

**ITEK og Dansk Industri's  
Vejledning i fysisk IT-sikkerhed**

# Indholdsfortegnelse

Indholdsfortegnelse.....	2
Indledning .....	4
Kort om driftstab, beskyttelse af følsomme data og digital overvågning .....	4
Læsevejledning .....	5
Fysisk IT-sikkerhed.....	5
Udendørs sikring .....	5
Hvilke områder skal sikres?.....	5
Hvordan skal de sikres? .....	5
Kortlægning af personalegrupper.....	6
Kortlægning af vare ind- og udlevering .....	6
Fysisk barriere.....	6
Mekanisk sikring .....	6
Adgangskontrol og overvågning .....	6
Ikke-elektronisk adgangskontrol.....	6
Elektronisk adgangskontrol.....	6
Elektronisk overvågning .....	7
Udendørs videoovervågning .....	7
Vurdering af naboernes betydning .....	8
Brand og eksplosioner.....	8
Kemisk påvirkning .....	8
Beskyttelse mod naturskabt skade .....	8
Beskyttelse mod lynnedslag.....	8
Beskyttelse mod oversvømmelse .....	8
Indendørs sikring.....	8
Hvilke områder skal sikres?.....	9
Hvordan skal de sikres? .....	9
Indretning af lokaliteter/bygningslayout .....	9
Klassifikation af celler (sikkerhedsniveau).....	9
Cellesikring – adgangskontrol og overvågning .....	9
Mekanisk cellesikring .....	10
Elektronisk cellesikring.....	10
Elektronisk overvågning .....	10
Sikring af IT-relateret udstyr.....	10
Stationære Computere .....	10
Udstyrets placering og fysiske sikring .....	10
Adgangskontrol og overvågning .....	11
Mærkning .....	11
Vedligehold.....	11
Afvikling og genbrug .....	11
Bærbare Computere og andet udstyr i brug udenfor virksomheden .....	12
Udstyrets placering og fysiske sikring .....	12
Adgangskontrol.....	12
Mærkning og sporing .....	12
Vedligehold.....	12
Afvikling og genbrug .....	12
Servere .....	13

Udstyrets placering og fysiske sikring .....	13
Køling .....	13
Brandsikring.....	13
Nødstrømforsyning .....	13
Automatisk overvågnings- og alarmeringsanlæg.....	14
Backup af data.....	14
Adgangskontrol.....	14
Mærkning og sporing .....	14
Vedligehold.....	14
Afvikling og genbrug .....	14
Krydsfelter .....	15
Kabel- og vandinstallationer .....	15
Flytbare medier og ikke-elektronisk datamateriale.....	15
Checkliste.....	16
Overordnede/forberedende tiltag .....	16
Udendørs sikring .....	16
Indendørs sikring.....	16
Ordforklaring .....	17

# Indledning

Formålet med denne vejledning er at skabe en oversigt over hvilke overvejelser man skal gøre sig når man skal implementere fysisk sikring af virksomhedens informationer og desuden skabe en fælles referenceramme mellem virksomhedens leder(e) og det tekniske personale, der skal implementere den fysiske IT-sikkerhed.

Fysisk IT-sikkerhed defineres af Dansk Standard i DS484-1:2000, som de sikkerhedsforanstaltninger, der baserer sig på fysiske eller mekaniske foranstaltninger for imødegåelse af tyveri, indtrængen, hærværk eller anden ødelæggelse af aktiver. Det handler altså om hvordan virksomheden beskytter sine værdier mod uvedkommende indtrængen, tyveri, hærværk, brand, vand, røg og varme således at bygninger, inventar og diverse IT-installationer er funktionsdygtige og tilgængelige for virksomhedens ansatte.

Tilvejebringelsen af fysisk sikkerhed for informationsaktiverne er en del af den større sammenhæng, som handler om at tilvejebringe systemer og datas integritet, fortrolighed, autenticitet, uafviselighed og tilgængelighed.

Denne vejledning har hovedvægten på beskyttelse af IT-relaterede aktiver. Nogle punkter er intuitive og trivielle at implementere, mens andre vil kræve yderligere research og samarbejde med specialister. Vejledningens anbefalinger lever op til kravene i Dansk Standard. Hvilke valg den enkelt virksomhed træffer vil i høj grad afhænge af individuelle parametre så som virksomhedens størrelse, værdien af de enkelte informationsteknologiske aktiver og behov for fortrolighed og hemmeligholdelse af aktiviteter eller produkter, samt afhængighed af IT i driftsøjemed.

Både lederen og teknikeren skal være opmærksom på at fysisk sikkerhed er en lille delmængde under en stor paraply af IT-sikkerhed, og at forskellige tiltag, så som risikoanalyse og IT-sikkerhedspolitik, vil være yderst nyttige redskaber at basere valg og beslutninger der vedrører IT-sikkerhed på. ITEK og DI har udgivet et hæfte om ledelse af IT-sikkerhed hvor disse redskaber behandles nærmere.

## ***Kort om driftstab, beskyttelse af følsomme data og digital overvågning***

### *Driftstab*

Driftstab som følge af systemnedbrud er en reel trussel, og virksomheden bør forberede sig på en akut krisesituation, hvad enten den er forårsaget af interne trusler som f.eks. fejl på systemer og netværk eller eksterne trusler som f.eks. indbrud, brand som følge af lynnedslag, oversvømmelse mv.

Det er vigtigt, at virksomheden som del af risikoanalysen tager stilling til ikke mindst de økonomiske konsekvenser ved driftstab og hvilke handlinger, der kan sikre hurtig reetablering af systemer og rutiner.

En velfungerende katastrofebeskyttelse kræver, at virksomheden udformer beredskabsplaner som angiver klare retningslinjer for procedurer og ansvar ved et systemnedbrud og en fornuftig og jævnligt testet backopløsning.

### *Beskyttelse af følsomme data*

Den danske Persondatalov og DS484 foreskriver at uvedkommende ikke må kunne skaffe sig adgang til fortrolige oplysninger om andre menneskers forhold og at det er den dataansvarlige der

skal sørge for, at oplysninger ikke kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Loven gælder for behandling af personoplysninger, som foretages af offentlige myndigheder og af private virksomheder, foreninger og lignende.

### *Digital tv-overvågning*

Digital tv-overvågning er som udgangspunkt omfattet af persondataloven, da der sker elektronisk behandling af oplysninger. Såvel tv-overvågning med som uden optagelse medfører efter Datatilsynets opfattelse behandling omfattet af loven.

I Datatilsynets praksis vedrørende tv-overvågning er billeder af både personale, kunder og andre tilstedeværende blevet anset for at være personoplysninger omfattet af loven.

Medarbejdere skal i henhold til Persondatalovens princip om god databehandlingskik informeres om overvågningen.

