TEKNOLOGI-RÅDET

IT-infrastrukturens sårbarhed

TEKNOLOGI-RÅDET

Indholdsfortegnelse

1. Indledning

IT-infrastrukturen udgør en større og større del af samfundets kritiske infrastruktur. Det gælder i Danmark såvel som i den øvrige verden. Den kritiske infrastruktur er her defineret som den bærende struktur, der er afgørende for, at en nation kan fungere effektivt på alle niveauer. Infrastrukturen omfatter vidt forskellige sektorer, som fx energi og anden forsyning, telekommunikation, sundhedssektoren, finanssektoren, transportområdet og udrykning/beredskab.

IT-infrastrukturen er en selvstændig sektor – nemlig telekommunikation. Men telekommunikation støtter en række andre sektorer. Og vi er alle afhængige af de grundlæggende IT-protokoller, der sørger for at bringe information gennem teleselskabernes kommunikationslinier. Det gælder både traditionelle telefonsamtaler og datakommunikation som fx Internettrafik. Samtidig er vi koblet sammen – interconnected – globalt i langt højere grad end nogensinde før. Dette har uvurderlige fordele, men det gør os også mere sårbare. Der er i dag mere end 600 millioner Internetbrugere, som har direkte adgang til Danmark via Internettet.

Medierne fokuserer hyppigt på hackere og virusangreb. Stort set alle har hørt om de såkaldte "orme" – senest bl.a. "Slammer" og "Blaster". Men truslen mod IT-infrastrukturen er ikke begrænset til disse tophistorier. Hvordan forholder det sig med cyberterrorister - findes de? Kan telefontrafikken lammes? Kan fx den offentlige sektor eller finanssektoren blive lammet af et angreb via Internettet?

IT indgår i ethvert moderne samfund. E-dagen den 1. september 2003, som var skæringsdatoen for, hvornår offentlige myndigheder skulle kunne kommunikere via email, er blot et af eksemplerne på udviklingen af det digitale samfund. Derfor er det spørgsmålet, om vi kan mindske eller måske blot forudsige sårbarheder i IT-infrastrukturen. Både som situationen er i dagens Danmark, men også i forhold til morgendagens IT-infrastruktur, når nye teknologier og nye anvendelser sniger sig ind på områder, vi ikke har gennemtænkt – fx trådløs teknologi, kontrol og styring via Internettet, telefoni over IP (Internet Protokol) m.v.

IT-infrastrukturen er en lille, omend voksende del af samfundets kritiske infrastruktur. Der er mange, der beskæftiger sig med sårbarheden i hele den kritiske infrastruktur – det der i USA går under navnet Homeland Security og i Danmark "Totalforsvaret". Dette notat er afgrænset til IT-infrastrukturen.

Notatet er udarbejdet af journalist Jakob Vedelsby i samarbejde med Teknologirådets arbejdsgruppe på området. Det er bl.a. baseret på en række interview, hvor enkeltpersoner fra udvalgte sektorer giver deres syn på IT-sikkerheden – og synspunkterne er mange. Formålet med notatet er at fungere som øjenåbner og igangsætter for en debat af sårbarhederne i morgendagens IT-infrastruktur.

2. Truslen fra cyberspace – baggrund og konsekvenser

2.1. Samfundets digitale nervesystem er sårbart

Det danske samfund er på linie med den øvrige verden på rekordtid blevet invaderet af computere, mobiltelefoner, netværk og tusinder af produkter med indbygget IT – og udviklingen fortsætter. I denne virkelighed er Internettet – og samfundets informationsteknologiske infrastruktur – et "digitale nervesystem," der muliggør, at information og viden kan flyde frit.

Dataudveksling i Internettet foregår ved hjælp af Internetprotokoller – et fælles sprog og regelsæt, som sikrer, at alle tilsluttede computere kan kommunikere med hinanden. Internet Service Providere (ISP'ere eller "Internetudbydere") sørger via deres netværk for, at kommunikationen kan finde sted ind og ud af private og offentlige virksomheder, institutioner og private hjem. ISP'ernes netværk er endvidere forbundet med hinanden og med udenlandske netværk i såkaldte knudepunkter, der typisk er beliggende hos de store ISP'er. Flertallet af de danske ISP'er er forbundet i det danske Internet Exchange kundepunkt kaldet DIX (Danish Internet eXchange). Formålet med DIX'en, der drives af UNI-C, er at lette udvekslingen af datatrafik mellem danske Internetudbydere, således at indlandstrafik ikke skal sendes via dyre udlandsforbindelser, men kan sendes via DIX'en. Denne koncentration gør til gengæld DIX'en til et sårbart knudepunkt.

Internettet er opbygget af datanetværk, som er forbundet med hinanden på tværs af landsdele, lande og verdensdele. Selvom Internettet betragtes som anarkistisk, finder der alligevel en overordnet styring sted. I Danmark foregår al administration vedrørende det danske topdomæne (.dk) således hos virksomheden DK Hostmaster A/S. Teknisk set vedligeholdes domæneinformationerne i DNS (Domain Name System), der kan sammenlignes med en telefonbog.

