IT-sikkerhedspolitik (Bilag 8a)

Lene Wiola Elberg
IT-sikkerhedskoordinator

I de efterfølgende afsnit beskrives de specifikke delpolitikker i den overordnede sikkerhedspolitik.

Informationssikkerhed anvender en række begreber og termer, som det er vanskeligt at omskrive uden at udvande betydningen af begrebet. Derfor er der vedlagt en ordliste, som Dansk Standard har udarbejdet, som beskriver hvad de enkelte begreber betyder.

Grundlæggende retningslinjer

Organisering og ansvar

Byrådet har udpeget kommunaldirektøren, som den øverste ansvarlige for kommunens informationssikkerhed. Der er etableret en sikkerhedsorganisation, der under ansvar overfor kommunaldirektøren, skal varetage de daglige opgaver i relation til informationssikkerheden.

Arbejdet i sikkerhedsorganisationen skal sikre, at sikkerhedspolitikken og tilhørende retningslinjer implementeres effektivt i Greve Kommune. Organisationen skal sikre, at sikkerhedsniveauet altid er i overensstemmelse med sikkerhedspolitikken og skal derfor etablere og vedligeholde rutiner, der overvåger, hvor effektivt informationssikkerheden er implementeret i kommunen.

Sikkerhedsorganisationen skal specifikt sikre, at der mindst en gang årligt foretages en gennemgang af informationssikkerhedspolitikken og den tekniske og faktiske implementering.

Centercheferne er over for kommunaldirektøren ansvarlig for de enkelte centres behandling af informationer, herunder overholdelse af Greve Kommunes sikkerhedsregler.

Centercheferne kan overlade nærmere afgrænsede dele af deres funktioner til områdeansvarlige, der derefter varetager disse funktioner under ansvar over for den pågældende centerchef.

Risikovurdering

Greve Kommune vil gennemføre risikovurderinger, som skal identificere og prioritere risici med udgangspunkt i Kommunens forretningsmæssige forhold. Risikovurderingen omfatter en overordnet vurdering af de forretningsmæssige risici, kommunen er udsat for ved anvendelse af informationsteknologi, men også mulighed for en mere dybdegående analyse i forhold til kritiske områder.

Såfremt en risikovurdering afdækker et relevant sikkerhedsbehov, skal de nødvendige sikringsforanstaltninger udvælges og implementeres for at få reduceret risikoen til et acceptabelt niveau.

Resultatet af risikovurdering samt sikkerhedsanalysen skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

Det skal sikres, at:

- Risikovurderingen foretages regelmæssigt og ved organisatoriske eller tekniske ændringer.
- Risikovurderingen foretages metodisk og systematisk, så resultater er sammenlignelige og reproducerbare.

Lovgivning

IT-anvendelsen i kommunen skal til enhver tid være i overensstemmelse med gældende lovgivning.

Det skal sikres, at:

- IT-anvendelsen er i overensstemmelse med lovgivningskrav, herunder gældende bestemmelser i "Persondataloven", medfølgende bekendtgørelser og vejledninger.
- Greve Kommune til enhver tid har de fornødne licenser til kommunens aktuelle IT-anvendelse.
- Der ikke installeres og/eller anvendes uautoriseret programmel, herunder fildelingstjenester, i kommunens IT-infrastruktur, dvs. driftsenheder, netværk, pc'er mm.

Klassifikation af data

For at kunne opretholde et ønsket sikkerhedsniveau, er det væsentligt at kunne identificere og klassificere de data, som skal beskyttes. I forbindelse med ændringer, der påvirker IT-miljøet, skal det sikres, at berørte systemer og data fortsat kan beskyttes i overensstemmelse med gældende krav. For at få overblik over eksisterende data og deres anvendelse, skal disse data registreres og klassificeres. Der skal tilknyttes en systemejer, som har ansvaret for vedligeholdelse af databeskrivelsen og har ansvaret for tildelingen af adgang til data.

Dataklassifikationen skal stille krav til håndteringen og opbevaringen for de pågældende data. Eksempelvis skal det ved introduktion af et nyt system sikres, at sikkerheden i systemet er i stand til at beskytte de data, som systemet anvender i overensstemmelse med datas sikkerhedsklassifikation.

Det skal sikres, at:

- Alle data grupperes og klassificeres i forhold til ønsket sikkerhedsniveau.
- Alle data registreres og tildeles et ejerskab på en hensigtsmæssig og overskuelig måde.
- Krav efter persondataloven fremgår eksplicit af klassificeringen.