Det Kriminalpræventive Råd anbefaler, at man overvejer fordele og ulemper ved tv-overvågning - og hvis man beslutter sig for at sætte kameraer op, skal der være klare og kommunikerede retningslinier for tv-overvågningen: Hvordan bruges og opbevares materialet, hvem må se det, og hvem må det overdrages til?

## **Læsevejledning**

Denne vejledning i fysisk sikkerhed er opdelt i to hovedafsnit hver med uddybende underafsnit. Første hovedafsnit, *Udendørs sikring*, beskriver sikring af udendørsområder, herunder fysiske barrierer, adgangskontrol og overvågning, vurdering af naboernes betydning og beskyttelse mod naturskabt skade. Andet hovedafsnit, *Indendørs sikring*, beskriver på tilsvarende vis sikring af indendørsområder samt sikring af IT-relateret udstyr: Stationære og bærbare computere, servere, krydsfelter, samt behandling af kabel- og vandinstallationer og flytbare medier og ikke-elektronisk datamateriale.

På side 16 opsummerer en checkliste de emner, der er gennemgået i vejledningen.

## **Fysisk IT-sikkerhed**

### ***Udendørs sikring***

*Formålet med udendørs sikring er at sikre virksomhedens ydre skal og omgivende areal(er) mod uvedkommende indtrængen samt menneske- eller naturskabt skade.*

### ***Hvilke områder skal sikres?***

En risikoanalyse er et godt redskab til at afdække, hvilke omgivende arealer det er kritisk at sikre mod hvilke trusler og på hvilket niveau.

I analysen vurderes trusler så som uvedkommende indtrængen, skader på bygninger, utilgængelighed eller ufremkommelighed etc. og hvilke konsekvenser disse trusler kan medføre.

### ***Hvordan skal de sikres?***

På baggrund af beslutninger om hvilke områder der skal sikres og på hvilket sikkerhedsniveau, implementeres et eller flere af følgende tiltag:

## **Kortlægning af personalegrupper**

Kortlægningen er en formaliseret planlægning af personers trafik og ophold der skal sikre at kun autoriseret personale har adgang til bestemte sikkerhedsområder. Personalet kan kategoriseres som ledende medarbejdere, tekniske medarbejdere, almindelige medarbejdere, eksternt servicepersonale, kunde, gæst, fremmede håndværkere etc.

Kortlægningen kan med fordel understøtte adgangskontrol i form af nøglesystem, adgangs- og identitetskort eller rollebaseret adgangskontrol.

## **Kortlægning af vare ind- og udlevering**

En formaliseret planlægning af trafik for forskellige varegrupper skal sikre kontrol med ind - og udgående varer. Planlægning og kortlægning kan således understøtte at det ikke er muligt for uvedkommende at få adgang til virksomheden via potentielt svage punkter så som vareindlevering under påskud af at have et reelt ærinde (Social Engineering).

## **Fysisk barriere**

Fysisk barriere handler dels om at sikre sig at alle vinduer, døre og porte er forsvarligt låst, er mekanisk sikrede og/eller overvågede, samt at de eksterne mure er solide. Dels om at perimetersikre hele eller dele af virksomhedens areal.

### ***Mekanisk sikring***

Det anbefales at benytte klassificerede sikringsdøre eller forstærke eksisterende døre med f.eks. stålplader eller gitre. Vinduer kan sikres med gitre som monteres på den *indvendige* side af vindueskarmen for at give den bedste sikring i kombination med et alarmanlæg.

Sikring af døre og vinduer skal ske under hensyntagen til myndighedernes krav om flugtveje i tilfælde af brand.

For mere information om sikringsudstyr og –krav henvises til F&P's (SKAFOR) anbefalinger og klassificeringer i dette sikringskatalog: [http://www.forsikringenshus.dk/upload/forside\\_002.pdf](http://www.forsikringenshus.dk/upload/forside_002.pdf)  
Vinduer, døre, porte og hegn kan efter behov forsynes med overvågning i form af alarmer og video. Områder der anses som særligt sårbare, f.eks. vare ind- og udlevering, designes således at adgang til disse ikke automatisk medfører adgang til resten af virksomheden. Dette implementeres f.eks. ved en slusefunktion hvor interne og eksterne døre aldrig er åbne på samme tid. Der bør her være speciel opmærksomhed på at føre kontrol med såvel personale som materiale.

## **Adgangskontrol og overvågning**

### ***Ikke-elektronisk adgangskontrol***

Vagt eller vægterpersonale, nøglesystem, en bemandet reception eller slusefunktion som kontrollerer besøgendes aftaler og udsteder midlertidige identitetskort.

Trafik af mennesker og materiale bør registreres med dato, ankomst- og afgangstidspunkt og disse informationer logges. Gæster superviseres så længe besøget varer.

### ***Elektronisk adgangskontrol***

Adgang til virksomhedens område(r) sikres elektronisk ved implementering af f.eks. magnetkort, proxkort eller -brik med tilhørende PIN kode der administreres af et elektronisk adgangskontrolanlæg (ADK-anlæg).

Elektronisk adgangskontrol giver mulighed for automatisk at kontrollere, følge, logge og blokere adgang og identitet på flere niveauer og flere grupper (personer, materiale, maskiner) og kan

desuden kombineres med rollebaseret adgangskontrol, biometrisk identifikation og multifaktor autentifikation.

Elektronisk adgangskontrol eller en kombination af elektronisk og ikke-elektronisk adgangskontrol anbefales på områder med højt sikringsniveau.

Der bør som del af virksomhedens IT-sikkerhedspolitik være udformet en klar procedure omkring udlevering af nøgler, adgangskort, identitetskort og andre ting, der kan give adgang til virksomheden.

Ligeledes bør der være klare retningslinjer for hvorledes personalet skal forholde sig ved bortkomst af disse artefakter, samt procedure for inddragelse eller øgning af adgangsmuligheder ved fratrædelse, nyansættelse samt en ansats skift af lokalitet eller ansvarsområde.

### ***Elektronisk overvågning***

Elektronisk overvågning mod indbrud med f.eks. automatisk indbrudsalarmanlæg (AIA-anlæg). Anlæggene er konstrueret til automatisk at registrere indtrængen eller forsøg på indtrængen i en overvåget bygning eller lokale.

Et anlæg er ikke i sig selv en indbrudssikring, men en form for overvågning, der kan alarmere, hvis der bliver brudt ind i forretningen eller bygningen. Af samme grund bør man aldrig anvende et AIA-anlæg alene, men kun som en overvågning af den mekaniske indbrudssikring.