DNS har vist sig at indeholde flere sårbarheder og Internettets domæneservere har tidligere været udsat for alvorlige angreb. Dertil kommer, at ISP'erne, som er en vigtig faktor i al Internetkommunikation, ikke er underlagt nogen retningslinier for fx IT-sikkerhed – og "angreb" på domæneservere kan få alvorlige konsekvenser for muligheden for at kommunikere via Internettet.

Et andet eksempel på Internettes sårbarhed kan iagttages i forhold til de enheder, der forbinder datanetværk med hinanden. Al datakommunikation, som passerer fra et netværk til et andet, er reguleret af en eller af flere routere. Disse foranlediger, at de enkelte enheder i datatrafikken (datapakkerne) bliver sendt videre til de rigtige modtagere. Et koordineret angreb rettet mod routernes evne til at route korrekt, vil have en betydelig effekt på Internettes funktionalitet som helhed.

Internettets udbredelse og integration med IT-systemer overalt i samfundet har i det hele taget åbnet for nye former for sårbarhed på en lang række vitale samfundsområder. Jo flere samfundsaktiviteter, der bliver afhængige af en velfungerende, Internetbaseret IT-infrastruktur, des alvorligere bliver konsekvenserne, hvis systemerne bryder sammen – fx som følge af målrettede "angreb" via Internettet – eller fysiske angreb. En norsk rapport fra 2002 afdækker, at fysisk sabotage mod 3-7 centrale Internetknudepunkter kan stoppe al trafik i Norge på Internettet.

Der er mange faktorer, som kan påvirke IT-infrastrukturens sårbarhed. Udover at virksomheder og vitale samfundsområder kan rammes via fysisk sabotage og computervira eller hackere, er driftsstabiliteten i IT-

infrastrukturen også truet af tekniske svigt som følge af fejl i soft- eller hardware, eller fx ved at kommunikationskabler ødelægges i forbindelse med entreprenørarbejde.

Private virksomheder og offentlige systemer er dybt afhængige af, at IT og elektroniske netværk fungerer. Sikkerheden i den elektroniske kommunikation er derfor alfa og omega for aktiviteterne på stadig flere samfundsområder. De enkelte institutioner og virksomheder beskytter sig så godt de kan mod angreb via Internettet ved hjælp af bl.a. firewalls og antivirusprogrammer. Alligevel viser nye tal fra Danmarks Statistik, at 43 procent af danske virksomheder, 61 procent af de statslige institutioner, 83 procent af de amtslige institutioner og 57 procent af kommunerne har været udsat for virusangreb i 2002. Ca. 20 procent af de statslige og amtslige institutioner har oplevet uautoriseret adgang i form af hacking eller "Denial of Service" (angreb, der overbelaster de anvendte servere), mens 8 procent af kommunerne og 3 procent af de private virksomheder har haft problemer med dette.
De nævnte tal omfatter både "generende" og "alvorlige" sikkerhedsproblemer. Medregnes udelukkende de alvorlige sikkerhedsproblemer, viser det sig, at disse kun involverer 1-3 procent af de offentlige myndigheder. Tilsvarende har ca. 10 procent af de danske virksomheder oplevet sikkerhedsproblemer, der kan karakteriseres som alvorlige.
For både det offentlige og det private område er virusangreb det mest betydningsfulde sikkerhedsproblem, der efterfølges af sikkerhedsproblemer som følge af fejl i henholdsvis hardware og software.

På nuværende tidspunkt eksisterer der intet samlet overblik over det danske samfunds IT-relaterede sårbarhed. Et IT-nedbrud i elforsyningen, den finansielle sektor eller hospitalsvæsenet kan have alvorlige og endog livstruende konsekvenser, som det er i hele samfundets interesse at imødegå. På den baggrund er flertallet af de IT-sikkerhedseksperter fra både erhvervslivet og den offentlige sektor, Teknologirådet har talt med, også overordnet set enige om, at tiden er inde til, at der bliver iværksat en samlet analyse af karakteren og omfanget af de risici, der knytter sig til IT-infrastrukturen i Danmark – og at analysen efterfølges af konkrete beredskabsaktiviteter.

2.2. Truslen fra organiseret cyberterrorisme eller -sabotage

Der er kun meget begrænset viden om, hvorvidt der har fundet organiseret cyberterrorisme eller -sabotage sted. Der er dog enkelte bekræftede episoder. Fx angreb russiske hackergrupper NATO's åbne systemer under krigen i Kosovo. Der er også eksempler på, at tilsvarende angreb finder sted i disse år i Mellemøsten i opgøret mellem Israel og Palæstinenserne.

I rapporten "Samfundets sårbarhed som konsekvens af IT-anvendelsen" (Forsvarsministeriet, 2001) vurderer IT-sikkerhedseksperter, at "såfremt et systematiseret angreb på vitale danske samfundsfunktioner iværksættes understøttet af væsentlige ressourcer (...) kan kontrollen med vitale systemer blive overtaget af angriberen."