Retningslinjer for fysisk og logisk sikkerhed

Fysisk sikkerhed

Der skal etableres en fysisk sikkerhed i og omkring Greve Kommunes IT-systemer, som reducerer risikoen for ekstern påvirkning af systemer og data samt uautoriseret fysisk adgang til Greve Kommunes IT-udstyr.

Der skal etableres fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, for ikke at data, og især personoplysninger:

- Hændeligt eller ulovligt tilintetgøres.
- Kommer til uvedkommendes kendskab.
- Misbruges eller behandles i strid med gældende lovgivning. og derved skal det sikres, at:
- IT-driftsmiljøet (centralt IT-udstyr og – netværkskomponenter) er beskyttet mod fysisk skade, herunder særligt strømsvigt, ekstrem varme, brand og indtrængende vand.
- IT-driftsmiljøet er sikret mod uautoriseret fysisk adgang.
- Adgang til kritisk infrastruktur eksempelvis serverrum logges.
- Alt udstyr med lagringsmedier kontrolleres for at sikre, at kritiske/følsomme informationer og licensbelagte systemer er fjernet eller overskrevet i forbindelse med at udstyret bortskaffes eller genbruges.

Logisk adgangskontrol til IT-ressourcer

Det er Greve Kommunes sikkerhedspolitik, at IT-infrastruktur, IT-ressourcer og kritiske data, skal beskyttes mod uautoriseret logisk adgang [1].

[1] Logisk adgang er adgang via netværket uden egentlig fysisk adgang til udstyr.

Det gælder såvel de dele, der udgør Greve Kommunes IT-netværk, men også centrale og decentrale servere, applikationer og tilhørende data. Adgangskontrol til pc-arbejdspladser skal sikre beskyttelse i det omfang, det måtte være muligt.

Målet med at etablere logisk adgangskontrol er således at mindske risikoen for tab af integritet og fortrolighed af data samt tilgængelighed af Greve Kommunes IT-systemer.

Krav til logisk adgangskontrol skal stemme overens med de sikkerhedsmæssige krav, som de involverede data og systemerne, som helhed måtte stille.

Det skal sikres, at:

- Adgangen til informationer styres ved logisk adgangskontrol på baggrund af informationernes sikkerhedsklassifikation.
- Der er tilstrækkelig logisk adgangskontrol på bærbare enheder og fjernarbejdspladser.
- Der ikke gemmes følsomme og personhenførbare informationer på bærbare enheder, der ikke er godkendt til formålet og ikke er tilstrækkeligt sikret.
- Alle adgangsmuligheder til komponenter koblet til Greve Kommunes IT-netværk er kendte og kontrolleret af IT-afdelingen, al trådløs kommunikation godkendes af IT-afdelingen inden etablering.
- Udvekslingen af information og systemer mellem medarbejdere eller organisationer foretages på en måde, der sikkerhedsmæssigt lever op til de krav, som de berørte data måtte kræve.
- Uautoriseret adgang og forsøg på adgang til netværk, systemer og data logges og undersøges.

Brugeradministration

For at kunne fastholde informationssikkerheden omkring systemer og data skal det gennem en hensigtsmæssig administration af brugerne sikres, at brugere kun kan få adgang til de specifikke data og systemer, som de er autoriseret til, og som deres arbejdsfunktion kræver for at kunne levere den rigtige ydelse til f.eks. borgerne i Greve Kommune.

Det er den systemansvarlige, der autoriserer adgangen til systemerne, og det er Supporten, der forestår oprettelsen og efterfølgende vedligeholdelse af brugerne i systemerne

Det skal sikres, at: ·

- Den overordnede adgangspolitik, udstikker rammerne for kontrol af logisk adgang til systemer og data. Forretningsgangene skal dække alle trin fra registrering af nye brugere til nedlæggelse af brugere, som ikke længere skal have adgang.
- Der er implementeret en hensigtsmæssig brugeradministration, hvor system/områdeansvarlig autoriserer adgang til data.
- Tildeling af adgangsrettigheder med udvidede beføjelser som giver brugeren mulighed for at omgå de systemtekniske beskyttelsesforanstaltninger, skal have særlig opmærksomhed.
- Brugerne skal gøres opmærksomme på deres ansvar, specielt vedrørende personlige adgangskoder og IT-udstyr.

Retningslinjer for drift og overvågning

Driftsafvikling og overvågning

Greve Kommune anser det for væsentligt, at kommunen kan levere en god service og kvalitet over for brugerne af IT-systemerne og dermed de borgere, som er afhængige af kommunens service. Det er derfor vigtigt, at driftsafviklingen foretages på en stabil, kvalificeret og sikker måde, således at tilgængeligheden og pålideligheden af systemerne sikres.