Overvågning af virksomhedens ydre skal vil typisk foretages ved følgende overvågningstype:

*Skalovervågning*, hvor døre, porte, vinduer, lemme og lignende skal overvåges mod opbrydning. I skrivende stund anbefaler DS484-1:2000 at der udløses et alarmsignal, senest når der fremkommer en åbning på 60 mm. Til dette formål anvendes åbningskontakter eller en bagved installeret bevægelsesdetektor.

DS484-2:2000 anbefaler at der etableres skalovervågning af halvprivate-, private- og særlige sikkerhedsområder, samt at overvågningen omfatter skallen op til en højde af 4 meter over terræn og inkluderer eventuelle kældre.

### **Udendørs videoovervågning**

Planlægning af udendørs overvågningsanlæg adskiller sig på væsentlige områder fra planlægning af indendørs overvågningsanlæg. Komponenternes placering og virkning kan være afhængig af faktorer som vind, regn, sne-, jord- og bladfygning, omstrefjende dyr, fugle m.m. Sensorerne i et udendørs overvågningssystem må kunne fungere uden hensyntagen til de miljøafhængige faktorer, således at antallet af uønskede alarmer begrænses.

### **Sabotageforsøg**

Overvågningsudstyr skal kunne modstå sabotageforsøg.

Når udstyret skal vurderes med hensyn til sin evne til at modstå sabotageforsøg, bør blandt andet følgende forhold tages i betragtning:

- Udstyrets mekaniske opbygning og styrke
- Udstyrets evne til at forhindre, at ydre påvirkninger sætter det ud af funktion, så det ikke kan afgive alarmsignal som forudsat
- Udstyrets evne til at modstå overlistningsforsøg
- Udstyrets evne til at dokumentere hvem eller hvad der satte det ud af drift (logning)

Hele ledningsinstallationen skal være skjult eller ført i metalrør.

Ved etablering af videoovervågning skal virksomheden være opmærksom på Datatilsynets afgørelser omkring hvad der er omfattet af persondataloven og desuden begrænsningerne mod at overvåge offentlige tilgængelige områder.

## **Vurdering af naboernes betydning**

### ***Brand og eksplosioner***

Det skal vurderes, om der er risiko for at skader som følge af f.eks. eksplosioner og brand samt afledte påvirkninger fra støv, vand- og røgskader mv. opstået på naboejendomme, kan sprede sig til virksomhedens arealer og bygninger og i givet fald hvilke forebyggende tiltag f.eks. i form af fysiske barrierer eller den fysiske afstand til IT-funktioner, der er nødvendige.

Brændbart materiale, der udgør en væsentlig brandfare skal placeres og eventuelt isoleres på forsvarlig afstand til sikrede områder.

Brandslukningsudstyr skal forefindes og placeres hensigtsmæssigt, dvs. ved områder med høj risiko for udbrud af brand eller indeholdende kritisk udstyr, samt ved alle ind og udgange.

Der bør desuden, som del af virksomhedens IT-sikkerhedspolitik, angives retningslinjer for rollefordeling og procedure ved brand og der skal udarbejdes en beredskabsplan der dokumenterer hvorledes der konkret handles på en given krisesituation.

### ***Kemisk påvirkning***

Det skal vurderes om umiddelbare og fjernereliggende naboers aktiviteter med kemiske emner, enten ved daglig anvendelse eller ved udslip eller brand, kan udgøre en fare for afbrydelse af virksomhedens IT-funktioner. Der bør som del af virksomhedens beredskabsplan indgå overvejelser omkring hvorvidt og hvorledes det er muligt at forsætte driften i tilfælde af at virksomheden ikke er fysisk tilgængelig, f.eks. ved gasudslip i egne eller omkringliggende bygninger. Yderligere information herom kan indhentes hos Brandvæsenet og Beredskabsstyrelsen.

## **Beskyttelse mod naturskabt skade**

### ***Beskyttelse mod lynnedslag***

Anlæg til beskyttelse mod lyn kan deles op i ydre og indre beskyttelse. Den ydre beskyttelse, lynaflederanlæg, minimerer risikoen for skade på bygninger og personer i tilfælde af lynnedslag. Den indre beskyttelse, overspændingsbeskyttelse, minimerer risikoen for skade på elektriske apparater i bygningen som følge af overspændinger og –strømme enten fra direkte lynnedslag eller indirekte, dvs. op til 1 km fra den aktuelle bygning.

### ***Beskyttelse mod oversvømmelse***

Det skal vurderes hvordan det kan undgås, at IT-aktiver og installationer beskadiges af udstrømmende og opstigende vand fra egne, naboers og overboers vand- og kloakanlæg eller vandskader efter brand.

### ***Indendørs sikring***

*Formålet med indendørs sikring er at beskytte virksomheden mod tab, skade, tyveri eller kompromittering af værdier samt forstyrrelser af virksomhedens aktiviteter.*

## **Hvilke områder skal sikres?**

En risikoanalyse er et godt redskab til at afdække hvilke værdier det er kritisk at sikre, mod hvilke trusler og på hvilket niveau.

I analysen vurderes trusler så som uvedkommende indtrængen, skader på inventar, utilgængelighed eller ufremkommelighed etc. og hvilke konsekvenser disse trusler kan medføre.

Det vil desuden være en fordel at kortlægge virksomhedens arbejds- og informationsflow.

## **Hvordan skal de sikres?**

Bygningstekniske adskillelser med tilhørende adgangsåbninger mellem de forskellige sikkerhedsområder skal have en sådan konstruktion, at ulykker opstået i ét område ikke kan sprede sig til andre. Erfaring siger at flere mindre celler giver større sikkerhed end enkelte store sikkerhedsområder.

På baggrund af beslutninger om hvilke værdier der skal sikres og på hvilket sikkerhedsniveau, samt under hensyntagen til virksomhedens arbejds- og informationsflow implementeres et eller flere af følgende tiltag:

### **Indretning af lokaliteter/bygningslayout**

Placering af udstyr mv. kræver overvejelser omkring hvorledes udstyr mv. placeres så sikkerhedstrusler og ulykker i de enkelte rum og fra omgivelserne får minimale konsekvenser.

Nogle overordnede retningslinjer er her:

- Undgå at placere al udstyr i ét rum.
- Vær opmærksom på faren for afledte påvirkning: f.eks. udvikling af fugt og varme i rum i umiddelbar nærhed af et rum der brænder.
- Indretning og placering af IT-funktioner skal tilrettelægges således, at de forskellige personalekategorier kan færdes i bygningen, uden at de sikringsmæssige regler tilsidesættes.

Mere udstyrsspecifikke retningslinjer gennemgås i de følgende afsnit om computere, servere mv.

### **Klassifikation af celler (sikkerhedsniveau)**

Med udgangspunkt i en lokaleregistrering kan bygningen inddeles i sikkerhedsområder eller celler. Cellerne kan f.eks. være serverrum, krydsfelter, maskinstuer og produktionsfaciliteter.