Der er i de seneste 4-5 år observeret en stadig stigning i antallet af anmeldelser af hacking til Nationalt Efterforskningsstøttecenter under Rigspolitichefen. Også på internationalt plan sker der en kraftig stigning i antallet af hændelser.

I Danish Computer Emergency Response Team (DK-CERT), en offentligt finansieret sikkerhedsorganisation under UNI-C, som bl.a. rådgiver om og arbejder med forebyggelse af IT-sikkerhedsproblemer, mener man ikke, at der er belæg for at påstå, at der noget sted i verden har fundet hændelser sted i forbindelse med IT-installationer, som kan rubriceres under terrorbegrebet. I DK-CERT er man dog ikke i tvivl om, at grupperinger af forskellig art i stigende grad vil misbruge Internettet til fx at propagandere for deres budskaber ved at hacke sig ind – og forvanske indholdet – på offentlige hjemmesider.

I forbindelse med krigen i Irak blev hjemmesider under bl.a. Det Hvide Hus og Downing Street nr. 10 ændret af hackere, som på den måde demonstrerede deres krigsmodstand.

Fænomenet har fået betegnelsen "hacktivism". Der er bl.a. også identificeret en islamisk hackergruppe, USG, med rødder i Egypten, som har hacket sig ind og korrumperet utallige websider med antiamerikanske budskaber.

"Udover et atomangreb, er der intet som kan lamme USA hurtigere – bringe os til stilstand og destruere vores netværksøkonomi – end et veltilrettelagt cyberterroristisk angreb. Truslen er ikke længere blot teoretisk. Det er et spørgsmål om national sikkerhed," udtalte en topchef fra den globalt tilstedeværende IT-virksomhed, CSC, der bl.a. lever af at levere IT-sikkerhed, tilbage i 2001.

I DK-CERT er man heller ikke i tvivl om, at egentlig cyberterrorisme, som går målrettet efter at ødelægge vitale samfundsfunktioner, er i vente. En af de kendte metoder, som man vil se udnyttet endnu mere ondsindet end i dag, er "Distributed Denial of Service" (DDoS), som kan lamme kommunikationen i Internettet. Indtil dato er der observeret midlertidige lammelser, men langvarige og mere omfattende konsekvenser som følge af DDoS kan forventes i fremtiden, forudser man i DK-CERT.

2.3. Vira/orme – og deres konsekvenser

I cyberspace foregår en kontinuerlig konkurrence, hvor hackere og virusspredere forsøger at overgå hinanden i ødelæggelser via Internettet. Hver dag bliver der programmeret nye computervira, som bliver sendt i omløb globalt, og hver dag forsøger hackere at trænge ind i computere overalt i verden. Disse personer benytter ofte relativt enkle midler til at gennemføre deres forehavender. De nødvendige IT-værktøjer kan typisk downloades direkte via Internettet – og der bliver hele tiden udviklet nye værktøjer.

Siden 1997 er der observeret et stort antal forskellige vira af den traditionelle slags, som typisk overføres via disketter. Andre vira overføres ved besøg på hjemmesider. I de seneste år er der fremkommet nye, langt mere avancerede og skadevoldende vira/orme.

Et eksempel er ormen Slammer, der i januar 2003 udnyttede en fejl i Microsofts databasesoftware, SQL Server 2000. Softwaren anvendes af virksomheder, statslige organer og universiteter over hele verden. I modsætning til flertallet af tidligere vira/orme, lykkedes det Slammer at påvirke infrastrukturen uden for Internettet, hvilket bl.a. betød forstyrrelser i flytrafik og lukkede kontantautomater flere steder i verden. Målt i tabt produktivitet vurderes Slammer at have forvoldt skader for mellem seks og otte milliarder kroner.
I august 2003 forvoldte ormene Blaster og Sobig.F store problemer for IT-brugere over hele verden. Sobig.F ankom indpakket og krypteret og kunne derfor krybe udenom de fleste virusprogrammer. Sobig.F ramte bl.a. store dele af den hjemlige statsadministration, herunder Folketinget, hvis emailkommunikation blev blokeret.

Et DDoS-angreb kan i realiteten foretages af én person, idet de mange maskiner kan fjernstyres eller tidsindstilles til at foretage angrebene. Det er særlig vanskeligt for en virksomhed at beskytte sig mod denne type angreb, idet mængden og typen af trafik fra hver af de involverede afsendere ikke nødvendigvis vækker særlig opmærksomhed. Problemet er, at et angreb ofte iværksættes samtidig fra et stort antal afsendere forskellige steder på Internettet, hvilket gør et angreb stort set umuligt at opdage og stoppe i tide.

En virus/orm kan også have den effekt, at den tager magten over computeren og fx sletter hele eller dele af harddisken. Samtidig vil virus typisk åbne en bagdør til computeren, hvilket betyder, at den pågældende computer er åben for, at hackere uhindret kan trænge ind og gøre hvad de vil og fx bruge computeren som platform for yderligere kriminelle aktiviteter – fx distribution af programpakker, som andre hackere henter. Ifølge danske IT-eksperter bliver disse vira stadig mere ondsindede og ødelæggende – og vurderingen er, at problemet vil vokse markant i de kommende år.