Dette nødvendiggør en formalisering omkring procedurer og instrukser for driftsafvikling og planlægning. Endvidere bør det tilstræbes, at der er en klar funktionsadskillelse for at forhindre tilsigtede fejl og misbrug.

Det skal sikres, at:

- IT-systemerne som minimum er tilgængelige for brugerne inden for normal arbejdstid.
- Procedurer for driftsafvikling dokumenteres og godkendes.
- Datamedier håndteres og opbevares på en sikker og forsvarlig måde.

Håndtering af sikkerhedsproblemer

Opståede IT-problemer skal håndteres på en måde, så det pågældende problem umiddelbart korrigeres alt efter graden af alvor i problemet. Alvorlige problemer skal endvidere være genstand for en analyse med henblik på at korrigere eventuelle årsager og uhensigtsmæssigheder, og dermed bidrage til den løbende forbedring af informationssikkerheden. Alvorlige problemer kan for eksempel være uautoriseret netværksadgang eller gentagne servernedbrud.

Det skal sikres, at:

- IT-problemer håndteres efter en vurdering af væsentligheden af problemet, således at såvel problem og eventuelle dybere liggende årsager og evt. sikkerhedsbrister korrigeres
- Medarbejdere og brugere deltager aktivt i rettelse af fejl, løsning af problemer og forbedring af Informationssikkerheden.
- IT-afdelingen og IT-sikkerhedskoordinatoren fører log over alvorlige hændelser, med henblik på at opretholde dokumentation af et hændelsesforløb.

Sikkerhedskopiering

Det er væsentligt, at Greve Kommune til en hver tid kan fremfinde de informationer, som anvendes i forbindelse med kommunens aktiviteter. Derfor skal der etableres procedurer for sikkerhedskopiering og backup, som sikrer, at data og systemer kan retableres i tilfælde af tab af systemer og data.

Det skal sikres, at:

- Data sikkerhedskopieres i overensstemmelse med dataklassifikationen, lovgivningskrav og beredskabsplanlægningen.
- Der foretages verifikation af, at sikkerhedskopier kan genindlæses regelmæssigt. Sikkerhedskopier opbevares sikkert og uden for Greve Kommunes lokaliteter, således at disse altid kan fremfindes ved igangsættelse af nødplaner eller i forbindelse med andet behov.

Beskyttelse mod ondsindet programmel

Ondsindet programmel udgør en stor trussel mod tilgængelighed af systemer og integriteten af data. Der skal derfor på samtlige relevante punkter være etableret en veldefineret og effektiv beskyttelse mod ondsindede programmer.

Det skal sikres, at:

- Der etableres og vedligeholdes foranstaltninger til at forhindre og konstatere angreb af skadevoldende programmer.

Retningslinjer for håndtering af ændringer

Udvikling og anskaffelse af hard- og software

IT-systemerne og netværk indgår som et væsentligt element i det daglige arbejde i Greve Kommune. Det er derfor af vital betydning, at nyanskaffelser og opdateringer af hardware og software lever fuldt op til den eksisterende kvalitets- og sikkerhedsstandard.

Da Greve Kommune samtidig har valgt ikke at påtage sig udvikling af eget programmel i nævneværdigt omfang, vil det være nødvendigt at sikre, at Greve Kommune udelukkende anvender pålidelige og kompetente leverandører, samt at der anvendes standardprodukter fra pålidelige leverandører i størst muligt omfang.

Det skal sikres, at: ·

- Der indarbejdes en tilstrækkelig sikkerhed og kontrol i alle systemer, såvel standardsystemer som specialudviklede eller tilrettede systemer.
- Al IT-udstyr godkendes af IT-afdelingen.
- Alle systemer, der behandler personhenførbare data, vurderes af en sikkerheds - og juridisk medarbejder i samarbejde med henblik på en afgørelse om, hvorvidt databehandlingen skal anmeldes til Datatilsynet.
- Krav til nye systemer eller ændring af eksisterende systemer omfatter krav om kontrol- og transaktionsspor, automatiske kontroller, samt den generelle sikkerhed.
- Der er sikkerhed og kontrol i udviklings- og vedligeholdelsesprocessen.

Håndtering af konfigurationsændringer

Ændringer i konfigurationen af hardware og software kan have konsekvenser for sikkerheden i IT-anvendelsen. Derfor bør sådanne ændringer kun implementeres, hvis der er tilstrækkelig sikkerhed for, at disse ikke medfører svagheder i sikkerheden. Derfor skal der være en klar formel retningslinje for håndtering af konfigurationsændringer for at forhindre fejl. Dette gælder også, hvis det er eksterne samarbejdspartnere og leverandører, som foretager den tekniske implementering.