Der skal der tages stilling til om sikringen af den enkelte celle foretages af brand- eller IT-sikkerhedshensyn, da forskellige bygningstekniske valg som f.eks. cellens tolerance overfor høje temperaturer og dermed væggenes isoleringsgrad, vil basere sig på denne beslutning.

Vurderingen af cellernes klassifikation eller sikkerhedsniveau dokumenteres i form af en plan over hvordan IT-anlæg, -udstyr, -installationer og -funktioner samles eller separeres i en eller flere celler inden for et defineret sikkerhedsområde.

Der skal i virksomhedens IT-sikkerhedspolitik være dokumenterede retningslinjer for hvilke områder, der kræver særlig tilladelse for adgang og tilstedeværelse, og hvorledes medarbejdere og servicepersonale opfylder disse krav.

### **Cellesikring – adgangskontrol og overvågning**

Forud for implementering af forskellige kontroller/tiltag til cellesikring er det en fordel at foretage en klassifikation af lokaliteter og en kortlægning af personalegrupper som tidligere beskrevet.

Omfang af adgangskontrol og overvågning vurderes i henhold til virksomhedens IT-sikkerhedspolitik.

### ***Mekanisk celsesikring***

Se afsnit om mekanisk sikring under *Udendørs sikring*.

### ***Elektronisk celsesikring***

Adgang til cellerne sikres elektronisk ved implementering af f.eks. magnetkort, proxkort eller -brik med tilhørende PIN kode, som beskrevet i forudgående afsnit om adgangskontrol og overvågning af udendørs arealer.

### **Elektronisk overvågning**

Elektronisk overvågning mod indbrud med f.eks. automatisk indbrudsalarmanlæg (AIA-anlæg). Se mere om AIA-anlæg i tilsvarende afsnit under *Udendørs sikring*.

Overvågning af virksomhedens indre celler vil typisk foretages ved følgende overvågningstyper:

*Fældeovervågning*, som skal udløse et alarmsignal, når en person passerer det overvågede område. Der skal etableres et passende antal fældeovervågninger i forhold til resultatet af risikovurderingen.

*Rumovervågning*, som skal foretages ved hjælp af detektorer, der dækker det ønskede område og afgiver alarmsignal, når en person bevæger sig omkring i området. Der skal etableres rumovervågning af de celler, som indeholder IT-aktiver af væsentlig værdi, således f.eks. de celler, hvor der opbevares følsomme eller fortrolige informationer, sikkerhedskopier eller anden data af væsentlig betydning. Celler med servere eller krydsfelter for dataforbindelser skal ligeledes sikres med rumovervågning.

*Objekt- eller punktovervågning*, af større IT-aktiver, således af der udløses alarmsignal ved fjernelse eller forsøg på fjernelse af værdierne. IT-udstyr, der befinder sig i celler, som ikke er under permanent opsyn, og som er væsentlige for firmaet, skal sikres med punktovervågning. Punktovervågning kan ske ved at der etableres et af følgende:

- fældeovervågning (se ovenfor), eller
- magnetkontakter, som aktiveres hvis IT-udstyret fjernes fra sin plads, eller
- begrænset rumovervågning eller,
- seismiske detektorer, som måler bevægelser eller rystelser når IT-udstyret fjernes.

### ***Sikring af IT-relateret udstyr***

Det skal sikres at det generelle indeklima ikke forstyrrer den elektroniske drift. Det vil f.eks. sige at specielt udsat udstyr bør isoleres (se mere under afsnit om *servere*) og der i planlægningen tages hensyn til parametre som støv, varme samt kemisk- og elektromagnetisk påvirkning fra omkringliggende lokaler.

Der bør holdes en opdateret liste over virksomhedens IT-aktiver, samt oversigt over deres placering i eller udenfor virksomheden. Informationen skal som minimum inkludere fabrikat samt type- og serienummer. Disse inventarlistes skal opbevares sikkert.

### **Stationære Computere**

#### ***Udstyrets placering og fysiske sikring***

Det anbefales at disse placeres således at det ikke er muligt for uvedkommende at læse information fra skærmen.

IT-udstyr der befinder sig i områder, der ikke er tilstrækkeligt barriereafspærrede eller tyveriovervågede, skal fastholdes mekanisk, således at uretmæssig fjernelse besværlig- eller umuliggøres.

Desuden foreslås fastlimning eller wirebefæstelse af udstyret til borde eller lignende, fastgørelse af aktivet ved hjælp af skinner, der er beregnet for montage på bordplader, produkter der kan omslutte de enkelte aktivdele, samt sikringskabe, hvori hele IT-udstyret kan opbevares, og som fastboltes til stabile bygningsdele. Der findes også akustiske tyverialarmer, som aktiveres når et aktiv flyttes.

### ***Adgangskontrol og overvågning***

Computeren skal som minimum forsynes med adgangskontrol i form af unikt brugernavn/password pr. bruger eller PIN-kode som er underlagt en, i IT-sikkerhedspolitikken anført, fornuftig passwordpolitik. Yderligere adgangskontrol kan opnås ved brug af USB token eller smartcard som sikrer multifaktorautentifikation eller biometri.

Disse udvidede kontroller kan med fordel bygges på princippet om rollebaseret adgangskontrol.

Desuden bør der føres logning af adgangstrafik mhp. at udredning af forhold vedrørende (forsøg på) uautoriseret adgang. De enkelte maskiner skal 'låses' når de forlades i kortere perioder eller der skal logges helt af.

Det er muligt at implementere automatiske time-outs, så brugerne skal logge sig ind igen efter en bestemt tidsrum med inaktivitet. En mere avanceret løsning er radiobaserede tokens, som brugerne bærer på sig. Computeren bliver så automatisk låst, når brugeren forlader lokalet.

Der skal foretages en risikovurdering af, om virksomhedens data og udstyr skal beskyttes med elektronisk indbruds- og tyveriovervågning som beskrevet i forudgående kapitel om *elektronisk celsesikring*.

### ***Mærkning***

IT-aktiver kan sikres med beskyttelsesmærkning. Det reducerer afsætningsværdien af det stjålne, og det letter identifikation ved efterforskning.

Personale og serviceteknikere skal være instrueret om reglerne for fjernelse af IT-aktiver.

### ***Vedligehold***

Vedligehold af udstyr skal sikre tilgængelighed.

Generelt vedligehold sker gennem vejledende regler for omgang med udstyret og overvågning af indendørsklima så som temperatur og luftfugtighed. Det anbefales at logge opståede fejl og tilhørende reparationer samt forhold omkring hvem som har udført reparationerne.

