Risici ved forsikringer der dækker tab som følge af IT.relaterede skader

af Truels Kjær

Truels Kjær
tuk@codan.dk

Forsikringsbranchens berettigelse har til alle tider været at overtage den risiko der kan true en privatperson eller virksomheds eksistens. Den væsentligste risiko har altid været, og er stadig brandrisikoen. Men nye og ukendte risici er opstået i forbindelse med computerteknologiens udvikling, IT-relaterede skader og risici, samlet i det det nye begreb e-risk. Alt for få virksomheder har gjort sig klart hvilke alvorlige konsekvenser disse skader kan få. Tidligere var afhængigheden størst hos de teknologitunge virksomheder. Dette har ændret sig markant, således at alle kategorier af virksomheder er afhængige af deres IT-anlæg og data i en grad der først konstateres når skaden er sket. Hvilke risici er der? Hvordan håndteres de af forsikringsbranchen?

I det følgende vil IT-relaterede risici blive vurderet, herunder eksempler på skader og hvilke forholdsregler man kan tage.

Det vil være naturligt at dele risikobilledet op i skader og tab relateret hhv. til hardware og til data.

Hardware

Hardwareskader er de traditionelle kaskoskader, tyverier, lynskader og brand. Ud over brand- og tyveridækningen er standarddækningerne de gængse kaskodækninger, med tilhørende udvidelser og tillægsdækninger så som databærer og meromkostninger.

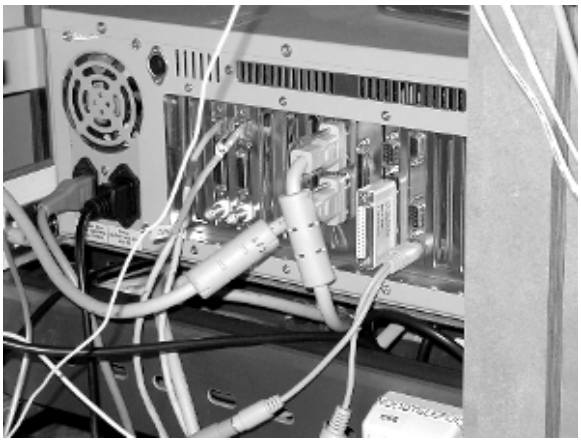
Kaskoskader

Den tekniske udvikling kombineret med leverandørernes prispolitik, har medført at den økonomiske risiko ikke så meget er skade på den enkelte pc, men mere på de "udenomsinstallationer" som kobler pc'erne sammen i netværket, samt arbejdsløn til installation af udstyret. Netværkskomponenternes ydeevne og kompleksitet har dels gjort dem til nøglekomponenter og dels været den del af IT-installationen der ikke har været omfattet af prismæssig konkurrence.

Hardwarelås /dongle

Der er en særlig komponent der traditionelt har været bekostelig at erstatte. Hardware-

Truels Kjær er akademiingeniør og er ansat i Codan Forsikring's ingeniørafdeling. Han beskæftiger sig blandt andet med produktudvikling, risikovurdering og skadebehandling af industrianlæg, specielt energianlæg og anlæg hørende til e-risk. Deltager i arbejdsgruppen for sikring af data under F&P.



Figur 1.
Dongle hørende til program i kraftværkssektoren. Nypris ca. kr. 200.000 for licensrettigheden, der også typisk er kravet ved tyveri af pc/dongle.

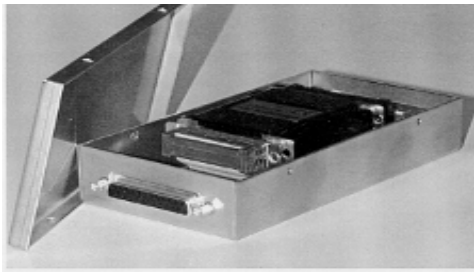
låsen eller dongelen som den også benævnes. Den fungerer som programbeskyttelse for et program, og sikrer mod uautoriseret kopiering af det program den skal beskytte. Det er en elektronisk dims på størrelse med en tændstikæske, og den monteres i printerstikket bag i netop den pc hvor det pågældende program er installeret og afvikles fra, og programmet fungerer kun hvis dongelen er monteret.