Danske virksomheder og institutioner bliver kontinuerligt angrebet via Internettet – det er bl.a. gået ud over ministerier, TV2, Københavns Lufthavn, Kommunernes Landsforening,

kommunale hjemmesider, TDC og Novo Nordisk. Angrebene har været generende, men vurderingen er, at skaderne kunne havde været væsentlig større, hvis der havde været tale om organiserede angreb.

2.4. Alvorlige sikkerhedsproblemer på mange websites

I takt med at stadige flere private og offentlige virksomheder beskytter sig med firewalls, finder hackerne nye veje. Senest er der i forbindelse med krigen i Irak som nævnt set eksempler på hacktivism, hvor hackere er trængt ind på hjemmesider og har forvansker indholdet. Ifølge IT-sikkerhedseksperter fra bl.a. DK-CERT er dette først og fremmest muligt, fordi virksomhederne anvender webserverprogrammer med kendte sikkerhedshuller. Der findes rettelser til disse huller, men rettelserne installeres ofte for sent eller slet ikke.

Denne "åbenhed" udgør et alvorligt sikkerhedsproblem i forhold til hjemmesider, som fx formidler anvisninger til borgerne i forskellige sammenhænge – og de mulige konsekvenser vil vokse i takt med, at især offentlige hjemmesider i stigende grad benyttes til formidling og udveksling af vigtige informationer med borgere og virksomheder. Derudover indebærer dette potentielt alvorlige økonomiske konsekvenser for virksomheder, som i kortere eller længe tid får ødelagt deres webbårne budskaber eller muligheder for at praktisere e-handel.

Et andet alvorligt sikkerhedsproblem er webspoofing. Ved denne angrebstype ændres websidens adresser, så alle oplysninger routes via tredjepart, som på den måde kan opsnappe kommunikationen. Når brugeren derefter i god tro indtaster password og andre personlige oplysninger, vil disse data tilgå den kriminelle. Dette svarer stort set til den svindel med falske dankortterminaler, som var udbredt for et par år siden.
Angreb via DNS (Domain Name System) kan give samme resultat som webspoofing. Løsningen er servercertifikater, sikker kommunikation og brugeropmærksomhed.

2.5. Ensartet teknologi – en forudsætning og et problem

Den globale kommunikation i Internettet opnås ved brug af fælles kommunikationsstandarder. Samtidig er der en tendens til at standardisere ved brug af ganske få softwareproducenter. Begge dele indebærer den risiko, at vira kan ramme bredt og sprede sig med lynets hast, ligesom hackere har nemmere adgang, end hvis der blev anvendt mere forskelligartet software.

Der er talrige eksempler på, at deciderede fejl i software har åbnet for, at hackere kunne trænge ind i IT-systemer og forrette ødelæggelse. "Internet Security Threat Report" fra marts 2003 fra antivirus/firewall-producenten Symantec fastslår, at antallet af erkendte huller i software er steget eksplosivt det seneste år. Rapporten dokumenterer, at der i 2002 er fundet mere end 2.500 nye sårbarheder i software, hvilket er et stigning på 81 procent i forhold til 2001. Antallet af kendte moderate og kritiske sikkerhedshuller – det vil sige mulige åbninger, hvorigennem hackere og vira kan trænge ind – steg med 85 procent på ét år.
De seneste tal fra det amerikanske CERT Coordination Center, der siden 1995 har indsamlet og registreret sårbarheder i IT-systemer, viser imidlertid en stagnerende tendens. Centrets tal viser, at der siden 1998 har været en voldsom stigning i antallet af sårbarheder, der opdages på et år. I 1998 fandt CERT CC således 262 nye sårbarheder, mens tallet var 2.437 i 2001 og 4.129 i 2002. I første halvår af 2003 blev der imidlertid "kun" fundet 1.993 nye sårbarheder.

Efter IT-boblens kollaps har IT-branchen i de senere år oplevet generel nedgang verden over. Men nu er i hvert fald ét forretningsområde i kraftig vækst – og det er sikkerhed. Analysefirmaet IDC forventer, at verdensmarkedet for IT-sikkerhed vil vokse fra 355 millioner dollar i 2002 til 754 millioner dollar i 2007.

2.6. Den menneskelige faktor er afgørende for sårbarheden

Tal fra Danmarks Statistik for året 2002 viser som nævnt, at 83 procent af amterne, 57 procent af kommunerne og 61 procent af de statslige

institutioner inden for det seneste år har oplevet virusangreb. Det er sket på trods af, at de alle næsten uden undtagelse har investeret i antivirusprogrammer. I Rådet for IT-sikkerhed mener man på den baggrund, at den menneskelige faktor er afgørende. Manglende sikkerhedsuddannelse af de IT-ansvarlige vurderes bl.a. at være en medvirkende årsag til virusproblemerne i det danske samfund.