Ved reparation af datamedier der, jf. Lov om personoplysninger, indeholder fortrolige eller følsomme data, anbefales desuden at indhente tavshederklæring fra reparatør. Skal der ske reparationer i udlandet af datamedier, der indeholder fortrolige eller følsomme data, skal Datatilsynet orienteres, inden der foretages forsendelse ud af Danmark.

### ***Afvikling og genbrug***

Sikker afvikling eller genbrug af udstyr indbefatter at al følsom data og licensbaseret software overskrives så der ikke er mulighed for at læse indholdet (ikke trivielt overskrivning!). Datatilsynet anbefaler i sikkerhedsbekendtgørelse af 2001, at der til overskrivning af datamedier anvendes et af de dertil beregnede specialprogrammer, som overskriver data flere gange i overensstemmelse med en anerkendt specifikation (f.eks. DOD 5220.22-M).

Alt IT-udstyr, der indeholder lagermedier f.eks. fastmonterede harddiske i arbejdsstationer og servere, skal kontrolleres før fjernelse for at sikre at alle følsomme og fortrolige data tillige med licenserede og egne brugerprogrammer er slettet. Se desuden Lov om personoplysninger. Der udarbejdes en politik for kriterier til vurdering af om beskadiget udstyr skal repareres eller skrottes.

For beskadigede datamedier eller forældet udstyr, der indeholder personfølsomme- eller forretningskritiske data, skal ejeren afgøre, hvorvidt datamediet skal destrueres helt eller repareres.

## **Bærbare Computere og andet udstyr i brug udenfor virksomheden**

### ***Udstyrets placering og fysiske sikring***

Uanset ejerforhold skal alt IT-udstyr, der benyttes udenfor virksomhedens sikkerhedsområder, omfattes af den samme sikkerhed, som findes inden for virksomhedens sikkerhedsområder. Virksomhedens IT-sikkerhedspolitik skal indeholde klare retningslinjer for hvordan udstyr udenfor virksomheden anvendes og beskyttes, samt for hvorledes personalet instrueres herom.

Personalet skal instrueres om at udleverede bærbare arbejdsstationer (laptops, PDA'er, mobiltelefoner) og det tilhørende kommunikationsudstyr skal anvendes med de samme kontroller, som anvendes i virksomheden. En komplet mobil sikkerhedsstruktur bør inkludere adgangskontrol, VPN, antivirusprogram, personlig firewall og kryptering. Bærbart udstyr, der efterlades skal opbevares i et aflåst skab eller lokale.

Under rejser må udstyr og medier ikke efterlades uovervågede og arbejdsstationer skal medtages som håndbagage ved flyvning.

Virksomhedens IT-sikkerhedspolitik skal indeholde retningslinjer om, at forud for autoriseret fjernelse af virksomhedens IT-aktiver skal der foreligge en formel godkendelse fra aktivets ejer, og fjernelse skal dokumenteres med en kvitteret følgesedel. Fjernelsen skal ajourføres i opgørelsen over virksomhedens IT-aktiver.

### ***Adgangskontrol***

Se tilsvarende afsnit under *Stationære Computere*.

### ***Mærkning og sporing***

IT-aktiver kan sikres med beskyttelsesmærkning. Det reducerer afsætningsværdien af det stjålne, og det letter identifikation ved efterforskning.

Der findes desuden trackingssoftware (f.eks. CompuTrace) som, installeret på den bærbare computer, kan spore dens lokation i tilfælde af f.eks. tyveri - også selv om den skilles ad og sælges i løsdele.

Virksomhedens IT-politik skal indeholde klare regler for autoriseret fjernelse af IT-aktiver og personale og serviceteknikere skal være instrueret om disse.

### ***Vedligehold***

Se tilsvarende afsnit under *Stationære Computere*.

### ***Afvikling og genbrug***

Se tilsvarende afsnit under *Stationære Computere*.

## Servere

### *Udstyrets placering og fysiske sikring*

Servere er i Dansk Standard kategoriseret som *særligt sikkerhedsområde* hvilket betyder at der bør stilles høje krav til adgangskontrol og vedligehold for at sikre optimal stabilitet og driftsikkerhed. Rummet skal sikres mod varme, støv, brand, røg og vand og serverne skal tilkobles en nødstrømsforsyning. Desuden bør ingen uvedkommende installationer såsom vandrør, afløb og elforsyning føres igennem et serverrum.

### **Køling**

Typisk er servere i dag forholdsvis små, kraftfulde og placeres i store antal i rack skabe i et serverrum. Ofte vil der være meget høj varmeudvikling i et rack og det stiller store krav til effektiv køling med konstant temperatur og luftfugtighed for at opretholde stabilitet og driftsikkerhed. Det er vigtigt at man ikke placerer de rack skabe med den største varmelastning i en samlet gruppe så de varmer hinanden op, men fordeler dem i rækkerne og så vidt muligt tæt på køleenheden.

Store koncentrationer af kabler og ledninger bag serverne skal så vidt muligt undgås for at sikre fri strømning af den kølende luft.

ITEK og Dansk Industri's Vejledning i køling af serverrum beskriver de forskellige løsninger nærmere.

### **Brandsikring**

Et serverrum opbygget med traditionelle brandsikre byggematerialer som gips, sten og beton vil forhindre at branden ikke trænger ind i rummet, men materialerne er ikke tilstrækkelig tæt og isolerende til at beskytte mod den indirekte brand: Varme, røg, slukningsvand og brandgasser fra en brand i naborum eller nabo bygninger. Til beskyttelse mod den indirekte brand anbefales byggelementer af stål med varmeabsorberende kerne, gastætte kabelgennemføringer mv.

### *Automatisk BrandalarmeringsAnlæg (ABA-anlæg)*

Brandsektioner, der indeholder centrale IT-anlæg eller udstyr, som er nødvendigt for IT-driften, dataarkiver, IT-krydsfelter og datakommunikationsanlæg skal være forsynet med ABA-installationer og manuelle brandtryk.

### *Brandslukningsanlæg*

Brandslukningsanlæg skal som minimum findes i form af håndslukningsanlæg, der placeres let tilgængeligt. Personalet skal informeres om udstyrets tilstedeværelse samt instrueres i procedure og rolle-/ansvarsfordeling i forbindelse med brand.

Slukningstypen (kulsyre, pulver, inertgas eller vand) skal tilpasses slukningsformålet.

Automatiske rumslukningsanlæg anbefales til alle rum hvor der er placeret centralt IT-udstyr, servere, telekommunikationsudstyr, krydsfelter og større blanketoplag.

Ved brug af automatiske rumslukningsanlæg med inertgas, skal en manuel udløsning af automatiske slukningsanlæg kunne iværksættes, mekanisk ventilation skal stoppes eller spærres og frisk luft må ikke tilføres rummet efter indblæsning af gassen.

Hvis rummet er følsomt for trykstigning skal der indbygges et brandsikkert aflastningsspjæld.