Det skal sikres, at:

- Konfigurationsændringer planlægges, kvalitetssikres og godkendes af IT.

Øvrige retningslinjer

Krav til eksterne parter og leverandører

Konsulenter med adgang til systemer skal være underlagt de samme krav, som beskrives i sikkerhedspolitikken og tilhørende retningslinjer. Andre eksterne parter og leverandører skal ligeledes leve op til de sikkerhedskrav, som Greve Kommune stiller.

Det skal som udgangspunkt sikres, at:

- Konsulenter, som har adgang til Greve Kommunes systemer, er underlagt sikkerhedskrav mindst svarende til sikkerhedsniveauet hos Greve Kommune.
- Sikkerheden i leverancer fra outsourcing partnere/leverandører er på et niveau mindst svarende til sikkerhedsniveauet hos Greve Kommune.

Beredskabsplanlægning

Der skal etableres et beredskab, som skal sikre, at Greve Kommune i tilfælde af større driftsnedbrud eller egentlige katastrofer er i stand til at genoptage kritiske forvaltningsmæssige aktiviteter inden for en acceptabel tidshorisont. De større driftsnedbrud eller katastrofer betyder tab af tilgængelighed af væsentlige systemer, udstyr og/eller faciliteter, hvorfor retablering af tilgængeligheden af disse er et centralt område i beredskabsplanlægningen.

Det skal sikres, at:

- Der er beskrevet en beredskabsstyrings proces som klart beskriver organisation, eskalering og ansvar.
- Kritiske forvaltningsmæssige aktiviteter kan fortsætte inden for ledelsesgodkendt tidshorisont i tilfælde af større driftsforstyrrelser, nedbrud, større brud på sikkerheden eller større katastrofer.
- Beredskabet altid er ajourført og testet.

Medarbejdere

Medarbejdere i Greve Kommune skal på baggrund af deres kendskab til og ansvar for sikkerhed motiveres til at bidrage til en opretholdelse af sikkerheden i Greve Kommune. En del af medarbejderne i kommunen har adgang til centrale fortrolige informationer i IT-systemerne bl.a. via administratorrettigheder. Ved ansættelse af sådanne betroede medarbejdere skal disse gennemgå en særlig screening, der bidrager til vurderingen af den pågældende person.

Det skal sikres, at:

- Medarbejderne har kendskab til Greve Kommunes informationssikkerhedspolitik.
- Medarbejderne uddannes i nødvendigt omfang til at kunne anvende Greve Kommunes IT-systemer i overensstemmelse med gældende sikkerhedspraksis.
- Medarbejdere motiveres til at bidrage til den samlede sikkerhed i Greve Kommune.
- Medarbejderne er bekendt med potentielle personlige og kommunale konsekvenser for bevidst og ubevist brud på sikkerheden.
- Der er en formel proces i forbindelse med ansættelse, rokering og ansættelsens ophør.

Logning og audit

For at sikre at uautoriserede handlinger registreres, opsættes der logning på infrastruktur elementer, samt kritiske systemer og systemer, som er omfattet af reglerne i Persondatalovgivningen. Logningen sikrer, at uønskede forhold konstateres, samt verificerer at sikringsforanstaltningerne fungerer efter hensigten. Logningen tager udgangspunkt i DS484:2005 afsnit 10.10 samt Sikkerhedsbekendtgørelsen.

Det skal sikres, at:

- Der dannes en opfølgningslog, som registrerer brugeraktiviteter, afvigelser og sikkerhedshændelser. Denne log skal opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.
- Brugen af kommunes IT-systemer skal overvåges, og der foregår en løbende opfølgning på hændelser.
- Aktiviteter udført af systemadministratorer og –operatører, samt andre med særlige rettigheder logges.
- Fejl logges og analyseres, og nødvendige udbedringer og modforholdsregler gennemføres.
- Logoplysninger beskyttes mod manipulation og tekniske fejl.

For at sikre at Greve Kommune lever op til retningslinjerne i sikkerhedspolitikken, vil der løbende foretages audit. Auditeringen har til formål at sikre, at politikken efterleves, og at der opsættes handleplaner i forhold til eventuelle afvigelser.

Termer og definitioner

Nedenfor findes en ordforklaring for de begreber, som anvendes i vores sikkerhedspolitik samt tilhørende bilag.

Ordforklaring

Adgangskontrol – fysisk
Enhver fysisk sikringsforanstaltning mod uautoriseret adgang til et sikkerhedsområde.

A**dgangskontrol – logisk**
Enhver programmerbar sikringsforanstaltning mod uautoriseret anvendelse af en virksomheds informationsaktiver.