En dansk IT-sikkerhedsekspert fra MindSoft fremhæver, at IT-systemer, som er vurderet til at være meget sikre, i virkeligheden kan vise sig at være mindre sikre, fordi der er foretaget en ufuldstændig risikovurdering. En faktor der ofte overses er netop den menneskelige faktor. Sikre systemer er uundgåeligt mere besværlige at anvende end mindre sikre systemer. Dette kan få personer til at undgå at anvende systemer, der er meget sikre, eller få personer til at søge at omgå sikkerheden. I en risikovurdering er det derfor nødvendigt at inddrage denne menneskelige faktor, vurderer eksperten.

Ifølge ITEK, Dansk Industris branchefællesskab for IT-virksomheder, kan en tredjedel af virksomhedernes IT-problemer henføres til fejl i opsætning eller manglende opdatering af software eller hardware. De resterende 70 procent af sikkerhedsfejlene skyldes medarbejdere, der downloader programmer fra Internettet, åbner virusinficerede filer, glemmer at opdatere virusbeskyttelsesprogrammer, eller bevæger sig ind på tvivlsomme Internetsider, der kan være skjulested for hackere. Mange virksomheder har installeret omfattende sikkerhedssystemer, men glemmer at uddanne og motivere medarbejderne på sikkerhedsområdet. Hvis medarbejderne ikke ved, hvorfor og hvordan de overholder virksomhedens IT-sikkerhedsregler, bliver de en markant sårbarhedsfaktor, mener man i ITEK.

I en undersøgelse fra 2003 har revisionsselskabet Deloitte & Touche interviewet 242 danske virksomheder om IT-sikkerhed. Undersøgelsen viser, at virksomhederne generelt fokuserer på sikkerhedsteknologi frem for på uddannelse af medarbejderne. Mange virksomheder tror, at IT-sikkerhed kan købes for penge. Sagen er imidlertid, som det bliver understreget i rapporten, at det er medarbejdernes holdninger og uddannelse, der har en reel IT-sikkerhedsmæssig effekt. Deloitte & Touche opfordrer til, at uddannelse og reel oplysning om IT-sikkerhed indgår i enhver virksomheds forretningsmodel. Målet er at forbedre sikkerhedsbevidstheden hos medarbejdere og ledelse og skabe en sikkerhedskultur med et højt IT-sikkerhedsniveau.

Som supplement til ovenstående kan det nævnes, at en undersøgelse fra Danmarks Statistik viser, at omtrent halvdelen af den offentlige sektor løbende uddanner deres medarbejdere i IT-sikkerhed. For private, danske virksomheder set under ét, er det kun hver tiende virksomhed, der løbende uddanner deres medarbejdere i IT-sikkerhed. Tallet er dog væsentlig højere for virksomheder med mange ansatte.

Tekniske løsninger med automatisk og tvungen integritetskontrol af arbejdspladserne før der bliver givet adgang til virksomhedens netværk – kombineret med udrulning af virusmønstre, konfigurationsfiler m.v. – kan medvirke til at reducere dette problem. Brug af tynde klienter på arbejdspladserne kan ligeledes være en supplerende løsning, som dog ikke vil fjerne behovet for uddannelse og sikkerhedsbevidsthed.

2.7. Certificeret og revideret IT-sikkerhed

Finanstilsynet udsendte i februar 2003 en vejledning om finansvirksomheder og deres IT-kontrol- og sikringsforanstaltninger. Her stilles der krav om, at bestyrelsen i en finansvirksomhed skal opstille en IT-strategi med IT-sikkerhedspolitik og risikovurdering. Samtidig er der nye internationale vejledninger på vej til brug for de statsautoriserede IT-revisorer. I disse nye vejledninger er IT-sikkerhed integreret som en naturlig del af den almindelige revision.

WebTrust, der udbydes af en række statsautoriserede revisorer i Danmark, er en af de øjeblikkelige muligheder for, at man som fx ISP'er, traditionel virksomhed eller webbutik

kan blive certificeret efter et sæt uafhængigt formulerede, objektive kvalitetsregler. WebTrust konceptet er udviklet af amerikanske og canadiske revisorer med henblik på at hjælpe virksomheder og deres kunder med at vurdere de risici, der er forbundet med elektronisk handel.

Derudover findes en række andre standarder inden for IT-sikkerhed – bl.a. ISO/IEC 17799 (BS 7799-1) og DS484. Hertil kommer Best Practise Guidelines fra Information Security Forum, der er en sammenslutning af store, sikkerhedsbevidste virksomheder i Europa og USA.

2.8. PET varetager Internetsikkerheden i Danmark

En lang række lande har, i modsætning til Danmark, etableret en overordnet samfundsinstans, der håndterer alle de sikkerhedsmæssige aspekter, som knytter sig til Internettet. Sverige har et nationalt organ i regi af "Överstyrelsen för civil beredskab", USA har "National Infrastructure Protection Center," og i England har man "National Infrastructure Security Coordination Center."

I Danmark er Politiets Efterretningstjeneste (PET) Danmarks nationale sikkerhedsmyndighed. Det betyder, at PET også har til opgave at følge og forebygge ødelæggende angreb på danske IT-systemer, der har betydning for Danmarks sikkerhed. Nationalt Forskningsstøttecenter under Rigspolitichefen har bl.a. til opgave at overvåge organiseret og kompliceret IT-kriminalitet, ligesom Forsvarets Efterretningstjeneste (FE) udfører opgaver inden for sikkerhed og varsling på FE's arbejdsområder.