### **Nødstrømforsyning**

Serverne skal elforsynes via et nødstrømsanlæg af typen UPS-anlæg (Uninterrupted Power Supply) med en spændingsstabilisator og filter mod spændingsspidser. UPS'en har til formål at holde

serverne kørende præcis så længe at de kan lukkes ned på en sådan måde at data gemmes korrekt. Det er derfor vigtigt jævnligt at checke at UPS'en herunder dens batterier fungerer som forventet. UPS-anlægget kan med fordel suppleres af en dieselgenerator.

### **Automatisk overvågnings- og alarmeringsanlæg**

Der skal være etableret et automatisk overvågnings- og alarmeringsanlæg, som afgiver alarm ved svigt eller tekniske fejl på anlæggene.

Nedenstående anlæg skal være tilsluttet overvågningsanlægget, medmindre svigt på de pågældende anlæg umiddelbart kan konstateres af driftspersonalet:

- Elforsyningsanlæg herunder UPS-anlæg
- Køleanlæg/Ventilationsanlæg
- ADK-, AIA-, og ABA-anlæg
- Automatiske brandslukningsanlæg

Overvågningsanlægget skal være elektronisk og logge alle hændelser på de tilsluttede anlæg. Der skal ligeledes logges for alarmkviktering.

Overvågningsanlægget skal være nødstrømforsynet med en kapacitet, der muliggør mindst 30 minutters drift.

### **Backup af data**

For at sikre integritet og tilgængelighed af virksomhedens data i tilfælde af tyveri, driftsnedbrud og lignende, skal der jævnligt tages backup (sikkerhedskopiering) af virksomhedens information og software.

Virksomheden skal formulere en klar politik og strategi for hvorledes backup foretages. Strategien skal bla. indeholde tidspunkter og omfang for sikkerhedskopieringen, angivelse af backupmedier, samt procedure for komplet gendannelse (restore) af data herunder prioritering af reetablering baseret på IT-behovet hos brugerne.

Det er meget vigtigt at det jævnligt checkes at backupfunktionen fungerer.

Servere til backup bør ikke placeres i samme rum som de servere de kopierer fra og skal naturligvis sikres efter samme høje krav som virksomhedens øvrige servere.

Flytbare backupmedier som f.eks. magnetbånd, CD og DVD skal opbevares i godkendte tyverisikrede brandskabe og ligeledes placeres i en separat adgangskontrolleret celle.

### **Adgangskontrol**

Det anbefales at serverens indgange til flytbare medier som f.eks. CD-, DVD låses og USB porte, Bluetooth og kortlæsere deaktiveres. Keyboards og skærme til servertilslutning bør ikke stå fremme og de enkelte rackskabe skal låses af.

Se desuden tilsvarende afsnit under *Stationære Computere*.

### **Mærkning og sporing**

Se tilsvarende afsnit under *Stationære Computere*.

### **Vedligehold**

Se tilsvarende afsnit under *Stationære Computere*.

### **Afvikling og genbrug**

Se tilsvarende afsnit under *Stationære Computere*.

## Krydsfelter

Krydsfelter er det sted hvor eksterne og interne kommunikationslinjer sammenkobles med forskelligt IT-udstyr.

Krydsfelter tilhører kategorien *særligt sikkerhedsområde* og der bør stilles tilsvarende høje krav til adgangskontrol og vedligehold som krav fremstillet under forudgående afsnit om sikring af *Servere*.

## Kabel- og vandinstallationer

Kontinuerlig driftafvikling af IT-anlæg er afhængig af at elforsyning og kommunikationslinjer ikke afbrydes enten ved et uheld eller en bevidst handling. Derfor er en fleksibel installationsform, der tillader hurtige omlægninger, ændringer og udvidelser af kabelføringer, hensigtsmæssig.

Kabler og tilhørende udstyr til elforsyning og datakommunikation skal installeres således at de ikke er umiddelbart synlige og tilgængelige for uautoriserede personer. Dog skal stophaner til vandforsyning og afbrydere til elforsyning være umiddelbart tilgængelige for personalet som også skal have kendskab til deres placering.

Elektronikkomponenter/koblingsudstyr som sikringer, afbrydere, omskifttere og lignende skal placeres indenfor det sikkerhedsområde de betjener.

Netværksenheder som hubs, bridges og switches skal placeres i aflåste skabe eller celler.

## Flytbare medier og ikke-elektronisk datamateriale

Der skal foreligge procedurer for hvorledes følsomme og fortrolige data på magnetbånd, disketter, CD'er, DVD'er, samt print, sikres mod uautoriseret adgang og misbrug.

Det skal på baggrund af risikoanalysen vurderes i hvilket omfang der skal være separate funktionsadskilte celler for

- Opbevaring af større mængder blanketter og forbrugsgods,
- Arkiver for datamedier med sikkerhedskopierede data og programmer
- Printning og efterbehandling af dokumenter

Værdiopbevaringsenheder (godkendte tyverisikrede brandskabe), hvori der opbevares værdifulde eller fortrolige data, skal være overvåget med specielle boksdetektorer.

Printerens harddisk bør krypteres da denne er et følsomt medie med høj koncentration af værdifulde eller fortrolige data og der skal foreligge politik og procedure for hvorledes print opbevares og transporteres.

Brændbart materiale, der udgør en væsentlig brandfare, skal lagres i sikker afstand fra de celler, hvori der foretages driftafvikling.

# Checkliste

## Overordnede/forberedende tiltag

- Har virksomheden et afsnit om fysisk sikkerhed i sin sikkerhedspolitik?
- Har virksomheden foretaget eller fået foretaget en risikoanalyse som indbefatter den fysiske sikkerhed?

## Udendørs sikring

- Har virksomheden taget de nødvendige sikkerhedsforanstaltninger mod uautoriseret adgang?
  - Mekanisk sikring og forstærkning af døre, porte og vinduer
  - Elektronisk adgangskontrol og overvågning
- Er der taget højde for oversvømmelse, lynnedslag og anden naturskabt skade?
- Er der taget højde for brand, eksplosioner eller kemisk udslip - også i nabovirksomheder?

## Indendørs sikring

- Har virksomheden taget de nødvendige sikkerhedsforanstaltninger mod uautoriseret adgang?
  - Adgangskontrol på computere
  - Adgangskontrol på serverrum, krydsfelter og andre datafølsomme celler
  - Sikker transport og opbevaring af ikke-elektronisk datamateriale
- Er terminaler og servere sikret mod strømsvigt og andre driftsforstyrrelser?
  - UPS eller dieselgenerator
  - Backup
- Er terminaler og servere sikret mod tyveri?
  - Mekanisk vha. mærkning og fastspænding
  - Elektronisk vha. alarmer og trackingudstyr
- Har virksomheden taget de nødvendige sikkerhedsforanstaltninger mod brand som f.eks. at serverrummet er en brandcelle og med nødvendig brandslukning?
- Har virksomheden sikret klimaet i serverrummet via ordentlig køling de rigtige steder?
- Har virksomheden sikret føringsveje til el og datakommunikation?
- Har virksomheden udarbejdet politik og procedure for vedligehold af IT-udstyret og det teknikudstyr der installeres, f.eks. kølingsudstyr?