Adgangskontrolliste
En liste over brugere og deres tildelte autorisationer og rettigheder til at anvende virksomhedens informationsaktiver. Se også "autorisation" og "rettigheder".

Adgangskode (password) Kombination af tegn, som benyttes til verifikation af en brugers identitet.

Aktiver
Alt, der har værdi for virksomheden – således også immaterielle værdier som fx informations behandlingssystemer, data, procedurer og dokumentation. Se også "informationsaktiver".

Applikationssystem
Se "informationsbehandlingssystemer".

Arbejdsstation/plads
Betegnelse på en PC, skærmterminal eller lignende, der benyttes af en enkelt bruger, og som er tilkoblet et netværk, der giver mulighed for at anvende fælles ressourcer og datakommunikation.

Arkiv (dataarkiv)
Opbevaringssted, hvor man systematisk opbevarer data på maskinlæsbare medier.

Autenticitet
Egenskab, der sikrer, at en ressource eller person er den hævdede (anvendes fx ved log-on og elektronisk underskrift/ digital signatur).

A**utentificering/autentifikation**
Verifikation af en afsenders eller en modtagers autenticitet.

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

Backup af data

Sikkerhedskopieringsaktivitet. Lagring af vigtige data og programmer på et eksternt lagermedie, der kan opbevares sikkert og anvendes i tilfælde af, at de originale data er gået tabt.

Barriere

Fysisk afgrænsning, der har til formål at danne en adskillelse mellem et bestemt område og omgivelserne. Afgrænsningen kan være reel (fx væg) eller eventuelt være symbolsk (fx malet linje på gulv suppleret af adgang forbudt skilt).

Basissystemer

Opdeles i operativsystem(er) og hjælpeprogrammer. Se også "informationsbehandlingssystemer".

Beredskabsplan

En skriftlig, opdateret dokumentation for, hvad der skal iværksættes af definerede redningsaktioner, og hvem der skal igangsætte disse, hvis der indtræder en forstyrrende afbrydelse af virksomhedens forretningsprocesser, der kræver en redningsaktion.

Bibliotek (for data og programmer)

Et system, der registrerer opbevaring af og fører kontrol med til- og afgang af fx basis- og netværksprogrammer, brugerprogrammer, udviklings- og testprogrammer, programkildekoder og data, samt hvilke brugere der har fået tilladelse til at anvende disse. De forskellige biblioteksdele holdes adskilt.

Brugerprogram/system

Se "informationsbehandlingssystemer".

Centralt udstyr

Informationsbehandlingsudstyr, hvor flere arbejdsstationer (klienter) er tilsluttet en server eller en samling af servere ("cluster"). Se også "informationsbehandlingsudstyr".

Data

En formaliseret repræsentation af kendsgerninger eller instruktioner.

Se også "information".

Dataansvarlig

En person der er udpeget til at have sikkerhedsmæssigt ansvar for et system- og/eller data.

Se også "ejer".

Dataintegritet

Se "integritet".

Datamedier

Fysiske lagringsmedier, hvorpå der ad elektronisk vej er lagret data, fx på disketter, bånd, diske, CD-ROM, EPROM, USB-lagringsenheder.

Dekryptering

Den modsatrettede proces af en kryptering.

Diagnoseport

Tilkoblingsstik i informationsbehandlingsudstyr til kommunikationsforbindelse med ekstern servicetjeneste. Via kommunikationsforbindelsen kan en servicetekniker fra et andet geografisk sted registrere udstyrets driftstekniske data, statusinformationer og øvrige informationer samt foretage fejlrettelser, under forudsætning af at diagnoseporten er aktiv/åben. Se også "port".

Digital signatur

En digital signatur dannes ved en kryptografisk transformation af en hashværdi beregnet ved hjælp af meddelelsen, og som knyttes til denne. Bruges til verifikation af meddelelsens integritet og til verifikation af afsenderens autenticitet.

"Ejer"

For manuelle systemer er der ofte i en virksomhed en naturlig forventning til, hvem der er "ejer" af et system og dets informationer, og at "ejeren" har såvel ansvar som rettigheder vedrørende informationerne. Bogholderen "ejer" de finansielle informationer, salgslederen "ejer" de afsætningsmæssige informationer, og lagerforvalteren "ejer" de beholdningsmæssige informationer. Ansvar for og rettigheder til systemer og informationer bliver ofte mere diffust, når et system digitaliseres. Derfor er det nødvendigt, at der gøres noget aktivt for at bibeholde dette ansvar. "Ejeren" bestemmer, hvilke brugere der kan anvende et system og dets informationer.

