OPERATOR CONSULT ApS
Mac Donald Allé 23 • 2750 Ballerup • Tlf.: 44 65 39 44 • Giro: 4 89 17 16 • Reg. nr. 111.092

# Noter

**til en**

# EDB-RISIKO- &

# SÅRBARHEDSANALYSE

*Copyright (C)*
Poul Badura,
*Operator Consult ApS*
*1996, 1997*

# Indledning

**RISIKOANALYSE OG SÅRBARHEDSANALYSE** er to sider af samme sag - og der vil uden tvivl kunne findes mange forskellige definitioner på både den ene og den anden

Så ikke mindst derfor må det være på sin plads her at skrive endnu en definition således, at læserne i denne sammenhæng har samme referenceramme.

**RISIKO-ANALYSEN**, som her opdeles i 2 faser omfatter den fysiske og tekniske gennemgang af virksomhedens edb-anvendelse - fra de fysiske bygningsmæssige rammer til organisation og personale, samt interview med virksomhedens ledere og udvalgte medarbejdere.

Gennemgangen vil udpege de svage punkter, hvor der eksisterer en risiko (set med drifttekniske briller) for at en negativ hændelse kan forekomme - med større eller mindre konsekvenser til følge for drift og/eller data.

Der tages i denne afdeling ikke specielt hensyn til sandsynligheden for at hændelsen rent faktisk indtræffer eller for de forretningsmæssige konsekvenser som en sådan hændelse vil påføre virksomheden.

I **Fase-1** foretages:

- **en fysisk inspektion af bygninger og lokaler,**
- **en fysisk inspektion af edb-rum og -maskiner**
- **inspektion af systemopsætning og dokumentation**
- **interview's med ledere og medarbejdere i virksomhedens berørte afdelinger.**

I **Fase-2**

- **analyseres risiciene og de drifttekniske konsekvenser.**

I det omfang det er muligt bør man påføre forslag til afdækning af de anførte risici een for een, (ref. Appendix) men samtidig være opmærksom på, at der på dette tidspunkt ikke er det store overblik over situationen, og at løsningsforslagene kun er vejledende til evt. senere diskussion og vurdering.

# Indledning

**SÅRBARHEDSANALYSEN** omfatter kun een enkelt fase, her kaldet Fase-3 i det samlede forløb.

**Fase-3** er:

- **den egentlige vurdering af, hvor sårbar virksomheden forretningsmæssigt er overfor en given hændelse, som en beregnet konsekvens af sandsynligheden for forekomst og den deraf afledte konsekvens.**

**IMPLEMENTERING**

Om det skal med under sårbarhedsanalysen som en fase, eller om det skal fremstå som et selvstændigt hovedpunkt bliver en strid om ord. Her betragtes IMPLEMENTERING som et selvstændigt punkt, kaldet Fase-4 i det samlede forløb.

**Fase-4:**

Resultaterne fra både Risiko- og Sårbarhedsanalysen skal danne grundlag for cost/benefit-beregninger med efterfølgende stillingtagen til:

- **prioriteret valg af løsninger**
- **budgettering**
- **tids- og ressourceplanlægning**

# Indledning

På de følgende sider findes oplæg til en række inspektionspunkter samt en lang række spørgsmål som kontrolpunkter for en risiko-gennemgang.

Vi gør her opmærksom på, at det på ingen måde er fulddækkende, men skal opfattes som et skelet man i den enkelte virksomhed kan bygge videre på.

Hvis virksomhedens aktiviteter er spredte over flere adresser (fabrikker i 3 byer eller kommunale forvaltninger rundt i kommunen) skal mange af spørgsmålene stilles for hver fysiske lokation.

Der findes på markedet adskillige bøger og edb-systemer med tilsvarende og lignende spørgsmål, men i alle tilfælde gælder, at ingen er fulddækkende, mange er for omstændelige så man gennem mere end tusinde spørgsmål mister ethvert overblik, og ingen passer 100% til den enkelte virksomhed.

I alle tilfælde er det nødvendigt, at undersøgeren bruger sin sunde fornuft, lytter, observerer og på stedet stiller yderligere spørgsmål til uddybning af observationer og svar, altså spørgsmål man ikke nødvendigvis ville kunne have forberedt.

Gennemgangen kan naturligvis foretages på flere niveauer afhængig af behov.
F.eks. kan man nøjes med en "temperaturtagning" på sikkerheden som udgangspunkt for udarbejdelse af en edb-sikkerhedspolitik, mens man må noget dybere til værks for efterfølgende at kunne udarbejde en "differenceliste" mellem den formelle edb-sikkerhedspolitik og de faktiske forhold.

De efterfølgende overskrifter og spørgsmål følger nøje Operator Consult's "Noter til en edb-sikkerhedspolitik" (for konsistensens skyld), som her er suppleret med både teoretiske betragtninger og oplevelser fra det virkelige liv.

# Fase-1:

## Fysisk inspektion af bygninger og lokaler:

Det er naturligvis nødvendigt at gå en tur gennem virksomheden og foretage en generel vurdering af mulighederne for

- **illegal indtrængen**
- **tyveri og/eller hærværk**
- **vandskader**
- **ildebrand**
- **andre forhold som kan skade virksomheden/driften**

F.eks. kan illegal indtrængen sagtens foregå i arbejdstiden ved at besøgende har fri adgang fra receptionsområdet til andre dele af bygningen, måske fordi der ikke foregår en formel modtagelse og indskrivning af gæster, gæsterne forsynes ikke med ID-kort og døre mellem 'ankomsthal' og øvrige dele af bygningen er ikke aflåste.

Det kan lige såvel være omhandle uhindret adgang til virksomhedens varelager fra læsseramper og vareindlevering. Fremmede chauffører og vognmænd kan uhindret bevæge sig rundt.

I begge tilfælde kan virksomheden være udsat for risiko for direkte tyveri eller for indirekte tyveri ved, at de besøgende fortæller videre om de mange herligheder der gemmer sig i kontorerne og på lageret.

Inspektionen bør også omfatte

- **porte,**
- **døre,**
- **vinduer,**
- **låse,**
- **adgangssystemer,**
- **overvågning og alarmer.**

Det handler om kvalitet, placering og afprøvning.

F.eks. er det set at vinduer har været forsynet med alarmfolie, men virksomheden havde opsagt abonnementet til alarmcentralen !

I en anden sag havde håndværkere monteret et kraftigt ventilationssystem på en måde så enhver form for røg blev blæst bort fra brandmelderne (røgmeldere).

Ref. Appendix for flere eksempler fra 'det virkelige liv'.

# Fysisk inspektion af edb-rum og -maskiner:

Inspektionen omhandler edb-rum og edb-afdelingens lokaler, hvor man bl.a. hurtigt vil få et overordnet indtryk af, om rummene er velordnede, rene og om placeringen af edb-udstyr er hensigtsmæssig i relation til mulighederne for indbrud, tyveri, vand- og brandskader.

Flyder det f.eks. med papkasser, kabler og kredsløbskort er der stor sandsynlighed for, at der heller ikke er orden i andre forhold.

Man bør bl.a. kontrollere om

- **edb-udstyret er placeret lige indfor et vindue,**
- **er der frit indsyn,**
- **er vinduet sikret med gitre og/eller alarmer,**
- **går det vandrør direkte over edb-udstyr og/eller kabelsamlinger,**
- **er der gulvafløb,**
- **er der grundvandspumpe,**
- **er der overløbsalarm osv.**
- **er der nødstrøm**
- **andet**

Kort og godt: Er der risiko for, at edb-udstyret blive udsat for fysiske skader og nedbrud på grund af placering og/eller risici påført fra andet udstyr i rummet, eller ved fremmedes ind trængen.

Ref. Appendix for eksempler fra 'det virkelige liv'.

## Inspektion af systemopsætning og dokumentation:

Som en del af gennemgangen er det relevant, sammen med den systemansvarlige, at gennemgå driftsystemernes opsætningsparametre i relation til edb- og datasikkerheden.

Det letteste vil være at få en udskrift af systemparametrene.

I det omfang enten edb-afdelingen eller inspektionen råder over Audit-/Revisionsprogrammer kan man med fordel køre disse og få klar dokumentation på sagen.

F.eks. vil et produkt som PC-UNIX Audit hurtigt afsløre manglende konsistens i de sikkerhedsmæssige opsætninger gennem mere end 80 forskellige analyser af UNIX-opsætningerne.

Det kunne f.eks. være:

- **bruger-identer uden gruppetilknytning**
- **grupper uden bruger-identer**
- **for korte password**
- **bruger-id's ikke brugt de seneste 100 dage**
- **brugere uden home directory**
- **osv.**

Andre og lignende produkter gør tilsvarende på andre systemtekniske platforme.

Inspektionen omfatter også dokumentation af:

- **konfigurationen,**
- **driftvejledninger,**
- **forretningsgange for brugeradministration,**
- **testregler i forb. med maskininstallationer**
- **testregler i forb. med program- og systeminstallationer**
- **serviceaftaler,**
- **forsikringer**

og andet, som kan påvirke de sikkerhedsmæssige og forretningsmæssige aspekter - positivt ved sin tilstedeværelse og aktualitet - og negativt ved sin manglende eksistens eller ufuldstændige udformning og eventuelle manglende vedligeholdelse.

# Interview's med ledere og medarbejdere

Under den fysiske rundgang og inspektion vil det være hensigtsmæssigt samtidig at tage en lille 'snak' med de mennesker man møder rundt i afdelingerne, for bl.a. at danne sig et indtryk af deres kendskab til og viden om edb- og datasikkerhed (regler/retningslinier) her i virksomheden.

- **Er der rent faktisk trængt information ud i de yderste led til slutbrugerne ?**
- **Har slutbrugerne en fornemmelse for alvoren bag edb- og datasikkerhed ?**
- **Er de bekendt med de eventuelle mangeler man netop har konstateret ?**

Det er vigtigt ikke at lyde nedladende eller inkvisitiv i denne sammenhæng. Interview og samtaler må på ingen måde få anstrøg af anklager, men skal tværtimod afvikles i en hjælpsom, vejledende toneart med henblik på bedre regler, procedurer og fælles fodslag i virksomheden.

Samtalerne vil kunne give en retningspil for hvem der er (eller føler sig) ansvarlige for hvad og hvor travlt man har (så sikkerheden svigtes !) og afsløre eventuelle besværlige forretningsgange og procedurer som direkte afholder medarbejderne fra at overholde ellers fornuftige sikkerhedsregler.

De følgende mange spørgsmål skal betragtes som et udgangspunkt for de løse samtaler og de mere formelle interview med chefer, ledere, sikkerhedsadministratorer, edb-folk og andre interessenter i virksomhedens sikkerhedsmæssige forhold.

Stil gerne supplerende spørgsmål til underbygning af svarene.

## Virksomhedens edb-sikkerhedspolitik:

På overordnet niveau er det rimeligt at spørge:

- **Har virksomheden udarbejdet en formel skriftlig edb-strategi f.eks. for de kommende 2 - 5 år ?**
- **Indgår edb-sikkerhed som et klart element i den overordnede edb-strategi ?**
- **Har virksomheden udarbejdet en formel og skriftlig edb-sikkerhedspolitik for det/de eksisterende system/systemer ?**
- **Foretages der en samtidig revision af begge, eller halter edb-sikkerhedspolitiken bagud ?**
- **Gælder edb-sikkerhedspolitiken kun for edb-afdelingen eller gælder den for alle virksomhedens afdelinger og filialer i både ind- og udland ?**
- **Er edb-sikkerhedspolitiken grundigt formidlet ud blandt medarbejderne - og hvordan ?**
- **Fremstår edb-sikkerhed som et selvstændigt punkt i budgetterne under edb-omkostninger eller forsikringer - eller slet ikke ?**
- **Er der på noget tidspunkt udført en egentlig risiko- og/eller sårbarhedsanalyse i forb. med virksomhedens afhængighed af edb ? Hvornår ?**
- **Er der udarbejdet sikkerhedspolitikker for andre af virksomhedens forhold, afdelinger, produktioner m.fl. ?**
- **Er der udarbejdet nogen form for beredskabsplan for dele af, eller for hele virksomheden ?**
- **Har virksomheden nogen sinde afprøvet sit beredskab ?**

Spørgsmålene stilles bl.a. for at afdække om topledelsen er/har været involveret og i hvilket omfang edb- og datasikkerhed har ledelsens bevågenhed i det daglige.

Er der for mange negative svar bør man overveje hvor seriøst indeværende arbejde vil blive behandlet og hvilken effekt det evt. vil få i organisationen. Er det f.eks. et skinprojekt ?

På de spørgsmål, hvor der kan svares bekræftende, er det vigtigt at fremskaffe dokumentationen og konstatere dens omfang, niveau og kvalitet.

## Virksomhedens edb-sikkerhedsorganisation:

Her skal man afdække om virksomhedens har etableret klare ansvarsområder og pligter for diverse chefer, afdelinger og grupper f.eks. i relation til Registerloven og Bogføringsloven og samtidig finde ud af, om eventuelle overtrædelser af edb-sikkerheden rapporteres, hvordan og til hvem.