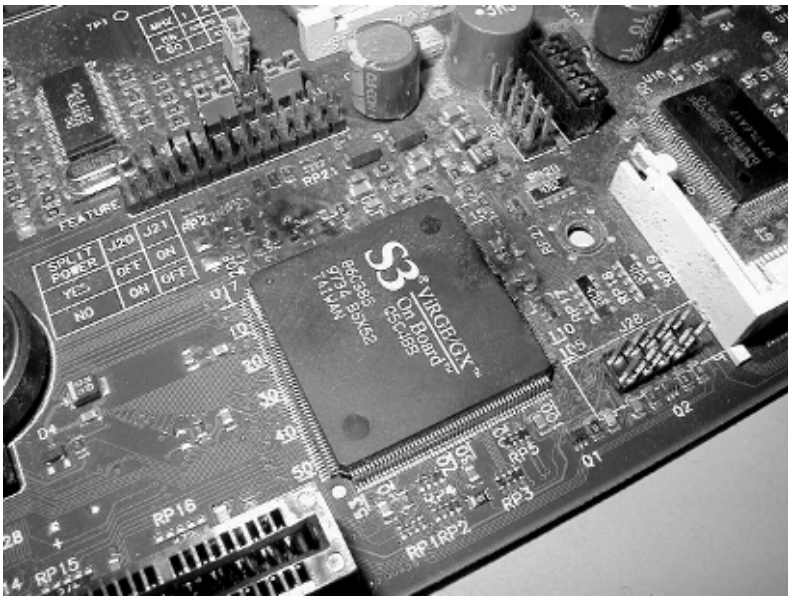
Problemet opstår ved tyveri af pc'en, hvor dongelen da følger pc'en og dermed også forsvinder. I erstatningssituationen hævder leverandøren af programmet typisk, at licensrettigheden og dongelen er en og samme ting, hvorfor genlevering af en ny dongle skal afregnes med den fulde nyværdi af programmet. Dvs. kravet for en dongle der i indkøb koster i størrelsesordenen 500 kr, er fra kr 20.000 til kr 1 mio., afhængig af programmets nypris. Forsikringstager er som regel fortørnet over kravet, der er både ulogisk og urimeligt, da han allerede har betalt for licensrettigheden. Hvordan kan man stjæle en licensrettighed? Tendensen hos de fleste forsikringsselskaber er dog blevet, kun at give erstatning for selve dongelens pris, samt selvfølgelig geninstallering af programmet. Samtidig kan der stilles krav om, at dongelen placeres i en aflåst boks væk fra pc'en, men tilsluttet denne via et kabel. En enkel men effektiv måde at sikre sig mod at dongelen utilsigtet forsvinder ved tyveri af pc'en.

De væsentligste afvigelser indenfor forsikringsbranchen er hvilke sikringsmæssige krav der stilles. Nedenstående eksempler på sikring er enten gode råd til forsikringstager eller krav og forudsætning for dækning ved skade:

- Overspændingsskader fra lyn: Lynbeskyttelse i form af overspændingsafledere, potentialudligning, online UPS, forbindelse med fiberkabler

Figur 2. *Sikring af dongle i en dongleboks der placeres væk fra pc'en.*





Figur 3. *Typisk lynskade på elektronik*

- Tyveri af IT-udstyr: AIA anlæg, kameraovervågning med alarmoverføring, fastgørelse i sikkerhedskabinetter, sløring med røgmaskiner, mærkning, så vidt muligt undgå fladskærme og bærbare pc'er.
- Nedbrud af IT-udstyret: Katastrofeplan (?), servicekontrakter, dokumenterede anlæg og konfiguration

Software /data

Håndteres vidt forskelligt selskaberne imellem, hvilket bunder i, at det i praksis er næsten umuligt at få reassurancedækning.