Engangskode

En logisk adgangskontrolmetode, hvorved den opkaldte parts valideringssystem er synkroniseret med en brugers transportable kodeomsætter (kan være elektronisk eller blot en udskrevet liste). Brugeren benytter et givet kodeord i omsætteren, der omsætter til en engangskode ved hjælp af en indbygget algoritme eller ved simpelt tabelopslag. Den nye kode kan kun benyttes en gang. I visse systemer skal den benyttes øjeblikkeligt, idet den kun er gyldigt i en kort periode.

Entitet

En uafhængig enhed, der har selvstændig eksistens, fx en node/en person.

Firewall

Se "logisk filter".

Fortrolighed

Egenskaben, at informationen ikke gøres tilgængelig eller kan afsløres for uautoriserede personer, entiteter eller processer. Se også "konfidentialitet".

Fysisk sikring

Sikringsforanstaltninger, der baserer sig på fysiske eller mekaniske foranstaltninger for imødegåelse af tyveri, indtrængning, hærværk, eller anden ødelæggelse af aktiver. Se også "tyverisikring, mekanisk".

Hacking

Betegner den ulovlige handling, at en ukendt og uautoriseret person i det skjulte anvender andres informationsbehandlingsudstyr, systemer, informationer eller data. Handlingen udføres fx ved hjælp af teknisk omgåelse af de logiske adgangskontrolsystemer. Se også "penetrering".

Hashværdi

En gentagelig beregning med hjælp af bestemte algoritmer af fx et programs "tværsum" til verifikation af, at selve programmet ikke er ændret.

Hemmeligholdelse

Sikkerhed for, at indholdet af en meddelelse ikke kan afsløres af uvedkommende.

Hjælpeprogram

Standardbetegnelse for værktøjsprogrammer, der anvendes til fx editering, filkopiering, filsammenligning, fejlrettelser og optimering.

Inddata

Alle data, der overføres til eller indrapporteres i et informationsbehandlingssystem.

Information

Den mening, der tillægges en mængde af data. Se også "data".

Informationsaktiver

De aktiver, der har tilknytning til og er nødvendige for virksomhedens informationsbehandling.

Informationsbehandlingssystemer

Betegnelsen for en samling programmer til løsning af en samlet mængde opgaver. Grundlæggende opdeles informationsbehandlingssystemer i to hovedgrupper:

– **Basissystemer**, der oftest er hardwareafhængige, består af **operativsystem**(er) og **hjælpeprogram**(mer). Basissystemer, ofte benævnt styre-, system- eller driftssystemer, er grundlaget for al informationsbehandling og skal være i funktion, før alle andre programmer kan anvendes. Operativsystemerne styrer kommunikationen mellem datamaskinen, andre datamaskiner, andet udstyr og brugerprogrammer og brugere. Hjælpeprogrammerne er værktøjer, der benyttes til fx at rette fejl i operativsystemet eller foretage optimering af driften på informationsbehandlingsudstyret.

– **Brugersystemer**, der er afhængige af det valgte basissystem, opdeles i **egenudviklede systemer** og **standardsystemer**.

· Egenudviklede systemer er unikke, specialudviklede programmer til specifikke opgaveløsninger eller sammenhængende opgavekomplekser i en virksomhed eller mellem flere virksomheder. De udvikles som en specialopgave af en udvalgt programleverandør eller af en virksomheds egne programmører.

· Standardsystemer er universelle programmer til løsning af virksomheders generelle arbejdsopgaver som fx bogholderi, lønningsregnskab, ordre- og lagerstyring, kalkulation, tekstbehandling og illustrationstegning. Standardsystemer anskaffes fra mange forskellige lagerførende leverandører.

De kan af den enkelte bruger ved at vælge mellem nogle indbyggede parametermuligheder tilpasses dennes ønsker om opsætning og de regelsæt, hvorefter standardsystemet skal fungere. Ofte sammensættes flere af ovennævnte programtyper til en integreret programpakke/ office suite.

Informationssikkerhed

Alle aspekter relateret til definering, gennemførelse og vedligeholdelse af fortrolighed, integritet, tilgængelighed, ansvarlighed, autenticitet og pålidelighed omkring informationsbehandlingssystemer.

Informationssikkerhedspolitik

Ledelsens overordnede retningslinjer for strategier, direktiver og forretningsgange, der regulerer, hvordan virksomhedens informationer, inklusive følsomme oplysninger, anvendes, styres, beskyttes og distribueres i virksomheden og dens informationsbehandlingssystemer.

Integritet

Sikkerhed for, at indholdet af en meddelelse eller en post i et register er korrekt og komplet.