- **Fremstår der en klar organisationsstruktur i al almindelighed ?**
- **Fremgår det af organisationsstrukturen hvem (funktion) der er ansvarlig for, og hvem der er udførende/administrerer edb-sikkerheden - centralt og decentralt ?**
- **Fremgår det klart af stillingsbeskrivelser eller andet hvilket ansvar og pligter der er forbundet med opgaven ?**
- **Er der etableret et egentligt sikkerhedsforum som afholder regelmæssige møder, eller indgår diskussioner om sikkerhed/edb-sikkerhed uformelt/ustruktureret i anden mødesammenhæng ?**
- **Hvordan koordineres sikkerhedsmæssige forhold mellem virksomhedens afdelinger ?**
- **Fremgår det af organisationsstrukturen og/eller andre beskrivelser, hvem der er ansvarlig for og hvem der er udførende af daglige og periodiske kontroller , og hvordan ?**
- **Rapporteres overtrædelser af edb-sikkerhedspolitik og -regler formelt ?**
- **Findes der regler for under hvilke forhold, og af hvem, evt. anmeldelse til politi af sikkerhedsbrud udefra skal foretages ?**
- **Findes der regler for under hvilke forhold, og af hvem, evt. anmeldelse til politi af sikkerhedsbrud indefra skal foretages ?**

# Virksomhedens edb-sikkerhedsorganisation:

Virksomhederne har ofte mere end eet styresystem/operativsystem indenfor de(t) lokale netværk plus at der ofte er adgang til andre systemer (f.eks. Kommunedata, Datacentralen, Post Danmark, bankerne m.fl.)

- **Hvordan er forretningsgangene for administration af brugere op mod det enkelte system ? Spørgsmålet omfatter: Oprettelse, tildeling af rettigheder og autorisationer, ændring af disse, flytning af brugere, password-administration, sletning mv.**
- **Hvilke funktion/person udfører i praksis dette arbejde ?**
- **Er forretningsgangene tilstrækkeligt beskrevet ?**
- **Hvordan sikrer man at der ikke sker fejl ? Kontrolmuligheder og kontroller.**

# Personalepolitik og edb-sikkerhed

Personalepolitikken er en vigtig del af edb-sikkerheden.

Man kan naturlig vælge om diverse forhold skal beskrives det ene eller det andet sted, men det væsentlige må være, at der har været en diskussion om sagen, at der er taget stilling fra virksomhedens side, og at det er nedfældet et eller andet sted.

- **Findes der en formel og skriftlig personalepolitik i virksomheden i dag ?**

CLEARING:

- **Er der i forbindelse med ansættelseskriterier, udvælgelse mv. taget stilling til clearing af personale - specielt i relation til edb-stillinger, hvor der kan forekomme adgang til følsomme og kritiske maskiner, systemer og data ?**

- **Tages man referencer til tidl. arbejdspladser, forlanger man straffeattest mv. ?**

- **Hvor ofte udføres der en personalevurdering/kontrol i relation til clearing ?**

TAVSHEDSPLIGT

- **Gøres nye medarbejdere opmærksom på deres ansvar og pligter omkring beskyttelse af virksomhedens informationsmæssige aktiver, f.eks. ved at underskrive tavshedserklæringer, indgå konkurrenceklausuler el. tilsv. ?**

UDDANNELSE

- **Gennemgår nye medarbejdere nogen form for introduktionskursus om virksomhedens formål, forhold, kultur mv. - og indgår emnet sikkerhed/edb-sikkerhed i dette ?**

- **Modtager medarbejderne information om, hvordan de skal forholde sig hvis de får mistanke om fremmede eller kollegers uretmæssige adgang og anvendelse af edb-systemer og data ?**

NØGLEPERSONER

- **Pålægges chefer og ledere at undgå at skabe nøglepersoner indenfor særligt følsomme og sårbare forretningsområder.**

# Personalepolitik og edb-sikkerhed

**VIKARER/AFLØSERE:**

- **Har virksomheden er særlig politik omkring anvendelse af vikarer, afløsere mv. specielt i relation til arbejde med særligt følsomme emner og/eller i særligt følsomme områder ?**

**OPSIGELSE/FRATRÆDELSE**

- **Findes der regler og procedurer for ændring af password og andre adgangskoder, overtagelse/overdragelse af data på den pågældende's PC, afkryptering af evt. krypterede filer, fratagelse af nøgler, følgen til porten m.v. når en medarbejder fratræder efter eget valg ?**

- **Findes der regler og procedurer for ændring af password og andre adgangskoder, overtagelse/overdragelse af data på den pågældende's PC, afkryptering af evt. krypterede filer, fratagelse af nøgler, følgen til porten m.v. når en medarbejder fratræder efter virksomhedens valg ?**

**KONSEKVENSER**

- **Har man taget stilling til konsekvenser for medarbejdere, som overtræder gældende regler og retningslinier inden for området edb- og datasikkerhed ?**

Man skal være opmærksom på, at negative svar ikke nødvendigvis indikerer stor risiko for virksomheden og dens anvendelse af edb.

Risikoen skal ses i relation til de opgaver der udføres i de enkelte afdelinger, sårbarheden mv.

## Teknikere, håndværkere, konsulenter m.fl.

Har virksomheden taget stilling til, hvordan den vil håndtere fremmedes (ikke ansattes) gøren og laden på virksomhedens område i samarbejde med ansatte medarbejdere og/eller når teknikere, konsulenter og håndværkere skal udføre selvstændigt arbejde for virksomheden.

Bemærk at rengøringspersonale og vikarer behandles særskilt på baggrund af deres særlige roller og arbejdsforhold i virksomheden.

- **Bærer virksomhedens medarbejdere tydelige identitetskort eller tilsvarende ?**
- **Findes der forretningsgange for hvor og hvornår håndværkere, teknikere, konsulenter m.fl. har adgang til virksomhedens specielt følsomme områder - og registreres det nogen steder hvornår de går ind og ud af virksomheden ?**
- **Giver man teknikere, håndværkere, konsulenter og andre gæster tydelige identitetskort ved ankomst i receptionen ?**
- **Er man altid bekendt med håndværkere, teknikeres, konsulenters og andres ankomst til virksomheden , eller kommer de nogle gange uanmeldt ?**
- **Foreligger der altid en formel godkendelse fra en chef eller leder til det arbejde der skal udføres ?**
- **Er man altid bekendt med formål, tidsforbrug og konsekvenser af det forestående arbejde ?**
- **Har man regler/retningslinier for, ved hvilke typer arbejder en af virksomhedens medarbejdere skal være til stede for at kunne gribe ind ?**
- **Har tekniker og konsulenter deres egne password til systemerne eller får de udleveret et eengangs-password ?**
- **Har man regler for adgang til 'fremmede' teknikere, konsulenter og håndværkere - altså personer som ikke normalt servicerer virksomheden ?**

## Vikarer og erhvervspraktikanter:

Vikarer udgør en særlig gruppe, da de ofte med meget kort varsel skal springe ind og erstatte jobbet for en fast ansat. Nogle virksomheder hyrer vikarer fra bureauer, andre har selv en tilkaldeliste over rådighedsmedarbejdere. Hvor kendte er disse mennesker i organisationen ? Og hvor frit får de lov at bevæge sig rundt i organisationen og i diverse edb-systemer ?

- **Benytter virksomheden sig periodisk af vikarer ? Fra bureau eller ... ?**
- **Eksisterer der en eller anden clearingprocedure for disse i det omfang de skal arbejde i særligt følsomme områder og/eller med særligt følsomme data ?**
- **Hvordan er procedurerne for vikarer's adgang til edb-systemerne ? Overtager de den faste medarbejders brugerprofil og/eller tildeles de særlige/begrænsede brugerprofiler i edb-systemerne ?**
- **Hvem afgører hvilke informationer de må få adgang til ?**
- **Af hvem og hvordan kontrolleres netop vikarers gøren og laden - også i edb-systemerne ?**

Erhvervspraktikanter og/eller udvekslingsstudenter (forskningsstipendiater) er en anden gruppe, som får adgang indenfor murene. Meningen er, som med vikarer, at de skal deltage i det daglige arbejde i et eller andet omfang, og det kræver både fysisk adgang til en række områder og lokaler i virksomheden, og adgang til edb-systemer og data.

Hvorvidt er disse forhold beskrevet, styret og kontrolleret ?

- **Hvem afgører hvem, hvor og hvornår erhvervspraktikanter er velkomne ?**
- **Knytter man altid en ansvarlig person sammen med erhvervspraktikanterne ?**
- **Er der regler/retningslinier for, hvor praktikanterne må bevæge sig rundt, skal de være i følge med andre, og kan de identificeres og kontrolleres med nøglekort el. lign. ?**
- **Informeres erhvervspraktikanter om virksomheden og forholdene inden de 'slippes løs' i virksomheden ? Og af hvem ?**
- **Er der regler/retningslinier for, hvad medarbejderne må udlevere til erhvervspraktikanter (kopier på papir og/eller disketter) ?**

# Rengøringspersonale

Rengøringspersonale udgør en særlig risiko såvel mod den fysiske som den logiske sikkerhed, dels fordi de arbejder i virksomheden på tidspunkter, hvor virksomheden normalt ikke er bemandet, dels fordi der ofte forekommer en stor udskiftning blandt rengøringsmedarbejdere, og dels fordi rengøringsmedarbejdere typisk er en blanding af folk med alle mulige baggrunde, heraf mange studerende indenfor områder som edb og elektronik.

Naturligvis skal denne gruppe ikke hænges ud som særligt suspekte, men med baggrund i foranstående er det relevant at kende situationen - for at kunne vurdere risikoen.

- **Benytter virksomheden egne fast ansatte rengøringsmedarbejdere, eller har man entreret med et eksternt rengøringsfirma ?**
- **Foretager man, el. stiller man krav til, en særlig clearing af disse medarbejdere ?**
- **Stiller man krav om faste rengøringsfolk fra eksterne leverandører ?**
- **Gøres disse medarbejdere særligt opmærksom på virksomhedens forventninger om gøren og laden i virksomhedens lokaler, brug af virksomhedens maskiner og hemmeligholdelse af evt. opsnappet information ?**
- **Har man regler for adgang til afløsere for de faste rengøringsfolk - altså personer som ikke normalt servicerer virksomheden ?**
- **Har man etableret særlige regler for rengøring af centrale edb-rum, installationsrum og rum med virksomhedens telefoncentral ?**

# Fysiske forhold: Skalsikring:

Her er vi ovre i den fysiske inspektion af bygninger og lokaler.

For virksomheder med egen grund starter inspektionen med perimetersikringen, dvs. hegn, porte, buskadser, trægrupper ved bygning osv.

Herefter arbejder man sig ind mod og ind i bygningen for at konstatere adgangsvejs for medarbejdere og leverandører, dør- og vinduessikring med låse og alarmer, sektionerede bygninger, medarbejderes og fremmedes adgang rundt i virksomhedens afdelinger mv.

**PERIMETERSIKRING:**

- **Er virksomheden omkranset af et hegn (tråd, mure, buskadser, træer mv.) og kan det modstå fysisk indtrængen af personer, alm. biler, lastvogne, entreprenørmaskiner ? Identifikation af de(t) svageste sted(er).**

- **Er virksomheden omkranset af buske, buskadser, trægrupper el. tilsv. tæt på bygningerne, som gør det muligt for indtrængende at skjule sine aktiviteter mod opdagelse af forbipasserende, vægtere m.fl. ?**

- **Forefindes der store træer og/eller findes der paller, tønder eller andet materiale, som indtrængende kan benytte som trappe for at opnå adgang gennem vinduer over stueplan ?**

- **Har virksomheden opsat eksterne projektører og/eller etableret kameraovervågning af de ydre områder, lagerplads mv. ?**

- **Har man etableret en vægterordning ? Hvornår og hvordan fungerer den, og til hvem, hvordan og hvornår rapporteres der ?**

# Fysiske forhold: Skalsikring:

## DØRE, LÅSE OG VINDUER

- **Er de normale adgangsveje til bygningerne sikret med opbygning og låse jvf. SKAFOR klassificeringerne ?**
- **Fysisk inspektion af alle yderdøre og porte. Kontrol af karmkvalitet, dørkvalitet (glasdøre/glaspartier ?), låsetøjer/låsesystemer, sluser ved lager/produktion, mellemdøre, døre til rum med særligt følsomt udstyr (eller information).**
- **Fysisk inspektion af alle ydermure og vinduer. Mulighed for at klatre op ad mure. Mulighed for at skrue dækplader af under vinduer. Mulighed for at fjerne glasliste og hele vinduet.**
- **Er der etableret indbrudsalarmsystemer ? Hvilke ? Karmalarmer, vinduesalarmer, rumalarmer, rystealarmer. Hvornår er de aktive, hvem aktiverer og kontrollerer ?**
- **Er der frit indsyn fra 'offentlige' områder (f.eks. P-plads, stier o.lign.) til områder med edb-udstyr og/eller andre lokaler med tyvtækkeligt udstyr ?**
- **Sikrer man sig at alle vinduer og døre af aflåst indenfor bestemte klokkeslæt ? Hvem/hvordan ? Er der regler for aflåsning af yderdøre ?**

## BRAND

- **Er der etableret de fornødne brandalarmer ? Hvor og hvad reagerer de på ?**
- **Findes der funktionsdygtigt håndslukningsudstyr i tilstrækkeligt omfang, og specielt i kopirum o.lign. hvor der opbevares løst papir og/eller andet brandbart ?**
- **Er der udstedt rygeforbud i visse områder eller rum ? Hvor ?**
- **Benytter man brandsikrede papirkurve i kopirum o.lign. ?**
- **Findes der særlige regler for opbevaring af kemikalier og/eller andre brandfarlige stoffer i nærheden af teknikrum, edb-rum og rum med virksomhedens telefoncentral ?**
- **Findes der særlige regler for medarbejdernes tilslutning af kaffemaskiner, radioer og anden brandbar elektronik ?**

# Adgangsforhold - Bygning:

Er der styr på de mange mennesker der i forskellige ærinder kommer til virksomheden ? Medarbejdere, leverandører, chauffører, håndværkere m.fl..

Hvor og hvornår går de ud og ind ? Inspektion og interview skal bl.a. afdække om gæster har mulighed for at stjæle under et besøg, alternativt kunne researche med henblik på et senere indbrud.