På internationalt niveau er det paraplyorganisationen FIRST (Forum of Incident Response and Security Teams), der koordinerer Incident Response Teams rundt om i verden. I Danmark er bl.a. DK-CERT (Danish Computer Emergency Response Team). De tilbyder begge bl.a. at udsende virusvarsler, når der er kendskab til hurtigspredende vira samt at advare om og komme med løsningsforslag i relation til nyopdagede sikkerhedshuller i IT-systemer.

3. IT-sikkerhed på udvalgte samfundsområder

3.1. Indledende bemærkninger

Teknologirådet har interviewet repræsentanter fra følgende samfundsområder: Elforsyning, finanssektoren, telekommunikation, transportsektoren, sygehussektoren og repræsentanter fra den offentlige administration. Udover de her valgte samfundsområder, kunne det være relevant at interessere sig for bl.a. olie/gas/benzin (forsyning, lagre), øvrig transport (landevej, jernbane), vandforsyning, udrykning (politi, brandvæsen, ambulance), forsvaret, politiet og medierne.

Flere repræsentanter for vitale samfundsområder, som Teknologirådet har interviewet til dette projekt, har ytret en vis modstand mod at kommentere IT-sikkerhedsmæssige spørgsmål. Alle medvirkende har ønsket – og haft mulighed for – at godkende egne udtalelser.

3.2. Elforsyningen – ENERGI E2 og NESA

Et samfund uden strøm går i bogstaveligste forstand i sort. Derfor står elforsyningen højt på listen over vitale samfundsfunktioner, der kan tænkes at være et potentielt mål for terrorangreb, herunder cyberterrorisme. Elforsyningen i Danmark er inde i en fusionsbølge, hvor mange aktører skal samarbejde – og i den situation kunne man fristes til at bringe talemåden "kæden er ikke stærkere end det svageste led" på banen. Men der er ingen alvorligt svage led i elforsyningen, fastslår såvel ENERGI E2, der ejer en række elproducerende kraftværker, som NESA, der sidder på en stor del af det sjællandske forsyningsnet.

I ENERGI E2 understreger man, at det på grund af IT-systemernes opbygning ikke er muligt, via Internettet, at trænge ind i virksomhedens organisation og ramme bredt – det vil fx sige i ét hug at få ENERGI E2's kraftværker til ophøre med at producere strøm. Det skyldes bl.a., at meget begrænsede dele af de systemer, der betinger eldriften, kan nås via Internettet. Det ville kræve en omfattende insiderviden at ramme bare en lille del af systemerne ad den vej – og det er tæt på at være umuligt at trænge ind fra cyberspace og forrette så alvorlig skade, at elforsyningen ikke kan opretholdes. Det skyldes først og fremmest, at reguleringen af elproduktionen ingen forbindelse har med Internettet.
Erfaringerne med vira og hackere viser bl.a., at de i høj grad knytter sig til bestemte teknologier og fejl i software. I ENERGI E2 har man bevidst valgt en decentral struktur, hvor kraftværkerne kører uafhængigt af hinanden og på systemer, som er teknologisk forskellige. Falder et kraftværks IT-systemer for en hændelse er det derfor meget lidt sandsynligt, at et andet kraftværk gør det samme.
Worst case scenariet er en situation, hvor det lykkes hackere at ødelægge de IT-systemer med adgang til og fra Internettet, som muliggør ENERGI E2's muligheder for at handle strøm på de internationale elbørser. Det kan koste virksomheden millionbeløb. Dog understreger ENERGI E2, at der er taget højde for den situation og planlagt alternative metoder til at varetage handelsfunktionen, men på nedsat blus, indtil de Internetbårne systemer kan genetableres.

Hos NESA pointerer man, at den basale elforsyning i dag ikke på nogen måde kan blive berørt at computervira eller hackere. Det skyldes, at den IT-baserede overvågning, styring og regulering af elforsyningsnettet finder sted i lukkede netværk, som ikke kan nås udefra. Dette system vil dog efterhånden også blive integreret med de centrale dele af den øvrige IT-platform for at opnå effektiviseringer og udnytte data bedre end det sker i dag. Der vil ikke være tale om direkte adgang fra Internettet. Man vil opbygge et indre sikkerhedslag, hvor integrationspunkterne beskyttes med firewalls, oplyser NESA.

Der hvor der potentielt kan opstå problemer er i forbindelse med NESA's Internetbaserede kundebetjening. Her er NESA – ligesom alle andre virksomheder, der er tilsluttet Internettet – sårbar over for endnu ukendte virustyper m.v. Hos NESA understreger man dog, at man i de sidste par år ikke har været generet af vira. Det skyldes bl.a. en meget omhyggelig virusskanning af alle indgående og internt udvekslede email og dokumenter.