IT-revision

Aktivitet, der udføres til kontrol af, at den ønskede informationssikkerhed i henhold til virksomhedens politik for informationssikkerhed og forskrifter for informationsbehandling er til stede og efterleves. Revisionen dokumenteres og forelægges virksomhedens ledelse.

Karakter

Ethvert stort eller lille bogstav, tal eller tegn, der anvendes enkeltstående eller som en tilladelig sekvens.

Kildekode

Et informationsbehandlingsprogram, der er skrevet i et symbolsk og standardiseret programmeringssprog.

Klartekst

Ubeskyttet og umiddelbar læselig tekst.

Kompatibilitet

Den forenelighed, der skal være til stede, for at noget (et system) kan virke sammen med noget andet (andre systemer).

Konfidentialitet

Se "hemmeligholdelse".

Kontrolspor

En specificeret udtrækning og samling af data, hvormed det kan konstateres, hvilke transaktioner der er udført, hvornår og af hvem, og hvilke direkte og indirekte konsekvenser de har haft på tidligere eller oprindelige data.

Kryptering

Omsætning (kodning) af læsbar klartekst, således at teksten ikke er læsbar for udenforstående, uden at de er i besiddelse af krypteringsforskriften og krypteringsnøglen.

Log off

Er den afsluttende procedure for brugeren af et informationsbehandlingssystem, hvorved forbindelsen mellem en arbejdsstation og programmerne afbrydes.

Log on

Er den nødvendige indledende procedure, hvormed en bruger etablerer sin tilladelse til at anvende informationsbehandlingsudstyr og -systemer.

Logisk bombe

En række destruktive programmer eller makroer, der er skjult i et i øvrigt normalt informationsbehandlingssystem, der regelmæssigt køres. Den destruktive kode aktiveres, når nogle forudsatte betingelser er opfyldt. Man kan fx tænke sig en logisk bombe indlagt i et firmas lønberegningssystem. Den logiske bombe udløses, når en medarbejder ikke længere er på lønningslisten. Bomben ødelægger fx vitale firmadata.

Logisk filter

Et filtreringssystem, fx en kombination af en router og nogle programmerede kontroller ved den grænse, hvorigennem datakommunikationen skal passere for at komme fra et netværk til et andet netværk. Ved grænsen bliver datakommunikationen tilladt, videredirigeret eller nægtet passage baseret på et sæt vedtagne regler.

Lokalnetværk (LAN)

Et netværk, der benyttes til datatransmissioner mellem forskelligt informationsbehandlingsudstyr inden for samme virksomhed, og som i nogle tilfælde kobles sammen med andre interne og eksterne netværk, med offentlige netværk eller andre datakommunikationsforbindelser. Se også "netværk".

Makulering

Destruktion, strimling eller sønderrivning af læsbare medier i strimmel- eller flagestørrelser, der ikke kan gensammensættes til læsbare informationer.

Netværk

Generel betegnelse, der dækker alle typer af sammenhængende datakommunikationsforbindelser mellem "centralt udstyr", servere, arbejdsstationer og andet kommunikationsudstyr.

Node

Adresserbart punkt på et datanetværk (fx en arbejdsstation, printer, switch, netværksomskifter, router).

Objektkode

Et maskinlæsbart program, der umiddelbart kan afvikles på en datamaskine.

Operativsystem

Et grundlæggende program eller programkompleks, der foretager den overordnede styring af alt, hvad der kan afvikles på informationsbehandlingsudstyr.

Opgradering

Udskiftning af hidtil anvendt informationsbehandlingsudstyr og -systemer med andet kompatibelt materiel, som kan yde mere eller muliggøre bedre rationel anvendelse.

Opkobling

Etablering af en datakommunikationsforbindelse.

Orm

Et selvstændigt program, der er i stand til at lave kopier af sig selv hele tiden uden at være afhængig af et andet program. Kan spredes via datanetværk og databærende medier m.v. til andet udstyr, hvor ormen starter sig selv og derved stjæler datakraft fra udstyret, som herved "overbelastes".

Overvåget område

Et afgrænset område, der fx elektronisk tyveri- og brandovervåges af et automatisk alarmeringsanlæg.

Password

Se "adgangskode".

Penetrering

At skaffe sig mulighed for ulovligt at anvende informationer, data eller datasystemer uden at have den fornødne autorisation og uden at blive opdaget. Se også "hacking".

Piratkopiering

At foretage kopiering af et informationsbehandlingsprogram eller information i strid med lovgivningen om licensaftaler.

Port

Generel betegnelse for elektriske kredsløb, der virker som interface mellem informationsbehandlingsudstyr, arbejdsstation og andre ydre tilsluttede enheder via datakommunikationsforbindelser.