## PERSONKONTROL

- **Hvor mange døre (og porte) benyttes som normale ind- og udgange for gæster, leverandører og personale ?**
- **Er adgangsvejene aflåste/uaflåste i arbejdstiden/uden for arbejdstiden ?**
- **Skiltes der på døre/vægge med hvad der gemmer sig bag dørene ?**
- **Benytter medarbejderne nøgle, nøglekort eller anden nøgletype ?**
- **Er der fysisk overvågning (vagt/reception) og/eller kameraovervågning på alle/nogle adgangsveje ? Hvor ? Optages det på video ? Hvor længe gemmes det ?**
- **Registreres alle besøgende ved ind- og udskrivning ? Foretages der identitetskontrol i tvivlstilfælde ?**
- **Har leverandører/chauffører fri adgang til virksomhedens bygninger fra vareindleveringen/ramperne, eller er der etableret en adgangssluse ?**
- **Er der særlige regler for medarbejdere som skal arbejde over aften/weekend ?**
- **Skal/kan medarbejderne identificere sig overfor vægterne uden for normal arbejdstid ?**
- **Er der regler for, hvordan en medarbejder skal forholde sig, hvis ukendte/fremmede antræffes i områder hvor de umiddelbart ikke burde befinde sig ?**

## NØGLEADMINISTRATION

- **Hvordan administreres og kontrolleres udlevering/inddragelse af nøgler/nøglekort i virksomheden ?**

# Fysiske forhold - Edb-rum og edb-afdeling

Edb-rummene er her defineret som de rum, hvor centralt og fælles edb-udstyr, dvs. centralenheder, servere, gateways, routere, bridges, krydsfelter og tilsv. udstyr befinder sig,

Brand, tyveri og sabotage i disse områder vil kunne blokere for al adgang til virksomhedens edb-systemer og dermed i større eller mindre omfang lamme forretningsdriften.

Edb-afdeling omfatter kontorerne til overvågning og administration af netværk mv. Specielt i disse rum kan der ligge mange attraktive softwarepakker, kredsløbskort, RAM-chips, harddiske og andre tekniske lækkerier, kort sagt: Tyvtækkelige varer.

Ikke mindst derfor bør der være begrænset adgang til edb-afdelingen. Adgangsbegrænsning vil omvendt også beskytte medarbejderne (både edb-afdeling. og øvrige) mod mistanke for tyveri fra edb-afdelingen.

**DØRE, LÅSE, VINDUER**

- **Er edb-rummene, på virksomhedens forskellige adresser, sikret tilstrækkeligt mod fremmed uønsket adgang gennem døre, vinduer og evt. ovenlyskupler ?**
- **Opfylder sikringen SKAFOR RØD klasse ?**

**ALARMER**

- **Er rummene forsynet med alarmer for: Høj/lav temperatur, fugt/vand, brand, indbrud ?**
- **Hvor/hos hvem registreres alarmerne og er der fastlagt en tilkaldeprocedure ?**
- **Hvor ofte, og af hvem testes alarmerne ?**
- **Hvem er ansvarlig for kontrol og test af alarmerne under eventuelle omflytninger og ombygninger ?**

**PERSONKONTROL**

- **Hvem har adgang til edb-rummene og under hvilke forhold/omstændigeheder ? Edb-medarbejdere, teknikere, konsulenter, håndværkere, rengøring.**
- **Registreres det på nogen måde hvem der går ud og ind hvornår ?**
- **Er der særlige regler for, under hvilke omstændigheder en 'fremmed' må arbejde alene i rummet, alternativt skal være fulgt af en medarbejder ?**

# Fysiske forhold - Edb-rum og edb-afdeling

Hvor edb-udstyr er placeret i kælderrum o.lign. er det en klassiker, at udstyret placeres direkte under vandrørssamlinger og/eller ventiler. Skulle et vandrør blive utæt sker det næppe på de lange strækninger, men typisk ved pakninger og sammenskruninger.

Nogle har tilsvarende monteret køleudstyr med kølevæsker på væggen direkte over edb-udstyret med samme risiko for udsivning og følgeskader.

Ikke alle kælderrum har gulvafløb, men selv om de har et, er det ingen garanti for at rummet er 'vandsikkert'. Ved meget kraftige regnskyld kan områdets kloaksystem blive belastet så kraftigt, at vandet i stedet slår tilbage og op i kældrene gennem afløbene.

**FUGT, RØG/GASSER, BRAND**

- **Er der gennemgående vandrør i edb-teknikrummene ? Er der ventiler, haner og/eller rørsamlinger på disse rørstrækninger ?**
- **Er edb-udstyret placeret direkte under rør/rørsamlinger/ventiler ?**
- **Er der gulvafløb og tilstrækkelig hældning på gulvet til at evt. vandudslip hurtigt vil løbe bort ?**
- **Ligger edb-rummet i kælderen med mulighed for kloaktilbageløb via gulvriste og er der installeret en grundvandspumpe ?**
- **Er edb-udstyr placeret direkte på gulvet eller er det hævet f.eks. mere end 20 cm over gulvhøjde ?**
- **Ligger der kabelsamlinger/stikforbindelser direkte på gulvet eller er de løftet f.eks. min. 20 cm over gulvhøjde ?**
- **Er tobaksrygning og brug af anden åben ild i edb-rummene forbudt ?**
- **Opbevares der særligt brandbart materiale (væsker, papirer) i edb-rummene eller i rum med tilknytning til disse ?**
- **Er edb-rummene forsynet med automatiske slukningsanlæg og et antal håndslukkere ?**
- **Er ventilationskanaler forsynet med automatiske brandspjæld, som lukker i forbindelse med aktiveret brandalarm ?**
- **Er kabelgennemføringer tilstoppet med godkendte materialer som hindring mod brandspredning ?**

# Dokumentation af virksomhedens edb-ressourcer:

## REGISTRERING AF UDSTYR

Manglende dokumentation er om ikke en direkte risiko for ulykker og nedbrud, så dog en risiko for, at en given forsikring ikke dækker tilstrækkeligt mod tyveri, hærværk o.a., og at det tager væsentlig længere tid at gøre evt. tab op såvel numerisk som værdimæssigt.

Mangel på relevant og aktuel dokumentation vil besværliggøre eller umuliggøre at virksomheden hurtigt og effektivt gen-etablerer sin edb-drift efter fysiske uheld og ulykker.

Det er jo langt fra sikkert, at den person som sidder inde med tilsvarende viden er til stede eller til at få fat i. Måske er den pågældende blevet alvorligt skadet eller død som følge af en opstået ildebrand, sammenstyrtning, eksplosion el. lign.

- **Er virksomhedens edb-udstyr registreret og dokumenteret f. eks. med**

- **fabrikat**
- **model/typebetegnelse**
- **serie-nummer**
- **konfiguration**
- **placering**
- **netkortadresse**
- **anskaffelsespris, købt/lejet/leased**

- **Er der regler/retningslinier for indførsel, flytning, ændring og fjernelse af virksomhedens edb-udstyr ?**

- **Er edb-udstyr og anden tyvtækkelig elektronik tyverisikret med mærkning, fastgørelse eller andet mekanisk eller elektrisk sikringsmateriel ?**

- **Er sammensætningen (konfigurationen) af udstyret beskrevet og aktuel ?**

- **Er virksomhedens kommunikationsforbindelser, linietyper og anvendte protokoller beskrevet ?**

Og i øvrigt er en grundig dokumentation vældig praktisk i det daglige arbejde for supporternes arbejde, så tidsforbruget til at udarbejde dokumentation er på ingen måde spildt eller misbrugt. Resultatet kommer flere gode formål til gode.

# Dokumentation af virksomhedens edb-ressourcer:

## REGISTRERING AF SOFTWARE

Softwaret er lige så sårbar som hardwaren, hvortil kommer at en registrering også kan bruges i forb. med licenskontrol. Risikoen her består i, at virksomheden bliver taget i alvorlig piratkopiering med bødeforlæg og imagetab til følge.

- **Er virksomhedens software registreret og dokumenteret f.eks. med:**

- **fabrikat**
- **type-betegnelse**
- **release**
- **licensantal**
- **anskaffelsespris**

- **Findes der regler/retningslinier for indførelse, opgradering, kopiering og sletning af software ?**

- **Har man udarbejdet en "positivliste" over godkendt software ?**

## UDBYGNING OG OPDATERING

Et gammelt mundheld siger: Virker det er det produktion - virker det ikke er det test !

- **Er der etableret særlige regler/procedurer til test af nyt udstyr, nyt software og/eller nye applikationer, så driftstop i videst muligt omfang undgås ?**

- **Er der etableret regler for, at systemændringer kun må foretages efter aftale med systemejeren.**

- **Findes der kontrollister som skal følges ved anskaffelse af nyt centralt udstyr eller omplacering af det eksisterende, så det sikres at de strømforsyningsmæssige, kølemæssige og alarmmæssige forhold er i orden ?**

# Dokumentation af virksomhedens edb-aktiviteter:

Som grundlag for både den daglige driftkontrol og for revisionen skal relevante maskinlog'er mv. kontrolleres - manuelt eller maskinelt.

F.eks. vil det udgøre risiko for virksomhedens evne til at genskabe data, hvis der har været fejl i de seneste backupkørsler eller hvis de f.eks., slet ikke er blevet kørt af den ene eller anden årsag.

I PC- og Server-verdenen er det begrænset hvor mange log'er der findes, f.eks. i modsætning de muligheder der er for kontrol af maskiner og systemer i et mainframemiljø.

Man må kontrollere det mulige.

- **SYSTEMLOG'er**
- 
- **Er der etableret procedurer der sikrer daglig kontrol af log'er specielt med henblik på kontrol af backupkørsler og eller andre tilsvarende vigtige kørsler ?**
- 
- **Er log'erne sikret mod manipulation ved at ligge i sikrede directories, ved kryptering eller anden metode ?**
- 
- **Tages der backup af log'erne og hvor længe gemmes kopierne ?**

**ANDEN DOKUMENTATION**

Manglende registrering af problemer og fejl kan udgøre en potentiel risiko for, at man ikke kan finde årsagen til fejl og uregelmæssigheder, f.eks. forsøg på uretmæssig adgang til programmer og datafiler, forsøg på hacking eller andet som kan kompromittere virksomhedens data.

- **Registrerer man, manuelt eller maskinelt, daglige problemer og fejl med systemer, maskiner og applikationer centralt ?**
- **Hvem følger op på meldte/registrerede problemer og fejl ?**
- **Findes der en escaleringsprocedure hvis fejlfinding og problemløsning tager længere tid end ..... timer ?**
- **Registrerer man konstaterede forsøg på hacking, virusinfektion mv. ?**
- **Registreres alle problemer og fejl i et lukket edb-system, hvor kun system- og sikkerhedsadministratoren har adgang til manipulation af registreringer ?**

# Teknisk sikring af det centrale edb-net

Følgende spørgsmål skal afdække risici omkring den tekniske sammenkobling af udstyret og ikke mindst muligheden for at holde større eller mindre dele kørende i forb. med uheld og ulykker. Derfor kikkes der også på diverse hjælpemaskiner, strømforsyning mv. - teknik som er uundværlig for edb-driften.

## SERVER- & NETVÆRKS-KONFIGURERING

- **Råder installationen over specielt gammelt, sjældent og/eller eksotisk udstyr, som kun finder begrænset udbredelse i Danmark ?**
- **Hvordan er service- og reservedelssituationen på området ?**
- **Er serverne konfigureret med een enkelt eller flere fysiske diske / logiske diske med henblik på hurtigst mulig genstart efter nedbrud ?**
- **Er netværket konfigureret med uafhængige ringe/forbindelser mellem bygninger/lokationer ?**
- **Vil et nedbrud på en bestemt server/bridge/router trække større eller mindre dele af netværket med sig ? Hvilke ? Identificer de kritiske knudepunkter.**

## AUTOMATISK GENSKABNING AF DATA

- **Er serverne konfigureret med spejlede diske (RAID-1) el. andet RAID-niveau ?**

## AUTOMATISK OG FORTSAT DRIFT VED NEDBRUD

- **Er serverne fysisk eller logisk krydskoblede ? Hot/cold standby ?**

## STRØMFORSYNING

- **Er edb-strømmen adskilt fra den øvrige bygningsstrøm og på egne tydeligt mærkede strømtavler ? Er adgangen til disse tavler sikret ? Døre, låse mv.**
- **Er serverne og andet vigtigt edb-udstyr sikret med UPS eller anden form for fejlstrøms-/nødstrømssikring ?**
- **Er evt. hjælpemaskiner, kølemaskiner, kompressorer, ventilationssystemer mv., som direkte influerer på edb-anlægenes drift tilsvarende sikret mod strømudfald, eller forsynet med nedbrudsalarmer ?**
- **Er der pga. vandrør i samme installationsrum mulighed for at udsivende vand kan løbe ind i stikforbindelser, eltavler o.lign. ?**

# Driftmæssig sikring af det centrale edb-net

## KRYDSFELTER

- **Er krydsfeltskabene aflåste ?**
- **Er kabelføring over skab til loft afdækket med skærm og sikret mod utilsigtede skader, hærværk og aflytning ?**
- **Er datakabler/kabelstrækninger <u>indendørs</u> fysisk inddækket og sikret mod utilsigtede skader, hærværk og aflytning ?**
- **Er datakabler/kabelstrækninger <u>udendørs</u> fysisk inddækket mod utilsigtede skader, hærværk og aflytning ?**
- **Er ubenyttede udtag og drop, f.eks. i mødelokaler patched op i krydsfelterne ?**

## BACKUP MEDIER

- **Er det muligt for fremmede uhindret at fjerne eller ombytte backupmedier i servere ?**

## BRUG AF NETVÆRKSANALYSATORER

- **Er der udarbejdet særlige sikkerhedsinstrukser forbrug af netværksanalysatorer, hvor bl.a. password's kan aflæses i klartekst ?**

## SERVICE-AFTALER

- **Er der etableret de fornødne serviceaftaler og er leverandørerne/deres medarbejdere behørigt informeret om virksomhedens holdninger, regler og procedurer for sikkerhed ?**

# System- og dataejerskab

Alle elementer af virksomhedens edb-ressourser, dvs. maskiner, systemer, applikationsprogrammer og dataregistre bør have en ejer, som er ansvarlig for vedligeholdelse og adgang til ressourcen.