Virus og hacking. I love You

Elektronisk Data Behandling har med en lidt fortærsket vending undergået en helt utrolig og uforudsigelig udvikling gennem de seneste 20 år. Normalt er det industrien der forestår den tekniske udvikling, drevet af et ønske om vækst og produktion af forbrugsgoder. Indenfor edb er der yderligere en med/modspiller, nemlig den anonyme nørd der sidder hjemme på sit værelse og herfra har mulighed for kontakt med alverdens edb-systemer, og dermed i princippet har mulighed for at påvirke ethvert system. Og netop det forhold, at den elektroniske infrastruktur giver ham mulighed for reelt at nå hele verden, giver nogle hidtil ukendte risici. Vi fik et håndgribeligt forvarsel om hvor sårbare vi alle er, da en nørd i et fremmed land sendte computervirusen „I love You" ud på den elektroniske motorvej og inficerede et hidtil uset stort antal professionelle computere over hele verden. Det chokerende var den hastighed hvormed virussen bredte sig over hele verden, og at den var i stand til at inficere selv det sikreste system. Indenfor kort tid havde virussen bredt sig til så at sige hele verden, og antivirusprogrammørerne kunne kun komme for sent med et brugbart antivirusprogram. Til alt held var "I love You" en forholdsvis fredelig virus, således at den ikke udviklede sig til en større katastrofe, og set i bakspejlet har vi lært meget af den. Det blev slået fast at antivirusprogrammer er et must, men samtidig nødvendigheden af at antivirusprogrammet er

opdateret. Endvidere at det er vigtigt at udnytte tidsforskellen jorden rundt til at udvikle og opdatere antivirusprogrammer. Det er derfor af afgørende betydning at antivirusleverandøren har et globalt netværk.

Igen gik forsikringsverdenen i chok

Igen gik forsikringsverdenen i chok, og gjorde straks undtagelse for dækning af skader som følge af virusangreb.

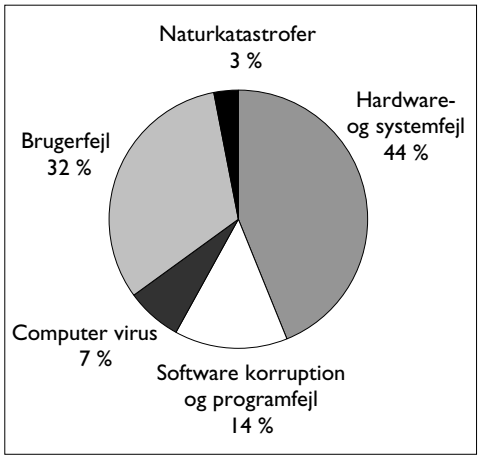
Seneste chok var frygten for konsekvenserne af år 2000-problemet, hvor primært edb-branchen fremmanede spøgelser af hidtil usete dimensioner. Konsekvensen blev, at mængder af ældre IT-udstyr blev skrottet på mistanken om at elektronikken f.eks. ikke kunne håndtere datoen 9.9.99 eller skiftet fra 1999 til 2000. Katastrofen udeblev heldigvis, men det blev meget tydeligt illustreret hvor afhængige og dermed sårbare vi er af elektronikken.

Reelt må vi nok se i øjnene, at skader som følge af virus kan blive økonomisk uoverskuelige pga. risikoen for ukontrolleret worldwide udbredelse. Den for forsikring så vigtige forudsætning, at risikoen kan kalkuleres, er derfor ikke opfyldt, og drevet af manglende reassurance, har forsikringsbranchen intet standardprodukt der dækker skade som følge af computervirusvirus.

Tab af data

For forsikringsbranchen er virustruslen den alvorligste, da skaderne som ovenfor nævnt ikke kan kalkuleres. Men for den enkelte forsikringstager, er den største risiko for tab af data utilstrækkelig backup kombineret med kvajeskader (egne medarbejdere eller leverandører) eller tyveri.

Det er til tider rystende at konstatere hvor lemfældigt mange virksomheder håndterer backupproblematikken. Og først i tilfælde af tab af data indser virksomheden hvor essentielle de er.



Figur 4. *Statistisk fordeling af årsagen til datatab i 2000. Tab som følge af virus er voksende pga. at virusprogrammørerne er blevet dygtigere og virus er blevet mere "ondsindet".*

Eksempel:

- Moderne tandlægeklinikker bliver mere og mere papirløse. Det betyder at alle patientaftaler, journaler, økonomi, røntgenbilleder og behandlingsplaner er gemt som data. At miste dem vil være fatalt og rekonstruktion ofte umulig.
- De fleste maskinfabrikker har programmeringen af CNC-maskinerne liggende som data. Hele virksomhedens produktion er afhængig af disse.
- Størstedelen af dagens virksomheder har hele virksomhedens økonomi liggende som data. Det være sig kundekartotek, debitorer, kreditorer, lager, status, kassebog. Der er krav til opbevaring, men blot 14 dages data kan være umulig at rekonstruere.
- Den grafiske branche arbejder 100 % med data, hvor kendetegnet er at de fylder meget, der er stor konkurrence i branchen og der er snævre deadlines. Tidsforbruget til reetablering af data er stort, og kan som oftest kun udføres af de personer der udførte de originale data. Igen er tab af data fatalt.