# Ordforklaring

*Ordene er opstillet alfabetisk*

## **Adgangskort**

Er f.eks. et plastikkort hvis indhold identificerer den person kortet er udstedt til.

## **ABA-anlæg**

Automatisk brandalarmeringsanlæg, et elektronisk overvågningsanlæg der registrerer brandkendetegn og alarmerer herom.

## **Bridge**

En bridge er en netværksenhed der bruges til at forbinde én type netværk med en anden gruppe eller type netværk.

## **ADK-anlæg**

Elektronisk adgangskontrolanlæg, en elektronisk sikkerhedsforanstaltning der har til formål at kontrollere personers adgang til og rundt i en bygning. Se også *Identitetskort, Chipkort, Biometrisk identifikation, proxkort.*

## **AIA-anlæg**

Automatisk indbrudsalarmanlæg, et elektronisk overvågningsanlæg, der registrerer og alarmerer ved gennembrydning, oplukning eller bevægelse i de overvågede rum.

## **Algoritme**

Et matematisk udtryk for et veldefineret regelsæt - en slags opskrift på, hvordan en bestemt opgave i et computerprogram udføres korrekt.

## **Autorisation**

Rettighed til at udføre specifikke funktioner samt tilladelse til at anvende på forhånd tildelte ressourcer.

## **Beskyttelsesmærkning**

Der er flere forskellige typer mærkningssæt, f.eks. elektrisk gravørværktøj, ridsepen, farvemærkning eller brændemærkning. Et mærkningssæt kan købes i butikker eller lånes hos det lokale politi.

## **Biometrisk identifikation**

Identifikation foretaget på baggrund af elektronisk aflæsning af fingeraftryk, ansigtsform, irisskanning, håndgeometri og stemmegenkendelse. Disse personlige karakteristika kaldes under et for biometriske egenskaber. De er entydigt knyttet til én person og kan derfor benyttes til identifikation af denne person.

## **Celle**

DS484-1:2000 definerer en celle som et lokale inden for et sikkerhedsområde der er beskyttet med yderligere sikring i form af bygningsmæssig adskillelse og med separat adgangskontrol.

Mindre virksomheder har typisk behov for færre celler, og celler kan godt bare være betegnelsen for en fysisk opdeling af rum, men fælles for alle størrelser af virksomheder er at serverne bør placeres i en selvstændig adgangskontrolleret celle.

### **Chipkort**

Speciel form for identifikationsbærer baseret på f.eks. et plastikkort med indlagt datahukommelse og dataprocesser. Udover at identificere ejeren kan kortet indeholde et stort antal data (eventuelt krypterede), der kan opdateres og regulere kortets anvendelsesmuligheder ved hjælp af specielle autorisationskoder og *algoritmer*.

### **Dansk Standard**

Dansk standard, DS484 er en norm, som for et defineret område opstiller krav, der tilsigter opnåelsen af et forsvarligt teknisk og administrativt kvalitetsniveau.

Normen er opdelt i to dele:

DS484-1:2000 omfatter de basale krav som en virksomhed, der påberåber sig at den lever op til normen, skal overholde.

DS484-2:2000 beskriver en række skærpede krav som forholder sig til særlige lovkrav, branchenormer mv.

### **Datatilsynet**

Datatilsynet, <http://www.datatilsynet.dk/> er den myndighed, der fører tilsyn med at persondataloven overholdes.

### **Datatilsynets Sikkerhedsvejledning (Vejl. nr. 37 af 2. april 2001)**

Findes på adressen [http://www.datatilsynet.dk/include/wrapper.asp?art\\_id=502](http://www.datatilsynet.dk/include/wrapper.asp?art_id=502)

En vejledning til Sikkerhedsbekendtgørelsen (bekendtgørelse nr. 528 af 15. juni 2000) om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

### **Den dataansvarlige**

Den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler der må foretages behandling af oplysninger. [jf. Lov om behandling af personoplysninger]

### **Det Kriminalpræventive Råd**

'Rådets målsætning er inden for gældende lovgivning at virke for forebyggelse af kriminalitet ved gennemførelse af sikkerhedsfremmende foranstaltninger, ved oplysningsvirksomhed eller på anden formålstjenstlig måde'. <http://www.crimprev.dk/sw241.asp>

### **Ejer**

Ejeren anses som værende den person der har ansvar såvel som rettigheder vedrørende specifikke eller generelle IT-registre og -systemer. Ejeren bestemmer, hvilke brugere der har adgang til og hvem som kan anvende et IT-system og dets registre. [Jf. Dansk Standard]

### **Halvprivat sikkerhedsområde**

*Et halvprivat sikkerhedsområde* er karakteriseret ved, at det kun i begrænset omfang er muligt at kontrollere personers adgang. Typisk er der tale om indgangspartier, forhaller, trappeopgange, vareindlevering og lignende.

## **Hub**

En simpel hub er en netværksenhed der broadcaster trafikken til alle porte så hver enkelt computerne selv skal sortere de datapakker der tilhører dem.

Mere avancerede hubs udfører nogle af de samme funktioner som en *switch*.

## **Identitetskort (ID-kort)**

Et kort eller lignende, der identificerer indehaveren, som legalt er i besiddelse af identifikationen.

Se også *Chipkort*.

## **IT-sikkerhedspolitik**

En IT-sikkerhedspolitik indeholder ledelsens ønsker om og krav til virksomhedens IT-sikkerhedsniveau og de nødvendige organisatoriske rammer.

Læs mere om IT-sikkerhedspolitik i "Ledelse af IT-sikkerhed",

<http://www.di.dk/Service/Produktside/?productid=2826> og på ITEKs hjemmeside om sikkerhed,

<http://www.itek.dk>

## **Kryptering**

Kodning af data til beskyttelse af disse.

## **Lov om personoplysninger**

Også kaldet Persondataloven. Se mere hos Datatilsynet <http://www.datatilsynet.dk/>

## **Magnetkort**

Adgangskort hvor informationer aflæses fra kortets magnetstribes.

## **Multifaktor autentifikation**

Her en adgangsmetode der kombinerer 'noget du ved' f.eks. et kodeord, 'noget du har' f.eks. et adgangskort og 'noget du er' f.eks. dit fingeraftryk.

## **Nøglesystem**

For eksempel systemnøgler.