**SYSTEM- OG DATAEJERSKAB**

- **Er der oprettet ejerskabet for de enkelte edb-systemer og -delsystemer ?**
- **Er der oprettet ejerskab for de enkelte dataregistre og filer ?**
- **Er ejerskabet tilknyttet personer eller funktioner ?**

**DATA KLASSIFICERING**

- **Er virksomhedens data (registre, filer, records, felter) klassificeret med en hemmelighedsklassifikation, f.eks. OFFENTLIG, HEMMELIG, FORTROLIGT, STRENGT FORTROLIGT eller tilsv. ?**
- **Følger disse klassifikationer de samme linier som de der gælder for papirsystemerne ?**
- **Hvem er ansvarlige for denne klassifikation, hvordan dokumenteres den og hvor ofte kontrolleres/revideres den ? Af hvem ?**

**ADMINISTRATION AF RETTIGHEDER:**

- **Hvordan og af hvem tildeles rettigheder og autorisationer til brugerne ?**
- **Administreres brugerne som enkelt individer eller i grupper ? Er tildelingen baseret på afdelingsfunktioner og/eller individfunktioner ? (Rolle-baseret sikkerhed ?)**
- **Hvor ofte kontrolleres/revideres tildelte rettigheder på den enkelte platform ? Benytter man manuelle metoder eller råder man over edb-baserede kontrol- & revisionsværktøjer ?**

# Logisk sikring af det centrale edb-net:

Den logiske sikring af adgang og virke i netværket ligger basalt i opsætning af operativsystemet og specifikt i operativsystemets sikkerhedsmoduler. Alternativt findes der en lang række produkter på markedet, som kan supplere og højne sikringen af virksomhedens data og ressourcer.

- **Benytter virksomhedens sig udelukkende af operativsystemets standardfaciliteter til styring og kontrol af adgang, autorisationer mv. ?**
- **Benytter man et supplerende/overordnet adgangssikringssystem ? Hvilke(t) ?**

## PASSWORD

Skal der være nogen ide i brug af password's skal de være opbygget fornuftigt, udskiftes jævnligt og ikke alt for let kunne gættes eller træffes ved en tilfældighed. Der er en risiko for integritetsbrud, hvis flere kender/bruger det samme password, hvis password'et ikke holdes hemmeligt eller udskiftes en gang imellem.

- **Anvendes password som grundlag for adgang/adgangssikring til det centrale edb-netværk ?**
- **Hvor mange karakterer består de nuværende password af ?**
- **Er der regler for tegnefordeling mellem alfabetiske og numeriske tegn i password'et ?**
- **Hvor ofte skal password ændres ? Bliver det tvangsstyret eller er det frivilligt ?**
- **Må/kan password genbruges indenfor en periode ?**
- **Hvornår kan det bruges igen ?**
- **Er der filtre/spærring på brug af de mest gængse og lettest gættelige password ?**
- **Har teknikere, konsulenter og andre eksterne hjælpere deres eget faste password, eller tildeles de et eengangs password for opgaven/for dagen ?**
- **Forekommer det, at flere kender/benytter kollegers id + password ?**
- **Logger sessionen automatisk af efter et forud defineret tidsrum, når der ikke er aktivitet ? Hvor langt tidsrum ?**

# Logisk sikring af det centrale edb-net:

## SYSTEMPARAMETRE

Det ses for ofte at de systemansvarlige på eget initiativ piller/roder/regerer i systemopsætningerne uden at det enten har været diskuteret, planlagt , godkendt eller er dokumenteret.

Ændringer i systemopsætningerne kan påvirke det generelle og specifikke sikkerheds niveau, hvorfor det kun bør udføres efter gensidig aftale i organisationen.

- **Er sikkerhedsparametre og andre parametre i styresystemer, sub-systemer, kommunikationssystemer skriftligt begrundet og dokumenteret.**
- **Hvor opbevares denne dokumentation ?**
- **Rettes der uplanlagt i systemet uden aftale/godkendelse ?**
- **Har systemansvarlige 2 user-id's, eet bruger-id og eet system-id ?**
- **Logger de(n) systemansvarlige sig altid på med system-id uanset hvilke opgaver de skal løse ?**

# Logisk sikring af det centrale edb-net:

## APPLIKATIONSADGANG

Applikationsadgang følger ofte den generelle adgang til netværket styret af samme adgangskontrolsystem, men der kan forekommer applikationer og/eller databaser, som yderligere er sikret med egen password- eller id-kontrol.

- **Anvendes password som grundlag for adgang/adgangssikring til applikationer/funktioner ?**
- **Hvor mange karakterer består det nuværende password af ?**
- **Er der regler for fordelingen mellem alfabetiske og numeriske tegn i password'et ?**
- **Hvor ofte skal password ændres ? Tvangsstyret eller frivilligt ?**
- **Må/kan password genbruges indenfor en periode ?**
- **Hvornår kan det bruges igen ?**
- **Er der filtre/spærring på brug af de mest gængse og lettest gættelige password ?**
- **Har teknikere, konsulenter og andre eksterne hjælpere deres eget faste password, eller tildeles de et eengangs-password for opgaven/for dagen ?**
- **Hvem administrerer det - og hvordan ?**
- **Forekommer det at flere kender/benytter kollegers id + password ?**

# Logisk sikring af det centrale edb-net:

## DATAADGANG

I det omfang sikkerheden ikke følger organisationen/funktionerne (rolle-baseret sikkerhed) opstår der let vanskeligheder med administrationen af sikkerheden. En medarbejder skifter afdeling, en anden forlader virksomheden.

- **Er man sikker på at alle referencer nu også ændres/slettes i sikkerhedssystemerne på de forskellige servere og platforme ?**

## KRYPTERING

Der er altid en risiko for fremmedes indsigt i virksomhedens data under reparationer, tyveri, kopiering eller aflytning. Sikres data med kryptering er det vanskeligt eller helt umuligt for den gennemsnitlige tyveknægt at få noget ud af informationerne, men det er sjældent ubrydeligt for de som ved hvad de beskæftiger sig med.

Den omvendte risiko forekommer ved at en medarbejder har mulighed for at kryptere data, som virksomheden efterfølgende ikke kan læse ved medarbejders pludselige dødsfald eller hvis en fyret medarbejder vil skade arbejdspladsen som hævn.

- **Benytter man kryptering til sikring af data på netværkets servere og/eller workstations ?**
- **Hvilken form for kryptering/algoritme benyttes ?**
- **Udføres kryptering af et software- eller hardware produkt ?**
- **Ligger krypteringsnøglen på maskinens harddisk eller ligger den eksternt fx. på et PC-kort, en speciel diskette, et Smartcard el. tilsvarende ?**
- **Hvordan sikrer man, at virksomheden har adgang til krypterede data, hvis medarbejderen siger op/siges op eller af forskellige årsager er fraværende ?**
- **Er data som flyder over lokal-nettet krypteret under selve transporten i nettet ?**

Specielt iforb. med kryptering af diskindhold på bærbart udstyr skal man være opmærksom på, at hvis krypteringsnøglen ligger på maskinens harddisk (hvilket den normalt gør når kryptering er foretaget med et softwareprodukt) kan koden i værste fald knækkes, hvis maskinen bliver stjålet med industrispionage eller lignende for øje.

# Logisk sikring af arbejdsstationer:

Arbejdsstationer som ikke er i netværket - stand-alone-PC'er - udgør på mange måder en større risiko for tab af data, for integritetsbrud mv. fordi de ikke indgår i den fælles overordnede administration af brugere, ressourcer, autorisationer, viruskontrol, afvikling af sikkerhedskopiering mv.

Men mange af risikopunkterne vil være de samme også for netkoblede arbejdsstationer.

**PASSWORD**

- **Er adgang til PC'en sikret med et adgangssikkerhedssystem ?**
- **Hvor mange karakterer består de nuværende password af ?**
- **Hvor ofte skal password'et ændres ? Tvangsstyret eller frivilligt ?**
- **Forekommer det at flere kender/benytter kollegers id + password ?**
- **Er diskettedrevet spærret logisk/fysisk mod uautoriseret anvendelse ?**
- **Er der regler/retningslinier for hvilke data der må kopieres ud og ind på stand-alone-PC'er ?**
- **Er der regler for, hvor længe følsomme data må befinde sig på en stand-alone-PC ?**
- **Er der procedurer for sikkerhedskopiering af data på stand-alone-PC'er ?**
- **Er der procedurer for oprydning og sletning på arbejdsstationer generelt ?**

# Sikring af bærbart, udlånt og hjemlånt PC-udstyr:

I disse tider, hvor bl.a. distancearbejde (dvs. at arbejde hjemmefra med en PC koblet op mod virksomheden) er ved at vinde indpas, skal der tages særlige forholdsregler med hensyn både til maskin- og databeskyttelse.

Når virksomhedens edb-udstyr og ikke mindst dens informationer fjernes fra virksomhedens sikrede lokaler opstår der risiko for tyveri af udstyret inkl. risiko for integritetsbrud i forb, med data som udstyr/medier måtte rumme.

Man bør også vurdere situationen, hvor 'lille Peter' får adgang til at spille spil på 'farmands' PC, dvs. virksomhedens !

Piratkopiering af virksomhedens programmel til andre, data der ved en fejl følger med til naboens PC, virus fra naboens PC til 'farmands' med 'lille Peters' piratprogram osv. - det skal også tages i ed.

Der ligger yderligere nogle forsikringsspørgsmål omkring ansvar hvis 'farmands' bil bliver stjålet, inkl.. virksomhedens edb-udstyr.

## FYSISK HÅNDTERING OG OPBEVARING

- **Er der udarbejdet særlige regler for, hvordan virksomhedens edb-udstyr skal transporteres mellem arbejdsplads og hjem ?**
- **Har man taget sin forsikring i ed med hensyn til ansvar og erstatning ved tyveri eller ødelæggelse under transport mellem arbejdsplads og hjem ?**
- **Gælder der særlige regler for opbevaring og sikring af virksomhedens aktiver, når de er flyttet hjem på privaten ?**
- **Har man taget stilling til om andre, f.eks. familiemedlemmer, må betjene virksomhedens PC hjemme på privaten ?**
- **Har man taget sin forsikring i ed med hensyn til ansvar og erstatning ved tyveri eller ødelæggelse af virksomhedens edb-udstyr og evt. datatab ved placering i medarbejderens hjem ?**

## Sikring af bærbart, udlånt og hjemlånt PC-udstyr:

PC- OG DATAADGANG

- **Har man taget stilling til, hvilke (typer) data som må hjemtages/ikke hjemtages ?**
- **Har man sørget for at data, som der arbejdes på under hjemlige former, er sikret fx. efter Registerlovens forskrifter ?**
- **Har medarbejderne den nødvendige viden og de nødvendige værktøjer til at sikre og til at udføre en regelmæssig sikkerhedskopiering af informationer, som er bearbejdet hjemme ?**
- **Er der procedurer for, hvordan man sikrer at informationer, som er bearbejdet i hjemmet, kommer tilbage på hovedsystemerne og evt. opdaterer ældre filer ?**
- **Har man klare regler for brug af softwarelicenser/piratkopiering ?**
- **Er der regler for og/eler værktøjer til kryptering af særligt følsomme informationer ?**

## Sikring af kundeterminaler og PC-udstyr:

Kunderteminaler/-PC'er defineres her som udstyr der er koblet på virksomhedens edb-netværk, og hvorfra den enkelte kunde uden særlige adgangskoder og kontrol kan forespørge på oplysninger, foretage transaktioner eller trække på andre edb-ydelser, som virksomheden stiller til kundens rådighed.

-
-

## Sikring af edb-udstyr til undervisning:

Edb-udstyr, som anvendes til undervisningsformål internt i virksomheden af egne medarbejdere eller af kunder.

- **Er undervisningsudstyret fysisk adskilt fra virksomhedens øvrige edb-netværk.**
- **Er undervisningsprogrammerne og eventuelle data logisk adskilt fra virksomhedens daglige data ?**

# Håndtering af datamedier:

Der er en række risici forbundet med brug og udveksling af databærende medier (disketter, CD'er, tape mv.), f.eks. muligheden for at få introduceret en edb-virus eller at få distribueret nogle gamle datafiler som modtageren kan genskabe fra mediet.