3.2.1. NESA: Brug IT-revisorer og implementér et nationalt Early Warning system

NESA's IT-chef fremhæver et godt samarbejde med IT-revisorer som en af årsagerne til, at det er lykkedes at holde hackere og vira fra døren. IT-revisorernes opgave er at kontrollere, hvorvidt driftssikkerheden, datasikkerheden og systemsikkerheden er i top. Og hvis det ikke er tilfældet, rådgive om, hvordan sikkerheden kan forbedres, således at virksomhedens økonomiske værdier bevares bedst muligt. NESA's IT-chef kan se en fordel i en koordineret national "Early Warning" indsats. Det ligger i sagens natur, at man altid er i defensiven i den evige kamp om at følge med udviklerne af computervira. Man er tvundet til at beskytte sig og tvunget til at støtte sig til antivirusleverandørernes opdateringer. Hos NESA foretages denne opdatering løbende i et professionelt regi af den eksterne driftsleverandør. En neutralt funderet, nationalt indsats, hvor man så tidligt i en ny virus' livsbane som overhovedet muligt får en advarsel om, at der er noget i gærde, kunne medføre en effektivisering og en forbedring, mener NESA's IT-chef.

3.2.2. ENERGI E2: Drop kassetænkningen og praktisér teknologisk diversitet

ENERGI E2's IT-chef er ikke fortaler for en koordineret national indsats i forhold til at sikre IT-infrastrukturen. Derimod mener han, at det er på tide at fokusere på det fornuftige i at decentralisere virksomhedens IT-bårne processer frem for at de – sådan som man i stigende grad ser det – finder sted på færre servere (serverkonsolidering) eller centraliseres i outsourcingcentre. Der er uden tvivl penge at spare på drift og vedligeholdelse, men ved at koncentrere sine vitale IT-systemer på få punkter, kommer man i en situation, hvor disse kan blive unødig sårbare. Når man udtænker sin IT-strategi bør man derimod sørge for, at man ikke samler alle sine systemer i ét centralt punkt. Og hvis man laver flere parallelle systemer, må man sikre, at de er teknologisk forskellige. IT-centre med identiske funktioner, software og hardware indebærer den risiko, at en negativ egenskab i fx en applikation finder sted på samme tid i alle centre – og så har man et alvorligt problem, understreger ENERGI E2's IT-chef, der mener, at man – frem for at stable en større national indsats på benene – skulle koncentrere sig om at udbrede et tankesæt, som foreskriver, at man laver sine IT-systemer så robuste, at de samlet set bliver fejlresistente over for enkelthændelser. Frem for løbende anbefalinger, som ikke er langtidsholdbare i en IT-verden i evig bevægelse, mener han, at man skal satse på at formulere og udbrede IT-sikkerhedspolitiske *holdninger*.

3.3. Finanssektoren – Danske Bank

Bankernes image og troværdighed knytter sig i høj grad til sikkerhedsspørgsmålet, og i finanssektoren har man da også lang tradition for at have kraftig fokus på IT-sikkerhed. Udfordringerne på dette område er vokset i takt med, at kunderne bliver tilbudt stadig flere muligheder og services via Internettet. På homebankingområdet har banksektoren et fælles sikkerhedskodex, som bidrager til at holde et til stadighed opdateret og højt sikkerhedsniveau.

Danske Bank – Danmarks største pengeinstitut – tager en lang række sikkerhedsmæssige forholdsregler. Alle bankens IT-løsninger, som skal anvendes i forbindelse med Internettet, gennemgår en særlig, detaljeret sikkerhedsvurdering. Bankens samlede Internetinfrastruktur er certificeret – og testes og gennemgås kontinuerligt – af et professionelt, eksternt IT-sikkerhedsfirma.

I Danske Bank er man bevidste om, at intet system er 100 procent skudsikkert. Derfor er opbygningen af Internetinfrastrukturen gjort særlig robust, så skadevirkningen af eventuelle

angreb kan begrænses og afgrænses fra de vitale systemer.
For bankens IT-sikkerhedschef vil det værst tænkelige scenarium være en situation, hvor nyudviklede vira eller ukendte fejl i softwaresystemer pludselig åbner for, at hackere eller vira kan komme ind og gøre skade. Derfor har man stor fokus på ændringer i Internet-trusselsniveauet og et teknisk beredskab på vagt døgnet rundt, som kan træde til, hvis virksomhedens "Intrusion Detection System" giver alarm om uvelkomne gæster eller indtrængen af virus. Vi har erkendt, at vi er koblet op til en verden, hvis adfærd vi ikke kan kontrollere, hedder det fra Danske Banks IT-sikkerhedschef.

3.3.1. Danske Bank: Behov for centraliseret Internetsikkerhed og national koordination

IT-sikkerhedschefen i Danske Bank mener i allerhøjeste grad, at der er behov for en koordineret indsats for at styrke den Internetrelaterede IT-sikkerhed på landsplan. I betragtning af, hvor mange samfundsaktører, der er afhængige af en sikker og stabil IT-infrastruktur, undrer det ham, at der ikke tidligere har været større fokus på dette område. I 2002 tog banken initiativ til at starte, hvad de kalder en Internet referencegruppe, som har deltagelse af ISP'er, finanssektoren, medicinalindustrien, teleudbyderne m.fl. Opbakningen om dette initiativ har været meget positiv og har vist, at der er et stort behov for at udveksle erfaringer og ideer på et bredere plan, fastslår Danske Banks IT-sikkerhedschef.