## **Offentlig sikkerhedsområde**

*Et offentligt sikkerhedsområde* er karakteriseret ved, at der er fri, ukontrolleret adgang til området det meste af døgnet. Et område kan således godt være offentligt i brugsmæssig og sikkerhedsmæssig betydning, selv om det er aflåst om natten; det gælder f.eks. visse parkområder.

## **Passwordpolitik**

Se ITEK og DI's anbefalinger til retningslinier for udformning af passwords her:

<http://itek.di.dk/show.asp?page=doc&objno=827001>

## **PDA**

Forkortelse for Personlig Digital Assistent, en håndholdt computer med funktioner som kalender, e-mail, fax, telefon osv.

## **Perimetersikring**

Perimetersikring betegner en barriere, der etableres i omkredsen af udendørsarealer med det formål at markere en afgrænsning af et område, hvortil der ikke ønskes adgang af uvedkommende. Ved

perimetersikring forstås normalt et udendørs hegn, der kan suppleres med et elektronisk overvågningssystem placeret på eller ved hegnet.

### **Personalekategorier**

Personalet kan kategoriseres som ledende medarbejder, eksternt servicepersonale, kunde, gæst, fremmede håndværkere etc.

### **Persondatalov**

Lov om behandling af personoplysninger, lov nr. 280 af 25. april 2001. Loven, der er trådt i kraft den 1. juli 2000, kaldes også persondataloven.

Loven har til formål - på baggrund af et EF-direktiv fra 1995 - at gennemføre en ny generel databeskyttelsesretlig regulering.

### **Personlig firewall**

En firewall er et system der er designet til at forhindre uautoriseret adgang til og fra virksomhedens netværk. Firewall'en checker al trafik f.eks. mellem Internettet og virksomhedens intranet og systemet kan sættes op til at blokere forskellige aktiviteter.

En firewall til en virksomheds netværk er ofte installeret på en dedikeret server.

En personlig firewall er en firewall der er installeret på den enkelte PC.

### **Privat sikkerhedsområde**

*Et privat sikkerhedsområde* er karakteriseret ved, at det er muligt at føre kontrol med adgang til og opholdsmuligheder i sikkerhedsområdet. Typisk for denne kategori er kontorer, opholdslokaler, lagerrum, værksteder og øvrige arbejdslokaler.

### **Proxkort (eller proxbrik)**

Forkortelse for *Proximity card*, et adgangskort (eller -brik) der ikke skal berøre kortaflæseren men blot holdes op foran 10 til 15 cm derfra for at give adgang. Det betyder, at kortet ikke slides på samme måde som f.eks. et magnetkort og derfor holder længere.

Kortet kan med fordel suppleres med en PIN-kode hvorved man opnår *two-factor authentication*.

Kortet kan desuden anvendes som *ID-kort*, der skal bæres synligt.

### **Rack Skab**

Reol eller reollignende skab som muliggør at mange servere kan opbevares (stables) på meget lidt plads.

### **Risikoanalyse**

En risikoanalyse har til formål at undersøge og vurdere de risici og trusler et informationsteknologisk system udsættes for. På dette grundlag er det muligt at tage stilling til hvilke egnede sikkerhedsforanstaltninger der skal tages.

### **Rollebaseret adgangskontrol**

Rollebaseret adgangskontrol giver mulighed for at klassificere brugerne i forskellige roller der giver dem forskellige adgangsrettigheder. Regler i ADK-anlæg kan bygge på Rollebaseret adgangskontrol.

### **Sikkerhedsniveau**

Dansk Standard 484 opdeler virksomhedens områder i fire niveauer: Et *offentligt sikkerhedsområde*, et *halvprivat sikkerhedsområde*, et *privat sikkerhedsområde* og et *særligt sikkerhedsområde*.

Karakteristika for hver af disse niveauer er beskrevet andetsteds i denne ordforklaring.

### **Skal(len)**

De bygningsdele, herunder vinduer, yderdøre og porte, der ud fra et indbrudssikringsmæssigt synspunkt danner begrænsning for et rumligt afgrænset område.

### **Social Engineering**

I sikkerhedssammenhæng betyder Social Engineering teknikker, der først og fremmest retter sig mod svagheder hos mennesker. Eksempelvis når en hacker opnår fysisk adgang til en pc eller et netværk ved at foregive at være ansat eller reparatør i firmaet.

### **Slusefunktion**

Her betegnelsen for en funktion der sikrer at adgang til et område foregår gennem to døre eller porte der aldrig er åbne på samme tid.

### **Smartcard**

Et elektronisk kort på størrelse med et VISA kort, der indeholder en microchip med hukommelse der kan indeholde data, og et operativsystem der kan køre programmer, kryptografiske funktioner mv.

### **Switch**

En switch er en netværksenhed der sorterer de pakker den modtager således at de forskellige computere i netværket ikke modtager datapakker som tilhører en anden maskine.

### **Særligt sikkerhedsområde**

*Et særligt sikkerhedsområde* er karakteriseret ved, at det udover at være privat har særlige forhold, der skal tages IT-sikringsmæssige hensyn til. Typisk stilles der skærpede krav til begrænsning af adgangsforhold og opholdsmuligheder, herunder til begrænsning af, hvilke *personalekategorier* der kan få adgang. Særlige sikringsområder er f.eks. lokaler, der inddeles i separate funktionsadskilte celler til f.eks. driftafvikling og overvågning, servere, kontorer med arbejdsstationer og printere, rum til teleudstyr og krydsfelter samt dataarkiver.

### **Teknisk personale**

Teknisk personale er i denne forbindelse IT-sikkerhedschef, systemadministrator eller netværksadministrator.

### **Token**

Her en autentifikations genstand (smartcard, USB nøgle el. lign.) som brugeren benytter til at få adgang til virksomhedens celler og computere.

### **Two-factor authentication**

En autentifikationsmodel der kobler to af de tre muligheder: 'noget du ved', 'noget du har' og 'noget du er'.

Se også *Multifactor autentifikation*.

**USB token**

En USB (Universal Serial Bus) token er et stykke hardware, der kan indsættes i computerens USB-port. Den kan indeholde en medarbejders personlige autentifikationsoplysninger så som en digital signatur.

**Virus**

En computervirus er et program eller et stykke kode der, hvis den inficerer en computer, kan replicere sig selv og gøre stor skade på data, programmer og operativsystem.

Antivirusprogrammer checker periodisk computeren for kendte vira således at der kan tages de nødvendige foranstaltninger til rensning af maskinen.

**VPN**

Forkortelse for Virtuelt Privat Netværk, et netværk der bruger Internettet til at transportere data, men som kan bruge kryptering og andre sikkerhedsmekanismer til at sikre at kun autoriserede brugere har adgang og at data ikke kan aflyttes.