## FREMMEDE DISKETTER OG EDB-VIRUS

- **Hvor mange disketter, eller andre databærende medier, modtages dagligt/ugentligt/månedligt fra partnere, leverandører, kunder, filialer ?**
- **Hvor mange disketter, eller andre databærende medier, sendes dagligt/ugentligt/månedligt til partnere, leverandører, kunder, filialer ?**
- **Bliver alle ind- og udgående disketter virus-testet ?**
- **Har virksomheden etableret en virussluse ? Hvordan sikrer man ellers at disketter og/eller andre medier virus-testes ?**
- **Udføres der automatisk virus-kontrol i forb. med isætning af disketter eller skal brugeren igangsætte testen manuelt ?**

## BEHANDLING AF KONSTATERET VIRUS

- **Er medarbejderne bekendt med hvordan de skal reagere og rapportere hvis de konstaterer en virus ?**
- **Er der udarbejdet procedurer for, hvem og hvordan man informerer leverandører/kunder mfl. om konstateret virus på modtagne/afsendte medier ?**
- **Er det helt klart i organisationen hvem der må/skal fjerne en anmeldt/konstateret virus ?**
- **Er der udarbejdet procedurer for virustest af diverse sikkerhedskopier i forb. med konstateret virus ?**

## UDVEKSLING MELLEM STATIONÆRT OG BÆRBART UDSTYR

- **Hvor omfattende er disketteforbruget i virksomheden ?**
  **Hvor mange disketter udleveres pr. måned - og hvor bliver de af ?**
- **Kan disketter frit udveksles mellem virksomhedens PC-udstyr eller benytter man specialformaterede disketter ?**

# Håndtering af datamedier:

Når man betænker hvor mange databærende medier der kører land og rige rundt i taxaer, med postbiler og cykelbude, og hvor mange databærende medier der afleveres i virksomhederne uden at nogen i organisationen vil kendes ved dem, er det mere held end forstand, at ikke flere informationer kompromitteres

F.eks. er der ikke mange der tænker på, at en disketteformatering ikke sletter det gamle indhold. Dvs. at data kan genskabes med mindre at det gamle indhold er fuldt overskrevet af noget nyere.

I laboratoriemiljø kan man rent faktisk genlæse ned til 5-6 generationer gamle data på overskrevne medier !

## MODTAGELSE AF FREMMEDE MEDIER

- **Er der særlige regler for hvem og fra hvem man må modtage databærende medier ?**

## TRANSPORT OG FORSENDELSE

- **Benytter man helt nye medier til forsendelse eller genbruger man tidligere anvendte medier ?**
- **Har man sikret at tidligere anvendte medier grundslettes inden de bliver genanvendt og sendt ud af virksomheden ?**
- **Tages der særlige forholdsregler for emballering, mærkning, forsegling, følgesedler, sende/modtage-kontrol mv. i forb. med forsendelse af informationer på databærende medier ?**
- **Tages der særlige forholdsregler for emballering, mærkning, forsegling, følgesedler, sende/modtage-kontrol mv. i forb. med modtagelse af informationer på databærende medier ?**
- **Krypteres personhenførbare og andre følsomme informationer på forsendelsesmedierne ?**

# Håndtering af datamedier:

## REPARATION AF UDSTYR MED FASTE DATAMEDIER

- **Er der procedurer for sikring af virksomhedens data på diske og/eller andre medier som en tekniker kan afmontere/fjerne fra virksomheden ?**

## SALG AF UDSTYR MED FASTE DATAMEDIER.

- **Er der regler/procedurer for oprydning, sletning mv. på diske i forb. med salg af PC'er til medarbejdere eller andre ?**

## EDB-PRINTERE

- **Er edb-printerne placeret på en sådan måde så det ikke er muligt for fremmede at fjerne eller få indsigt i virksomhedens udskrifter ?**

- **Er edb-printerne placeret på en sådan måde, at det ikke er muligt for medarbejdere at fjerne eller få indsigt i oplysninger de ikke burde kende til ?**

## KASSATION AF EDB-UDSKRIFTER MV.

- **Findes der makuleringsudstyr i eller nær ved printere, således at udskrifter med følsom information omgående kan makuleres hvis de er fejlprintet eller af anden grund skal kasseres ?**

## KASSATION AF DISKETTER, DATATAPES MV.

- **Findes der særlige regler for kassation af gamle og/eller fejlbehæftede datamedier, f.eks. disketter og tapes, f.eks. indsamling/forbrænding ?**

## Sikring af kommunikationslinier:

Telefoncentralen er en vigtig og væsentlig del af virksomhedens daglige drift. Uden den ville al kommunikation til kunder og leverandører være umulig, eller meget langsom (pr. brev).

Moderne telefoncentraler er edb-systemer, hvor mange også kører deres edb-kommunikation sammen med og gennem den - med mulighed for telefonmisbrug og hacking udefra.

Mange virksomheder, specielt i gamle bygninger, har ofte kabeltræk (telefon, data, andre !) uden på bygningerne fra etage til etage, fra kælder til loft, i parkeringskældre og andre kælderrum osv. - oplagte steder at sabotere kommunikationen med en bidtang (fjern 30 cm), og oplagte steder at montere alternative telefonapparater og/eller lytteudstyr.

### TELEFONCENTRALEN

- **Anvendes virksomhedens telefoncentral også til datatransmissioner ?**
- **Hvem er ansvarlig for telefoncentralen og administration af systemet ?**
- **Har man taget særlige forholdsregler mod misbrug af og hacking i edb-systemerne via telefoncentralen ?**
- **Er rummet med telefoncentralen/krydsfeltet sikret effektivt mod indbrud og hærværk med fysisk sikring og/eller alarmer ?**
- **Er kabelstrækninger på åbne offentligt tilgængelige arealer inddækket fysisk mod tilkobling af lytteudstyr ?**
- **Råder virksomheden over en pulje af mobiltelefoner, som kan indsættes ved svigt af det faste telefonsystem ?**

### MODEMADGANG/-KONTROL

- **Er der adgang til edb-systemerne via modemer og opkaldslinier ?**
- **Kan medarbejdere kalde ind fra bærbart udstyr eller hjemme-PC'er ?**
- **Er der modemer med call-back faciliteter til faste numre/adresser ?**
- **Anvendes modemer med call-back på samme linie eller på alternativ linie ?**
- **Udføres der særlig identitetskontrol i forb. med opkald fra vilkårlige lokationer, fx. med elektronisk id, Smartcard, challenge response eller et tilsvarende system.**

## Sikring af kommunikationslinier:

**MODEMADGANG/-KONTROL**, fortsat:

- **Er servicemodemer altid tændt ? Findes der beskrevne regler ?**
- **Kan visse leverandører kalde ind præcis når det passer dem uden virksomhedens vidende og kontrol, også via andre forbindelser ?**
- **Kan kunder kalde ind og f.eks. bestille varer eller rette forespørgsler ?**
- **Er disse opkaldslinier specielt sikret eller er udstyr med data/databaser fysisk adskilt fra virksomhedens administrative netværk ?**

**INTERNET ADGANG**

- **Har virksomheden mere end een opkobling til Internettet ?**
- **Er opkobling til Internettet beskyttet af et såkaldt Firewall system eller tilsvarende andet system ?**
- **Hvem er ansvarlig for opsætning og vedligeholdelse af Firewall'en ?**
- **Kontrollerer man automatisk både ind- og udgående kald ? Og hvad kontrollerer man i øvrigt ?**
- **Udbyder virksomheden information til Internettet (WWW) ?**
- **Er Internet-serveren fysisk adskilt fra virksomhedens øvrige netværk og edb-systemer ?**
- **Hvordan er den sikret mod logiske angreb og misbrug ?**

**TRÅDLØS KOMMUNIKATION**

- **Benytter man mobiltelefoner til datatransmission ?**
- **Har man specielt sikret transmission af personhenførbare oplysninger ved kryptering ?**

# Sikring af kommunikationslinier:

**E-MAIL**

- **Hvordan er e-mail systemet beskyttet mod uvedkommendes indblik i andres meddelelser (både medarbejdere og hackere) ?**

- **Hvem administrerer og kontroller systemet ?**

**TELEFAX**

- **Er åbne Telefax-maskiner placeret således i kontorerne, at modtagne fax-meddelelser ikke kan blive læst af uvedkommende, inkl. medarbejdere/kolleger.**

# Sikkerhedskopiering:

Der er forskel på sikkerhedskopiering (backup) og sikkerhedsarkivering (offload).

Formålet med backup er primært at kunne genskabe en datasituation efter tab eller ødelæggelse af en datafil. Data findes derefter normalt både på serverdiske (men nu defekte) og på sikkerhedskopier i flere generationer.

Dataarkivering er langtidsopbevaring f.eks. af data jvf. bogføringsloven, hvor både operativsystem, drivere, applikationer og data skal være tilgængelige og funktionsdygtige i op til 5 år eller mere. Oplysningerne er normalt fjernes fra serverdiske og findes altså kun på databærende medier i en eller anden brandboks.

**SIKKERHEDSKOPIERING**

- **Er der etableret forretningsgange og procedurer for sikkerhedskopiering af operativsystemer, opsætningsfiler, subsystemer, applikationer og datafiler ud fra et sårbarheds- og genetableringssynspunkt ?**
- **Udføres sikkerhedskopieringen automatisk eller skal den igangsættes manuelt ?**
- **Finder der kontrolrutiner som sikrer at sikkerhedskopieringen er foretaget rettidigt og at der ikke er opstået fejl under kørslen ?**
- **Afprøver man jævnligt, ved stikprøver eller jævnlig anvendelse, at backup/restore procedurerne fungerer ?**
- **Findes der kontrolprocedurer, f.eks. som del af ethvert installationsforløb, der sikrer at datafiler skabt af den nye applikation automatisk sikkerhedskopieres ?**
- **I hvor mange generationer findes de forskellige sikkerhedskopier ?**
- **Konstrueres der automatisk en fortegnelse over hvilke filer (navn, dato mv.) der ligger på det enkelte back-up medie ?**
- **Registrerer man manuelt hvad de enkelte back-op medier indeholder ?**
- **Opbevares denne dokumentation sammen med medierne ?**
- **Er der særlige regler for sikkerhedskopiering af virksomhedssårbare data, som evt. findes på arbejdsstationer, stationære og bærbare PC'er, udenfor netværkets rækkevidde, samt findes regler for opbevaring af disse sikkerhedskopier ?**

# Sikkerhedskopiering:

## SIKKERHEDSARKIVERING

- **Er der etableret særlige retningslinier for Sikkerhedsarkivering med hensyn til offload af data, programmer, systemer, drivere mv. ?**
- **Hvor, hvordan og i hvilket omfang registrerer man hvad der er offloades ?**

## OPBEVARING

- **I hvilken type skab/boks opbevares virksomhedens sikkerhedskopier ?**
- **Opfylder skabet/boksen min. S60DIS specifikationen for databrandskabe ?**
- **Er databrandskabet samtidig indbruds- og tyverisikret ? (speciallås/fastgørelse)**
- **Er skabet/boksen placeret i edb-rummet eller på anden lokation ?**
- **Er boksrummet særligt sikret med uvedkommendes adgang og forsynet med alarmer ?**
- **Benytter man en fjernboks i anden bygning ?**
- **Registrerer man de enkelte backupmedier's aktuelle fysiske placering ?**
- **Føres der periodisk/aperiodisk bokskontrol af, om det der burde befinde sig i brandboksen nu også er der ?**
- **Findes der regler for hvem der må rekvirere data fra sikkerhedsboksen, hvornår og til hvilke formål ? Og registreres anvendelsen på nogen måde ?**

# Sikring af system- og applikationssoftware

## SYSTEMSOFTWARE

- **Hvor og hvordan opbevarer man originalsoftwarepakker ?**
- **Er alle licensnumre og super-password registreret og opbevaret forsvarligt ?**
- **Benytter man originalmedier eller kopier til installationer ?**
- **Fremstiller man boot/rescue-medier i det omfang det er muligt ?**
- **Tager man omgående en sikkerhedskopi af opsætningsfiler, parameterlister mv. efter afsluttet installation og/eller installationsændringer ?**
- **Hvor opbevares de og hvem har adgang til dem ?**

## APPLIKATIONSSOFTWARE

- **Hvordan opbevarer man originalsoftwarepakker ?**
- **Er alle licensnumre registreret og opbevaret forsvarligt ?**
- **Benytter man originalmedier eller kopier til installationer ?**
- **Fremstiller man boot/rescue-medier i det omfang det er muligt ?**
- **Tager man omgående en sikkerhedskopi af opsætningsfiler, parameterlister mv. efter afsluttet installation og/eller installationsændringer ?**
- **Hvor opbevares de og hvem har adgang til dem ?**

## EGENUDVIKLET SOFTWARE & APPLIKATIONER

- **Fører man automatisk eller manuelt versionskontrol i den takt systemet/programmerne udvikles, testes og godkendes ?**
- **Er der udarbejdets særskilte retningslinier for løbende sikkerhedskopiering,**
- **Er der særlige regler og procedurer for overførsel af programmer fra testbiblioteket til produktionsbiblioteker, og for offload og/eller sletning af tidligere programversioner ?**

# Sikring af system- og applikationssoftware

## EKSTERN PROGRAMUDVIKLING

- **Har man sikret sig kontraktligt på en sådan måde, at virksomheden indenfor en rimelig tidsperiode kan få adgang til kildekoden, hvis softwarehuset går konkurs, eller på anden måde ikke er i stand til at afslutte og/eller videreudvikle programmet ?**

# Forsikringer

- **Har virksomheden tilsikret en forsikringsdækning, der gør det muligt at etablere alternativ edb-drift i en nærmere defineret periode efter hærværk, tyveri, vandskader, brandskader, virusangreb og logiske bomber ?**

- **Dækker forsikringerne de omkostninger der må være forbundet med egne medarbejderes og eksterne konsulenters arbejde med genskabning af edb-systemer, både de maskinelle og programmelle ?**

- **Dækker forsikringerne de omkostninger der må være forbundet med genskabelse af tabte fysisk tabte data, efter indtræffelse af hærværk, tyveri, vandskader, brand, virusangreb og logiske bomber ?**

- **Foretager man jævnligt, f.eks. årligt, en revision af forsikringerne i takt med edb-systemernes udbygning, virksomhedens afhængighed af edb-systemerne, nye installationer og omflytninger mv. ?**