Privilegier

Betegnelsen for de rettigheder, som specificeres for en autoriseret bruger til legalt at anvende en vedtagen delmængde af informationsbehandlingsressourcer, herunder data, til sine arbejdsopgaver.

Protokoller

Regler, som er reguleret af standarder, normer, tekniske metoder og specifikationer, der er fastsat med det formål at kunne fortolke og udveksle data.

Pålidelighed

Egenskab, der sikrer, at den forventede opførsel og de forventede resultater opnås.

Rettigheder

Se "privilegier".

Risiko

Det beregnede eller konstaterbare resultat af en kombination af hyppigheden af en uønsket hændelse og omfanget af konsekvenserne (tabene).

Risikoanalyse

En detaljeret og systematisk procedure til at afdække virksomhedens trusler og sårbarheder samt konsekvenserne af uønskede hændelser.

Risikostyring

Den ledelsesmæssige styring af virksomhedens indsats for at imødegå forretningsmæssige risici.

Risikovurdering

En overordnet afvejning af virksomhedens risikobillede.

Sikkerhed

Resultatet af alle de sikringsforanstaltninger, der er foretaget for at imødegå de aktuelle trusler.

Sikkerhedsmiljø

Det samlede sæt af sikringsforanstaltninger og kontroller, virksomheden har etableret for at sikre, at sikkerhedspolitikken bliver efterlevet.

Sikkerhedsstyring

En løbende proces, hvor ledelsen gennem en systematisk rapportering om ændringer i risikobilledet, observerede svagheder samt konkrete hændelser til stadighed kan revurdere den fastlagte sikkerhedsstrategi og foretage de fornødne justeringer for at fastholde det ønskede sikkerhedsniveau.

Sikret område

Et område, hvis afgrænsninger er mekaniske/fysisk indbrudssikrede.

Sikringsforanstaltning

En praksis, procedure eller mekanisme, der reducerer sårbarheden. Dvs. alle de bestræbelser, forholdsregler og foranstaltninger, der tages i anvendelse for at modvirke såvel utilsigtede som tilsigtede fejl, tab og misbrug af data samt sikring af tilgængelighed for de autoriserede brugeres anvendelse af udstyr og data.

Single sign-on-procedure

Log on-procedure, der bevirker, at det ikke er nødvendigt efter den første log on-procedure at foretage selvstændige log on til flere specifikke systemer.

Skrivebeskyttelse

Sikringsforanstaltning, der har til formål at forhindre utilsigtede tilføjelser, ændringer eller sletninger af eksisterende data på datamedier.

Standardsystem

Se "informationsbehandlingssystemer".

Sårbarhed

Mangel på sikkerhed, som kan medføre uønskede hændelser.

Test

Verifikation af kvaliteten af et givet system og/eller program.

Tilgængelighed

Egenskaben at være tilgængelig og anvendelig ved anmodning fra en autoriseret entitet.

Transaktionsspor

Se “kontrolspor”.

Trojansk hest

Et program, der ser ud og virker som et almindeligt program, men som indeholder en eller flere uautoriserede programkommandoer eller programsekvenser.

Trussel

En potentiel årsag til en uønsket hændelse, som kan forvolde skade på virksomheden.

Tyverisikring, mekanisk

Hensigtsmæssig anvendelse af bygningsdele, låseenheder mv., således at tyveri og utilsigtet gennembrydning eller oplukning vanskeliggøres. Bygningsdele kan f.eks. være specielt udformede eller forstærkede.

Uddata

Alle data der, efter endt behandling i informationsbehandlingsudstyret, enten placeres i et baggrundslager eller et eksternt datamedie eller overføres til en printer for udskrift.

Uafviselighed

En procedure der beviser, at en specifik bruger på et givet tidspunkt har sendt en anden specifik bruger en bestemt meddelelse.

Validering

Kalkulation og kontrol af, at indrapporterede datas værdi eller et givet tegn eller ord er indeholdt i et forudbestemt gyldigt værdiinterval, fx er datoen den 30. gyldig for januar men ikke for februar måned.

Virus

En programkode, der er skjult og udfører handlinger, som brugeren ikke har tiltænkt. Handlingen har typisk en skadende eller ødelæggende virkning på data eller programmer. En virus laver kopier af sig selv og kan sprede sig selv til harddiske og netværk eller til andet udstyr via netværk og flytbare datalagringsmedier.

Åbent net

Et netværk, som er umiddelbart og offentligt tilgængeligt for alle, der har indgået en anvendelsesaftale, og som har det nødvendige udstyr, fx internet og telefonnettet.