgifter der er forbundet med ikke at kunne benytte programmet til det, som skulle have givet større effektivitet eller direkte besparelser i arbejdet.

Og derefter nye udgifter hvis andre skal forsøge at overtage det fallerede projekt - hvis det er muligt.

Som verden ser ud nu, er det altid en god idé at sikre sig løbende deponering af kildekoden hos en uvildig instans, så andre kan fortsætte arbejdet hvis udvikleren går konkurs.

Medio 1993 etablerede DTI i Århus et sådan depot.

Dansk Deponerings Institut
Dansk Teknologisk Institut
Teknologiparken
8000 Århus C *Tlf. 8614 2400*

Deponeringsinstituttet leverer det nødvendige kontraktmateriale, sikkerhed for udlevering når det er nødvendigt, sikkerhed mod uberettiget udlevering, sikker opbevaring, kontrol med opdatering mm.

Vilkårene udformes i samrbejde med instituttets medarbejdere.

Risiko og konsekvens:

Vi kan naturligvis være bange for alting og sikre os så omstændigt, at der reelt ikke kan udføres nogen form for normalt arbejde - men det er jo nok at skyde over målet eller helt forbi !

Det bedste er at skabe sit eget risiko-billede, dvs. nøgternt at identificere de risici, som kan være aktuelle for netop vores virksomhed. Hvad bør vi reelt frygte ?

Ligger virksomheden lavt kunne det være oversvømmelse, er vi nabo til en krudtfabrik kunne det være eksplosion, ligger vi i et mørkt industrikvarter kunne det være indbrud og hærværk, udvikler vi højteknologiske produkter skal vi måske være bange for konkurrentindsigt osv. osv.

Blandt de reelle risici vil der yderligere kunne vægtes og prioriteres, ligesom der vil kunne sættes konsekvenser på bla. iform af direkte og indirekte omkostninger.

Risiko og konsekvens:

TRUSSELS-BILLEDE:

TRUSSEL	HVORFOR	SANDSYNLIGHED
Brand	Brandbare emner på lager	Medium
Vandskade	Lav beliggenhed	Lille
Indbrud/ tyveri	**Bor afsides, ingen trafik efter fyraften, let adgang Attraktive maskiner**	**Stor <------**
Hærværk		Lille
osv.		

HVAD KAN SKE VED:	FRYGT FOR:	KONSEKVENS:
Indbrud/ tyveri	PC'erne stjæles med alle data ombord.	Ingen kontrol over produktion, lager, køb og salg i ca. 1 uge
	Kun PC-1 stjæles	Ingen. Data kan re-stores andetsteds på 1/2 time.
osv.		

OMKOSTNINGER:

Indbrud	PC'erne stjæles med alle data ombord.	5 x 5 dages løn + 2 x 2 dages overarbejde + rentetab på indbetalinger + rentetab på udbetalinger + bonus-tab på forsikring. Ialt. ca. 125.000,- kr.
	Kun PC-1 stjæles	Ingen nævneværdige.
osv.		

Risiko og konsekvens:

TRUSSELS-BILLEDE:

TRUSSEL	DATA-REGISTER	SAND-SYNLIGHED	GENSKABELSES MULIGHED
Data-tab	Kunde-register	Medium	Re-store - 5 dg
Data-tab	Debitor-register	Medium	Re-store - 2 dg
Data-tab	Kreditor-register	Medium	Re-store - 2 dg
Data-tab	Lager-system	Medium	Re-store - 5 dg
Forvanskning	Kunderegister	Stor	Mangler bilag
Forvanskning	Debitor-register	Lille	Bilag findes
Forvanskning	Kreditor-register	Medium	Bilag findes
Forvanskning	Lager-system	Stor	Bilag findes eller skaffes

osv. .....

Der er mange måder at gøre det på, flere modeller - men det vigtigste er:

FÅ DET GJORT !

APPENDIX A / Oplæg til Sikkerhedshåndbog

Følgende skal betragtes som et oplæg, et forslag, og ikke som en patentløsning.

Det er ikke overskrifterne der giver arbejdet eller vanskelighederne; det er beskrivelsen og ikke mindst at opnå enighed om, og at få gennemført procedurerne !

Forord:

Det er hensigten med denne håndbog, at .....

.....

Formålet med håndbogen, samt de deraf følgende tiltag er at sikre en pålidelig drift af virksomhedens systemer, at undgå tab af virksomhedens data, at sikre uvedkommendes adgang til systemer og data, samt at sikre medarbejderne mod ved fejl eller uheld at ødelægge eller forvanske data på en måde så de ikke kan genskabes.

Mere operationelt er formålet at give hver enkelt medarbejder en instruks for, hvorledes hun eller han skal administrere den PC eller arbejdsstation, som er stillet til rådighed, samt give et indblik i, hvorledes virksomheden som helhed driver sine edb-systemer.

Edb-Sikkerhedshåndbogen er et internt dokument, der kun efter aftale med .....kan forevises til .....

..... er ansvarlig for løbende opdatering, som vil ske .....

Ved opdateringer vil ændringer i forhold til tidligere udgave være markeret med .....

APPENDIX A / Oplæg til Sikkerhedshåndbog

Indhold:

Virksomhedens sikkerhedspolitik

Virksomhednes sikkerhedsorganisation

Risici og konsekvenser

Fysiske forhold - skal-sikring

Adgangsforhold - bygning

Fysiske forhold - EDB-afd / EDB-rum

Adgangsforhold - EDB-afd / EDB-rum

Driftmæssig sikring af centralt edb-udstyr

Logisk sikring af centralt edb-udstyr

Logisk sikring af PC-udstyr - Stationært

Sikring af PC-udstyr - Bærbart

Sikkerhedskopiering/Back-up

Håndtering af data-medier

Sikring af kommunikationslinier

Nødplaner

Personale

Konsulenter/teknikere

Lovgivningen

Forsikringer

APPENDIX B / Litteraturoversigt:

Litteratur, bla.:

EDB-ret for brugere
Mads Bryde Andersen / Teknisk Forlag 1987

EDB Sikkerhed
Lars Frank / Samfundslitteratur 1987

Sikkert
Anders Djurså & Torsten Madsen / Kommunedata's Forlag 1991

Bogen om computervirus
Jonathan L. Mayo / Teknisk Forlag 1989

Tyveri på arbejdspladsen
Ole Chr. Larsen & Stig W. Smith 1992

Markedsføringsloven
Jesper Møller-Andersen / Erhvervs-Bladets Jurabøger 1992

Den sårbare virksomhed
Dansk Arbejdsgiverforening 1993

Murphy's Computerlove
Joachim Graf / Borgen 1992