- **Dækker forsikringerne eventuelle forretningsmæssige tab, direkte og indirekte, i forbindelse med forsinkede eksterne programleveringer, som ikke dækkes af udvikleren, og eventuelle tab som må påføres på grund af fejl i de pågældende programmer ?**

- **Husker man at tage sine forsikringer i ed under omflytninger af edb-udstyret og under ombygninger ?**

## Nødplaner / Beredskabsplaner

- **Har virksomheden udarbejdet en sårbarhedsanalyse og ud fra den udarbejdet et beredskab som skal sikre virksomhedens fortsatte drift/edb-drift og overlevelse ved uventet tab af adgang til edb-drift ?**
- **Hvis JA, hvem er ansvarlig for den løbende vedligeholdelse af beredskabsplanen )**
- **Er beredskabsplanen for edb-tilgængeligheden afstemt med virksomhedens øvrige drift og beredskabsplaner ?**
- **Har virksomheden indgået aftaler med backup-centre, datterselskaber, nabovirksomheder eller tilsvarende med henblik på at kunne etablere nød-edb drift efter en eventuel ulykke eller katastrofe ?**
- **Er beredskabsplanerne behørigt dokumenteret ?**
- **Er beredskabsplanerne blevet afprøvet i større eller mindre omfang ?**
- **Hvordan er beredskabsplanens indhold formidlet ud til medarbejderne ?**

# Risiko-billeder / eksempler:

Følgende risiko-billeder er fra 'det virkelige liv' i både kommuner og private virksomheder, men er i denne sammenhæng naturligvis anonymiseret.

| | OBSERVATION | MULIG RISIKO | AFHJÆLPNING/LØSNING |
|---|---|---|---|
| | ORGANISATIONEN: | | |
| 1 | Organisationen/sikkerhedsorganisation/personale:<br><br>Der foreligger ikke nogen overordnet edb-sikkerhedspolitik for kommunen's anvendelse af edb og beskyttelse af informationer om borgerne, økonomi el. tilsv. | Kommunens medarbejdere, ledergruppe og politikere kan ved fejl eller fortsæt påføre kommunen og dens borgere imagemæssige og økonomiske tab ved uheldig omgang med edb-systemer og data.<br><br>Konsekvensen kan være alt fra mindre licensovertrædelser til omfattende manipulationer med programmer og data. | Kommunen bør udarbejde en edb-sikkerhedspolitik, som er afstemt med kommunens generelle edb-politik og ambitioner for edb-anvendelse fremover. |
| 2 | Der foreligger ikke nogen beredskabsplaner eller aftaler om alternativ edb-drift, hvis kommunens centrale edb-system(er) ved fejl, uheld eller forsæt, skulle blive sat ud af drift i kortere eller længere tid. | Kommunens afhængighed af edb i de daglige forretningsgange vokser med tiden, hvorfor også konsekvenserne af at være uden edb-kraft i krotere eller længere tid kan omfatte alt fra wen lille forsinkelse til store omkostningstunge reetableringer af data efter tab . | Risici, såbarhed, konsekvenser og alternative driftmuligheder bør fremover indgå i kommunens planer for investering, installation og implementering af edb-systemer. |
| 3 | Password sendes i lukkede kuverter med brev om at det skal ændres straks. | Risiko for at standard password'et står uændret. | Forvaltningens edb-ansvarlige bør kontrollere at det rent faktisk bliver skiftet. |
| 4 | NN har root-adgang til Bibliotekets maskine + den centrale server for at kunne oprette brugere. | Udgør en potentiel risiko for fejlagtig indgriben/betjening ved tilfældighed eller overlæg. | Oprettelse (administration) af brugere bør overføres til særlig funktion. |
| 5 | Ingen edb-medarbejdere er forsynet med ID-kort, og kan derfor ikke identificere sig overfor kolleger i andre forvaltninger iforb. med support-opgaver. | Fremmede kan i værste fald præsentere sig som værende fra kommunens edb-afdeling, og derved skaffe sig adgang til edb-installationer og -udstyr med ukendte konsekvenser. | Alle PC-supportere bør udstyres med ID-kort og forvaltningernes medarbejdere skal orienteres om, at ingen uden identifikation må have adgang til edb-installationer og -udstyr. |

# Risiko-billeder / eksempler:

| | OBSERVATION | MULIG RISIKO | AFHJÆLPNING/LØSNING |
|---|---|---|---|
| | HOVEDBYGNINGEN | | |
| 6 | Alle kældervinduer er sikret med stålstænger mod gårdsiden. Ingen speciel sikring mod gaden. | Ingen, eller meget lille, risiko for indbrud ad denne vej. | OK. |
| 7 | Der findes brandmeldere i gange og i kontorer.<br>Brandslukningsudstyr begrænses til nogel få brandspande med vand placeret i gangene. | | OK.<br><br>Godkendt af de lokale brandmyndigheder. |
| 8 | Der er adgang til kælderen via 3 separate døre til kælderhalse fra en relativt fredelig gård.<br><br>Alle døre er tynde fyldningsdøre med klart glas i øverste del.<br><br>Dørene er på ingen måde sikret ligesom der ikke findes adgangsalarmer i området. | Ualmindelig let adgang for enhver, som ønsker at trænge uretmæssigt ind.<br><br>Stor risiko for indtrængen i en række områder og rum i kældergangene med fri adgang til store dele af bygningens tekniske styring. | Der bør snarest muligt isættes solide yderdøre med dirkefri låse samt forstærkede karme. |
| 9 | Alarmfolie på hoveddør og på ca. 2/3 af alle vinduer i sidebygning.<br>Alarmen er hverken tilsluttet lokalt eller til alarmselskab.<br>Vinduer er fæstet med stiftede glaslister. Dækplade under vinduer er fastsat med alm. stjerneskruer.<br><br>Efter sigende er der tidl. sket indbrud ad denne vej. | Stor risiko for indbrud via vinduer, døre med gllaspartier, eller ved fjernelse af dækplader under vinduer. | Alarm-folien bør re-etableres med alarmering ti vagtselskab, så hele bygningen er sikret på samme måde og niveau. |
| 10 | Edb-udstyr er ikke mærket med forebyggende tyverimærkning/ejerforhold. | Potentiel risiko for at netop dette udstyr vil blive stjålet under et evt. indbrud. Stjålet udstyr vil ikke umiddelbart kunne identificeres. | Alt edb-udstyr bør være ætsemærket som et billigt første værn mod alm. lejlighedstyveri plus det planlagte efter research. |
| 11 | Printere og telefax-udstyr er placeret i gangarelaer, typisk i enderne.<br><br>Besøgende færdes i samme gangarealer.<br><br>Ved afdeling-x er printeren placeret en armlængde fra ventestolen på gangen. | Gæster kan få indsigt i, og i værste fald fjerne, udskrifter med mere eller mindre følsom information. | Printerne bør placeres et andet sted, alternativt anbringes i en lukket kasse specielt beregnet hertil med ventilation og mulighed for aflåsning. |

# Risiko-billeder / eksempler:

| | OBSERVATION | MULIG RISIKO | AFHJÆLPNING/LØSNING |
|---|---|---|---|
| | EDB-RUM / EDB-KONTORER | | |
| 12 | El-tavler/sikringsgrupper til edb-udstyr sidder åbent og tilgængeligt udenfor edb-rum. | Risiko for utilsigtet afbrydelse af strømforsyning. | Tavler bør inddækkes. Alternative tavler opsættes i edb-rum iforb. med evt. senere ombygning. |
| 13 | Brand-sensorer i loftet. | Vil næppe reagere på røg pga. MEGET kraftig udblæsning fra ventilationsrør umiddelbart under.<br><br>Som temperaturmelder vil næppe reagere pga. den meget lave udblæsningstemperatur. | Alarm- & ventalationsfirma bør kontrollere og evt. ændre på montering. |
| 14 | Ingen særlig brandsikring i lokaler omkring edb-rummet. | Risiko for at brand i omliggende rum kan brede sig til edb-rum og/eller skade udstyret pga varmepåvirkning gennem vægge. | Der bør installeres detektorer i rummene omkring edb-rum. ligesom der ikke bør opbevares særligt brandbart materiale i disse. |
| 15 | Meget kompakt pakke rum.<br><br>Mange ledninger hænger i guirlander på kryds og tværs over maskiner, reoler mv.<br><br>Ingen ledninger/kabler er mærket med tilhørsforhold. | Stor risioko for, at kabler trækkes ud af stik, at udstyr væltes ned og at der sker afbrydelser af edb-driften under alm. servicebesøg og/eller reparationer. | Der bør snarest muligt foretages oprydning i rummet, alternativt findes andet rum til det centrale edb-ydstyr. |
| 16 | Der findes ingen transientfiltre eller nødstrømsagregater til servermaskinerne. | Ved større udsving i strømforsyningen eller totalt svigt vil virksomhedens centrale edb være ude af drift, og i værste fald mere eller mindre skadet i elektronikken. | Man bør investere i en UPS-enhed, som både sikrer udstyret mod transienter og kortere strømudfald.<br><br>UPS'en giver tid til normal nedlukning af softwaresystemer og maskiner.<br><br>Det er ikke økonomisk forsvarligt at investere i egentlig nødstrøm, da længerevarende strømsvigt er yderst sjældne i området. |
| 17 | Gennemgående afløbsrør med 4 rør-samlinger under loft direkte over edb-udstyret.<br><br>Gips-skillevægge til bygningens faldstammer med mange rørsamlinger. Periodisk behov for reparation af disse rør.<br><br>Intet gulvafløb i edb-rummet, men gulvet skråner svagt mod dør.<br><br>Edb-udstry er hævet fra gulv på metal-reoler. | Stor risiko for, at utætte vandrør kan lække vand direkte ned i edb-udstyret med kortslutning til følge.<br><br>Konsekvenserne for den fortsatte drift kan gå fra ganske lille til totalt drift-stop i måske op til en uge eller mere.<br><br>Der har været flere eksempler på vand bl.a. fra lyskassen (stoppet afløb) og overløb fra faldstammer pga. stoppet kloak andetsteds. | Der bør snarest muligt findes en alternativ placering af virksomhedens centrale edb-rum/edb-udstyr. |

# Risiko-billeder / eksempler:

| | OBSERVATION | MULIG RISIKO | AFHJÆLPNING/LØSNING |
|---|---|---|---|
| | EDB-SYSTEMERNE | | |
| 18 | Der er 6-8 personer som er i besiddelse af pasword'et til UNIX-systemet "root": 4 fra edb-afd + 4 øvrige.<br><br>Årsagen er historisk betinget, og fordi der er enkelte superbrugere på serverne. | Mange personer skal orienteres ved udskiftning af password med risiko/mulighed for at det skrives ned. | Antallet af brugere med denne rettighed bør nedbringes til 2-3 personer. |
| 19 | Systemerne er ikke sat op til tvungen skift af password's.<br><br>Password bliver kun sjældent skiftet og er ikke skiftet de seneste 3 måneder. | Risiko for brud på integriteten ved for sjældne passwordskift.<br><br>Password gælder fortsæt efter at en medarbejder er fratrådt ! | Systemerne bør opsættes til tvunget skift af password efter antal dage eller efter antal log-on's.<br><br>Password bør skiftes min. 1 gang pr. kvartal og evt. oftere på de mest følsomme systemer. Systemadministratorer med max.adgang / rettigheder bør skifte oftere. |
| 20 | Kendte/faste konsulenter og teknikere til UNIX-systemerne har "root" login rettigheder med det til enhver tid gældende password.<br><br>Mindre kendte teknikere får tildelt et password til lejligheden, Password'et ændres umiddelbart efter arbejdets udførelse. | En ansat hos en leverandør vil også efter sin fratrædelse fra arbejdsgiver kunne medtage sin viden om password'et og i værste fald kune udgøre en trussel. | Eksterne konsulenter og teknikere må IKKE have egen passwords.<br><br>Passwords skal for alle eksteren tildeles til lejligheden og ændres umiddelbart efter arbejdets udførelse. |
| 21 | Der er ingen begrænsning i antallet af forsøg på LOGON/LOGIN.<br><br>Efter 3 forsøg uden success holder systemet en pause på ca 1/2 minut, hvorefter det igen er muligt at prøve.Der foregår ingen sporing/efterforskning af årsag til flere forsøg. | Med viden om programmering er det muligt at kode en sekvens der tester for password - og at finde et der virker. | Systemet bør opsættes så adgang låses efter fx. 3 forsøg uden success.<br><br>Gentagne forsøg fra samme person og/eller PC bør undersøges for årsag. |
| 22 | Der tages natlig backup til tape af alt. Der er dog tvivl om hvorvidt tapene bliver skiftet dagligt på de decentrale servere.<br><br>En del af backup tapene er gamle og sandsynligvis slidte, da de genanvendes konstant i den daglige backup cyclus på 14.<br><br>Der tages også måneds backup. | Chance for overskrivning af de mest aktuelle data fra dagen før, da UNIX ikke kontrollerer tapelabel<br><br>En evt. re-etablering kan umuliggøres pga. defekt tape. Konsekvensen kan være tab af mindre filer til hele systemet.<br><br>Hvis en fil bliver slettet ved en fejltagelse eller forsæt, er det ikke muligt at genskabe den efter 14 dage pag. cyclus'en. Månedsbackup'en vil ikke altid indeholde filen. | Medarbejderne bør føre en omhyggelig kontrol med backup medierne, kvittere for udført backup og rapportere fast til ledelsen.<br><br>Procedure bør indføres til jævnlig udskiftning af backup tapes. Gamle kan bruges til mindre følsomme data.<br><br>Cyclus bør udvides til 30 dage for at matche månedsbackup'en. |

## Sårbarhed/Konsekvensberegning

En gennemgang af de mange risici een for een med de deraf mulige konsekvenser siger noget om den tekniske sårbarhed - nu gælder det den forretningsmæssige sårbarhed, altså konsekvensen for forretningsdriften.