Den typiske forsikring der dækker reetablering af data, er en tillægsdækning til edb-kaskodækningen eller på løsøreforsikringens tyveridækning. Men bemærk, at forudsætningen for at udgifter til reetablering af data er dækningsberettiget er, at der er sket en fysisk skade på IT-anlægget eller at det er stjålet. Den rene dataforsikring kan kun tegnes i ganske få selskaber, hvor skader som følge af virus dog næsten altid er undtaget.

I eksempelvis Codan tilbydes en softwaredækning, der omfatter fejlfinding og rekonstruktion af ødelagte data som følge af kvajefejl, virus eller hacker-angreb. Det forudsætter dog, at virksomheden har fuldstændig styr på datasikkerheden, herunder opdateret antivirusprogram, opdateret firewall, nøje fastlagt backuprutine, passwordbeskyttelse og systematisk vedligeholdelse af IT-anlægget. Inden tegning bliver hele IT-anlægget gennemgået af en af Codans forsikringsingeniører, hvor specielt sikkerheden bliver gennemgået og drøftet med kunden, og kun de virksomheder der generelt har styr på datasikkerheden får mulighed for tegning af forsikringen.

Arbejdet med sikring af data i Erehvervsforsikringsudvalget i F&P

I erkendelse af at forsikring af data er kompliceret og til dels uigennemskueligt, og hvor både forsikringsselskabet og forsikringstager skal besidde fornøden teknisk indsigt for at kunne vurdere risikoen, har F&P nedsat en arbejdsgruppe der behandler problematikken omkring risikovurdering og sikkerheden ved håndtering af data. Arbejdsgruppen blev nedsat primo 2001, og består af Hanne Rasmussen (Alka) der er formand, Poul Øksenbjerg (Alm. Brand), Thor Normann (IF), Mark Andersen (TopDanmark), Thomas Møller (Tryg) og Truels Kjær (Codan), samt Charlotte Persson og Bo Baldshmidt fra F&P.

Formålet er at arbejdsgruppen skal systematisere sikring af data analogt med tyverisikring. Dette dels for at selskaberne arbejder med samme udgangspunkt og dels for at hæve det generelle sikkerhedsniveau i virksomhederne.

Resultatet pr dd. er at der er udarbejdet en foreløbig klassifikation af virksomhederne og en foreløbig niveaudeling af sikringskravene.

Sikringskravene er er niveaudelt i sikringsklasse 0, 1, 2 og 3. Hvor klasse 0 er det basale niveau, og kravene er stigende op til niveau 3.

Niveaudelingen tager bla. hensyn til

- Fysisk sikring (tyveri, brand, orden mv.)
- Sikring mod overspændinger
- Back up håndtering
- Indirekte sikring (it-politik, beredskabsplan, leverandøraftaler mv.)

Klassifikation af virksomhederne er baseret på:

- Værdien/følsomheden af virksomhedens data
- Konsekvens ved evt. tab af data
- Den fysiske størrelse af edb-systemet

hvor et pointsystem klassificerer virksomheden, og placerer denne på det sikringsniveau der vil være selskabets krav til virksomheden.

Klassifikation sammenholdt med sikringsniveau er blevet testet på forskellige kategorier af virksomheder, og med baggrund heri gøres justeringer.

Arbejdet i forsikringsbranchen og hos virksomhederne med at øge sikkerhedsniveauet er en stor men tvingende nødvendig opgave, der kræver konstant opmærksomhed omkring den tekniske udvikling. Opgaven er så stor, at samarbejde forsikringsselskaberne imellem er en nødvendighed, og ovenstående arbejdsgruppe er et flot eksempel på at dette samarbejde også sker i det virkelige liv.