Øvelsen er interessant fordi den bl.a kræver et interview med de enkelte afdelingsansvarlige - hvem skulle ellers vide hvor afhængige - og dermed sårbare - den enkelte afdeling er for manglende adgang til edb-ressourcerne ?

Man skal passe på detaljeringsgraden - for mange detaljer vil sløre billedet og ikke være specielt til mere gavn end en rimelig overordnet vurdering, hvor på man kan hæfte nogle tids- og krone-omkostninger.

For eksempel kan man lade afdelingerne tage stilling til konsekvenserne af manglende adgang til edb-ressourcerne i

**1 TIME -1 DAG - 3 DAGE -1 UGE - 2 UGER - 1 MÅNED**

eller hvad man mener er relevant i den aktuelle situation/virksomhed.

Konsekvensen af manglende adgang til en bestemt database behøver ikke at være lige alarmerende for alle afdelinger.

Ved at finde frem til den mest sårbare afdeling, vil det (måske) være muligt at udarbejde nødprocedurer/evt. manuelle procedurer netop for den.

Det kan også være hensigtsmæssigt at klarlægge afhængighedsforholdet mellem ressourcerne, og derved finde det svageste led i kæden (ihukommende den gamle regel om kæder ... !)

For eksempel er forudsætningen for at applikationen og databasen er aktive, at server og operativsystem kører.

Konsekvensen af at server/operativsystem ikke kører vil derimod være større, da det typisk rammer flere afdelinger.

## Sårbarhed/Konsekvensberegning

Man bør gruppere virksomhedens edb-ressourcer og påføre en sårbarhedsfaktor pr. ressource - et udtryk for en prioritering - hvor alvorligt vil det være for forretningsdriften ikke at have adgang til ressourcen i en kortere eller længere periode.

Ressourcerne kunne f.eks. være:

- **TELEFONCENTRALEN**
- **KRYDSFELT-1**
- **KRYDSFELT-2**

- **SERVER-1**
- **SERVER-2**

- **OPERATIVSYSTEM-1**
- **OPERATIVSYSTEM-2**

- **APPLIKATION-1**
- **APPLIKATION-2**
- **APPLIKATION-3**
- **APPLIKATION-4**

- **DATABASE-1**
- **DATABASE-2**

- **NØGLEPERSON-1**
- **NØGLEPERSON-2**

# Sårbarhed/Konsekvensberegning

Sårbarhedsfaktoren kan f.eks. beregnes på grundlag af formlen:

S1 x S2 hvor S1 = Sandsynligheden - hvor ofte rammes vi
S2 = Sårbarheden - hvor hårdt rammer ulykken

- **Hvad er sandsynligheden for at miste adgangen til ressourcen ?**

- **Hvor meget/hvor mange er afhængige af denne ressource ?**
- **Den umiddelbare vurdering af konsekvensen - hvis uheldet er ude !**

I det efterfølgende er der brugt et point-system (vægte) med værdierne 1, 2 og 3 for SANDSYNLIGHEDEN (S1), men ønsker man en mere klar markering af øget sårbarhed kan man f.eks. vælge værdier som 1, 3 og 5 som vil slå hårdere igennem i beregningen.

Mangel på adgang til den enkelte ressource er derefter vurderet på den forretningsmæssige SÅRBARHED (S2), f.eks. med værdierne 1 til 10.

Det står naturligvis frit for at benytte alle værdier her i mellem, ligesom man kan lade værdierne springe (som her) for at give et tydeligere billede, når sandsynligheden vægtes med sårbarheden.

Sårbarhedsværdierne kunne eksempelvis udtrykke:

- **1 - Ingen nævneværdige konsekvenser**
- **3 - Konsekvenser, men kan klares manuelt**
- **5 - Problematisk for produktion/ekspedition mv.**
- **8 - Alvorligt, kun enkelte arbejder kan udføres**
- **10- Intet kan udføres. Arbejdet hober sig op.**

Man kan med stor fordel sætte kroner/ører på sårbarheden i det omfang det er muligt at beregne eller anslå værdien.

Den deraf beregnede værdi kan så bruges til en cost/benefit vurdering af at investere sig ud af problemet - hvis det overhovedet er muligt.

# Sårbarhed/Konsekvensberegning

En konsekvensberegning kunne f.eks. se sådan ud:

Sandsynligheden for et database-nedbrud på 1 time (målt f.eks. indenfor en kalendermåned) vurderes til middel (2) og konsekvensen anslås til ikke at være specielt alvorlig og får derfor vægten (3).

Beregningen ser derefter sådan ud:

Sårbarheden = 2 x 3 = 6 som er en relativ værdi

Sætter vi kroner/ører på, f.eks. løn for de medarbejdere der skal løse problemet plus et fiktivt beløb for den gene det har påført vores kundeekspeditioner (f.eks.. 3.000 kr.) vil resultatet blive noget i denne retning:

Sårbarheden = 2 x 3.000 kr = 6.000 kr.

Her taler vi så om småpenge. Men forestiller man sig et større netværksnedbrud med udskiftning og genstart af en vigtig server ser tallene ganske anderledes ud. Der skal ikke meget nedbrudstid til at koste store beløb. 200 medarbejderes tid i 1 time uden edb-adgang svarer nu engang til 200 timer = 5 arbejdsuger ! Dvs. en god månedsløn plus lidt til på omkring 50.000 kr.

I denne sag vil beregningen se således ud:

Sårbarheden = 2 x 50.000 kr = 100.000 kr

Nu skal der ikke megen fantasi til at udføre en cost/benefit beregning.

Hvis man med en udgift på f.eks. 65.000 kr. kan halvere konsekvensen (100.000 kr.) (det går kun ud over det halve antal medarbejdere f.eks. ved at dele netværket) er investeringen tjent hjem efter 2 nedbrud. Herefter er der 'overskud'.

Hvis man investerer 65.000 kr. i en halvering af sandsynligheden synes resultatet noget mere usikkert, for når/hvis ulykken indtræffer er konsekvensen stadig en udgift på 100.000 kr. ved at det fortsat går ud over alle. Det fordrer altså at sandsynligheden bevisligt er reduceret, f.eks. ved investering i UPS-anlæg i områder, hvor man er hårdt plaget af strømsvigt eller uregelmæssigheder i det offentlige forsyningsnet.

## Sårbarhed/Konsekvensberegning

Stiller man det op i et regneark kunne det f.eks. se ud som følgende:

SANDSYNLIGHEDSFAKTOR: 1, 2 eller 3

SÅRBARHEDSFAKTOR: 1, 3, 5, 8 el. 10

| | Sand-synlig-hed | Sårbar-hed: 1T | Sårbar-hed: 1D | Sårbar-hed: 3D | Sårbar-hed: 1U | Sårbar-hed: 2U | Sårbar-hed: 1M |
|---|---|---|---|---|---|---|---|
| TELEFONCENTRAL | 2 | 1 | 3 | 10 | 10 | 10 | 10 |
| KRYDSFELT-1 | 1 | 1 | 1 | 5 | 8 | 8 | 8 |
| KRYDSFELT-2 | 1 | 5 | 8 | 10 | 10 | 10 | 10 |
| SERVER-1 | 1 | 1 | 5 | 5 | 8 | 8 | 8 |
| SERVER-2 | 2 | 3 | 5 | 8 | 10 | 10 | 10 |
| OPERATIVSYS-1 | 2 | 3 | 3 | 5 | 5 | 5 | 10 |
| OPERATIVSYS-2 | 2 | 8 | 10 | 10 | 10 | 10 | 10 |
| APPLIKATION-1 | 2 | 5 | 8 | 10 | 10 | 10 | 10 |
| APPLIKATION-2 | 2 | 1 | 3 | 5 | 5 | 5 | 5 |
| APPLIKATION-3 | 3 | 1 | 3 | 3 | 5 | 5 | 5 |
| APPLIKATION-4 | 1 | 3 | 8 | 10 | 10 | 10 | 10 |
| DATABASE-1 | 1 | 3 | 3 | 3 | 5 | 5 | 5 |
| DATABASE-2 | 2 | 5 | 8 | 10 | 10 | 10 | 10 |
| DATABASE-3 | 3 | 5 | 5 | 5 | 5 | 8 | 8 |
| NØGLEPERSON-1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 |
| NØGLEPERSON-2 | 2 | 1 | 5 | 8 | 8 | 10 | 10 |

# Sårbarhed/Konsekvensberegning

Beregnet KONSEKVENS som en multiplikation af SANDSYNLIGHED og SÅRBARHED:

| | Konse-kvens: 1T | Konse-kvens: 1D | Konse-kvens: 3D | Konse-kvens: 1U | Konse-kvens: 2U | Konse-kvens: 1M |
|---|---|---|---|---|---|---|
| TELEFONCENTRAL | 2 | 6 | 20 | 20 | 20 | 20 |
| KRYDSFELT-1 | 1 | 1 | 5 | 8 | 8 | 8 |
| KRYDSFELT-2 | 5 | 8 | 10 | 10 | 10 | 10 |
| SERVER-1 | 1 | 5 | 5 | 8 | 8 | 8 |
| SERVER-2 | 6 | 10 | 16 | 20 | 20 | 20 |
| OPERATIVSYS-1 | 6 | 6 | 10 | 10 | 10 | 20 |
| OPERATIVSYS-2 | 16 | 20 | 20 | 20 | 20 | 20 |
| APPLIKATION-1 | 10 | 16 | 20 | 20 | 20 | 20 |
| APPLIKATION-2 | 2 | 6 | 10 | 10 | 10 | 10 |
| APPLIKATION-3 | 3 | 9 | 9 | 15 | 15 | 15 |
| APPLIKATION-4 | 3 | 8 | 10 | 10 | 10 | 10 |
| DATABASE-1 | 3 | 3 | 3 | 5 | 5 | 5 |
| DATABASE-2 | 10 | 16 | 20 | 20 | 20 | 20 |
| DATABASE-3 | 15 | 15 | 15 | 15 | 24 | 24 |
| NØGLEPERSON-1 | 1 | 1 | 1 | 3 | 3 | 3 |
| NØGLEPERSON-2 | 2 | 10 | 16 | 16 | 20 | 20 |

Sæt f.eks. hvert konsekvens-point til 2.000 kr. og se det markante resultat:

| | Konse-kvens: 1T | Konse-kvens: 1D | Konse-kvens: 3D | Konse-kvens: 1U | Konse-kvens: 2U | Konsekvens: 1M |
|---|---|---|---|---|---|---|
| TELEFONCENTRAL | 4.000 | 12.000 | 40.000 | 40.000 | 40.000 | 40.000 |
| KRYDSFELT-1 | 2.000 | 2.000 | 10.000 | 16.000 | 16.000 | 16.000 |
| KRYDSFELT-2 | 10.000 | 10.000 | 20.000 | 20.000 | 20.000 | 20.000 |
| SERVER-1 | 2.000 | 10.000 | 10.000 | 16.000 | 16.000 | 16.000 |
| SERVER-2 | 12.000 | 20.000 | 32.000 | 40.000 | 40.000 | 40.000 |
| OPERATIVSYS-1 | 12.000 | 12.000 | 20.000 | 20.000 | 20.000 | 40.000 |
| OPERATIVSYS-2 | 32.000 | 40.000 | 40.000 | 40.000 | 40.000 | 40.000 |
| APPLIKATION-1 | 20.000 | 32.000 | 40.000 | 40.000 | 40.000 | 40.000 |
| APPLIKATION-2 | 4.000 | 12.000 | 20.000 | 20.000 | 20.000 | 20.000 |
| APPLIKATION-3 | 6.000 | 18.000 | 18.000 | 30.000 | 30.000 | 30.000 |
| APPLIKATION-4 | 6.000 | 16.000 | 20.000 | 20.000 | 20.000 | 20.000 |
| DATABASE-1 | 6.000 | 6.000 | 6.000 | 10.000 | 10.000 | 10.000 |
| DATABASE-2 | 20.000 | 32.000 | 40.000 | 40.000 | 40.000 | 40.000 |
| DATABASE-3 | 30.000 | 30.000 | 30.000 | 30.000 | 48.000 | 48.000 |
| NØGLEPERSON-1 | 2.000 | 2.000 | 2.000 | 6.000 | 6.000 | 6.000 |
| NØGLEPERSON-2 | 12.000 | 20.000 | 32.000 | 32.000 | 40.000 | 40.000 |

# Sårbarhed/Konsekvensberegning

Ved at vægte SANDSYNLIGHED med SÅRBARHED (med kroner på) fremkommer der nogle klare og tydelige spring i tabellen , som viser hvornår det for alvor bliver alvor !

Eksempelvis bliver det hurtigt problematisk, hvis der ikke er adgang til TELEFONCENTRALEN eller til OPERATIVSYSTEM-1, mens der ikke er særlige problemer forbundet med manglende adgang til DATABASE-1 og SERVER-1.

Hvad der ikke fremgår, og hvad der i princippet er umuligt at gøre er, at opstille kombinationer af hændelser - og hvordan det påvirker forretningsdriften.

Een ting er sikkert - går det galt med flere ting samtidig (Murphy's lov !) vokser konsekvensen væsentligt hurtigere end tabellen og graferne viser - både i kroner/tab og i gener.

Kombination af manglende adgang til f.eks. OPERATIVSYSTEM-1 og DATABASE-2 (forudsat at de kun kan fungere sammen) vil ikke nødvendigvis gøre skadeeffekten større, da ingen af dem alligevel vil kunne fungere uden den anden.

Kombinationen af manglende adgang til APPLIKATION-4 og NØGLEPERSON-2 vil til gengæld kunne øge skadeeffekten betragteligt, da rettelser i applikationen, foretaget af andre, dels vil tage længere tid og dels vil kunne introducere nye/andre fejl.

# Sårbarhed/Konsekvensberegning

Når sårbarheden er fastlagt gennem mere eller mindre komplicerede beregninger skal der sættes KR/ØRE på (hvis det ikke allerede er gjort !) - ikke mindst af hensyn til prioriteringen af i hvilken rækkefølge og takt skal risiciene minimeres/elimineres, så sårbarheden nedsættes.

KR/ØRE er naturligvis de direkte omkostninger forbundet med problemet og problemets løsen, f.eks.

- **tab ved manglende produktion/produktionsstyring i fabrikken,**
- **rentetab ved manglende finansielle transaktioner**
- **ekstraomkostninger ved manuelle procedurer**
- **ekstraomkostninger til problemets løsen**
- **omkostninger til erstatningsudstyr**
- **m.fl.**

Og hertil kommer så de indirekt/afledte omkostninger som

- **tabte kunder**
- **evt. erstatninger ved manglende levering**
- **forringet image blandt kunder/partnere**
- **m.fl.**

De direkte omkostninger vil ofte kunne dækkes helt eller delvis gennem forsikringer, men både bevisbyrde og dækning er mere tvivlsom for de indirekte/afledte omkostninger.

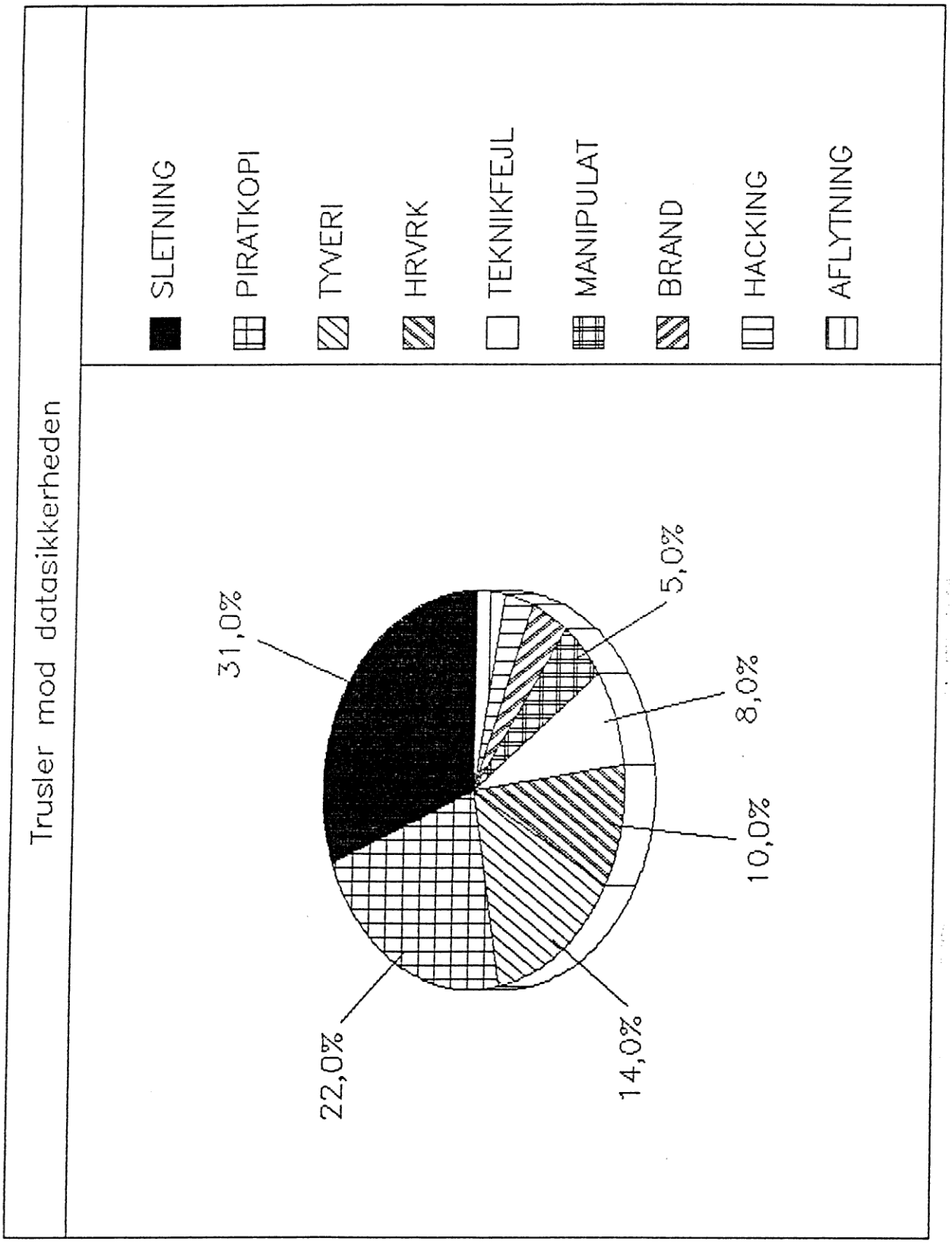
| Områder med høj sårbarhed: | Samlet tab direkte + indirekte | Omkostninger til risiko minimering | |
|---|---|---|---|
| | | | |
| PROBLEM-1 | 300.000 | 75.000 | + |
| PROBLEM-2 | 300.000 | 1.100.000 | - |
| PROBLEM-3 | 300.000 | 200.000 | ? |

\+ Sagen er klar. Relativt billigt at minimere risikoen og undgå problemer og tab

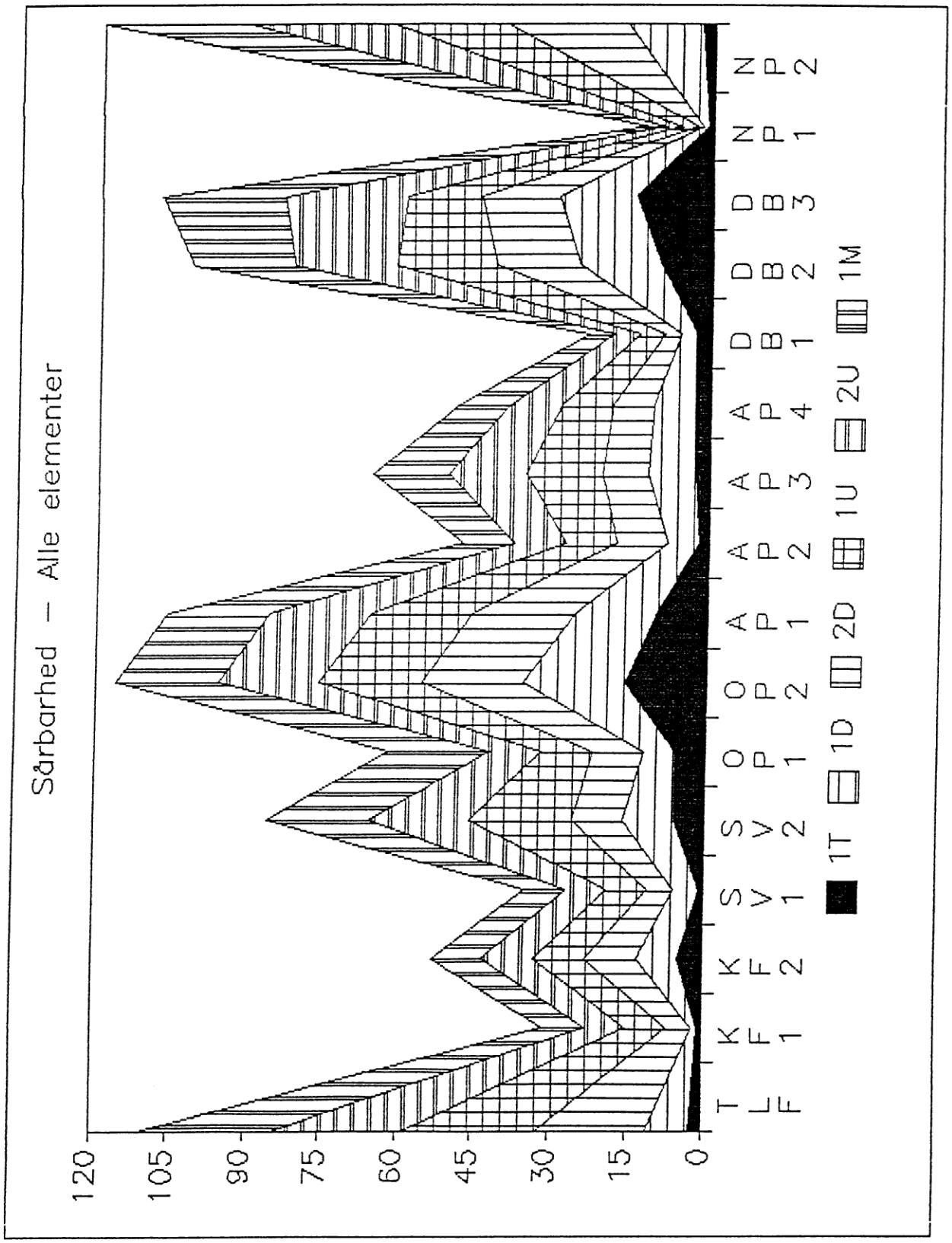
\- Omkostningerne til minimering af risikoen overstiger langt de samlede tab, hvis uheldet er ude. Spørgsmålet er nu: Hvor ofte er uheldet at være ude ?

? Skal/skal ikke ! Tabene er klart dokumenteret. Det vil være relevant at se på sammensætningen af tabene. Produktionstab eller imagetab ?

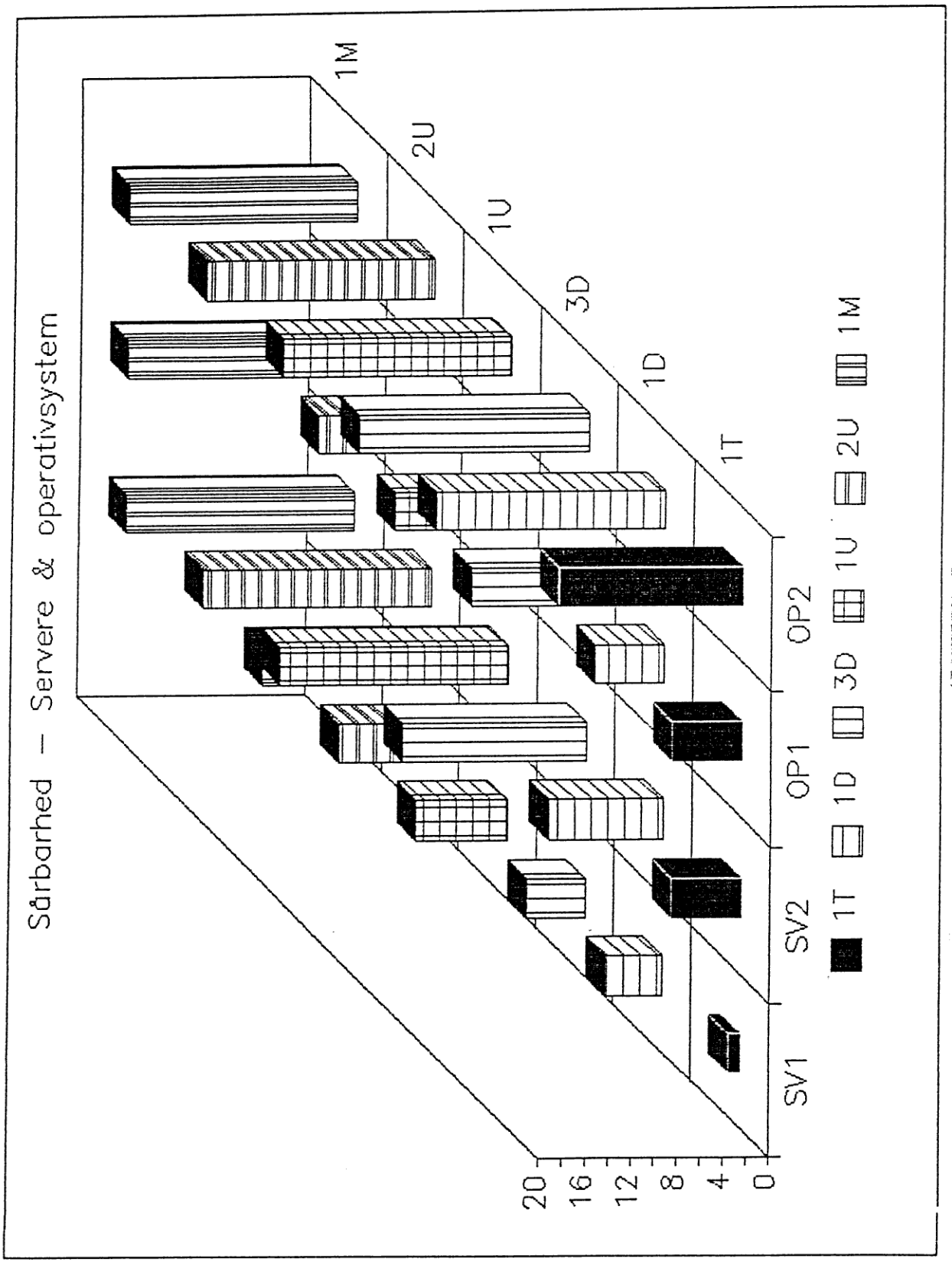
# Sårbarhed/Sårbarhedsanalyse



# Sårbarhed/Sårbarhedsanalyse



# Sårbarhed/Sårbarhedsanalyse



# Sårbarhed/Sårbarhedsanalyse