Hvis man ønsker et sikkert Internet er det ikke hensigtsmæssigt, at alle Internetbrugere skal indbygge de samme sikkerhedsmekanismer, når dette ligeså godt kunne foregå centralt – fx i regi af de knudepunkter, som ISP'erne repræsenterer. Med en sådan løsning ville man kunne beskytte hele den danske del af Internettet på en billigere og mere effektiv måde, mener Danske Banks IT-sikkerhedschef, der påpeger, at langt de fleste samfundsområder er underlagt kvalitetskrav, næringsbreve og kontrol, blot ikke Internetområdet. Her er der ingen retningslinier, forordninger eller krav til aktørerne, fx heller ikke til ISP'erne. Han efterlyser kvalitetskrav, struktur, standardisering, fordi det vil skabe større gennemskuelighed – ikke mindst i forhold til det sikkerhedsniveau, som den enkelte ISP'er tilbyder.

3.4. Sygehussektoren – Hovedstadens Sygehusfællesskab

Sygehusvæsenet er stigende grad afhængig af IT. Størstedelen af det anvendte apparatur er IT-styret og det samme er tilfældet med sygehusenes administration. Med Elektronisk Patient Journal (EPJ) på vej overalt i sektoren vokser kravene til IT-sikkerhed yderligere i de kommende år, hvor det bl.a. skal sikres, at ingen uvedkommende kan få adgang til – og dermed mulighed for at læse og eventuelt korrumpere informationer i – borgernes elektroniske journaler. Det kan havde livstruende konsekvenser, hvis fx informationer om medicinering, laboratorieresultater og lignende forvanskes.

I Hovedstadens Sygehusfællesskab (HS) – hvori der indgår seks hospitaler i Københavns og Frederiksberg kommuner, herunder Rigshospitalet – har man opstillet en lang række "State of the art" forsvarsværker. Disse omfatter bl.a. firewalls omkring de systemer, hvortil der er indgang fra Internettet. Derudover overvåges alle systemer i døgndrift.
I HS understreger man vigtigheden af, at man i enhver del af organisationen har gjort sig klart, hvem der har ret og pligt til at reagere, hvis alarmklokkerne lyder i en katastrofesituation – det vil sige, hvis overvågningssystemerne opdager, at der optræder virus eller uautoriseret indtrængen. Samtidig understreger man, at det er afgørende at sikre, at man har en til stadighed opdateret backup, som kan genetablere data, der måtte blive slettet eller korrumperet ved et angreb på IT-systemerne eller tekniske fejl på udstyret.

I erkendelse af, at intet forsvarsværk giver 100 procent sikkerhed, er arkitekturen i HS' IT-beskyttelse opdelt i individuelle netværk alt efter sårbarhed. Det betyder, at hvis det værst tænkelige skulle ske – det vil fx sige, at et hospitals IT-systemer (eller IT-systemerne i en "enhed" på hospitalet) inficeres med

computervirus – så vil skaden være isoleret til netop det hospital eller den enhed. En virus vil således ikke kunne sprede sig til andre hospitaler. Hver eneste enhed og hospital skal nemlig til enhver tid kunne fungere IT-mæssigt uafhængigt af hinanden, oplyser HS.

HS gennemgik i 2001 en omfattende kvalitetsvurdering i form af en art akkrediteringssproces, herunder også på det sikkerhedsmæssige felt. Ifølge HS' IT-sikkerhedskoordinator er der imidlertid ingen tvivl om, at HS og det øvrige sygehusvæsen i de kommende år bliver nødt til at indbygge yderligere sikkerhedslag i IT-systemerne, som kan sikre, at kun de rette personer kan komme i forbindelse med de rette data.
IT-styret hospitalsudstyr er alt overvejende selvkørende og uafhængigt af IT-systemer, som har forbindelse med Internettet. Med et fuldt implementeret EPJ-system i Danmark, må det dog forventes, at der sker en elektronisk sammenbinding af de fleste IT-systemer. Det åbner for nye sårbarheder, som man må arbejde på at fjerne, hedder det fra HS, hvor man endnu ikke har været udsat for egentlige angreb. Dog registrerer HS' firewalls til stadighed de såkaldte portscanninger, som man imidlertid vurderer som relativt harmløse og standardiserede søgninger efter åbninger i IT-systemerne.

3.4.1. HS: Der er behov for en koordineret indsats, som kan sikre IT-infrastrukturen

HS' IT-sikkerhedskoordinator understreger, at planerne om en digitaliseret offentlig sektor stiller store krav til IT-infrastrukturen i Danmark. På sundhedsområdet er både EPJ og en offentlig sundhedsportal på vej. Med alle disse initiativer bliver der i stigende grad åbnet for, at borgerne kan hente informationer og selvbetjene sig via Internettet. Jo større samfundsmæssig betydning Internettet får, des større bliver behovet for at gøre noget koordineret for at skabe en sikker IT-infrastruktur, pointerer HS' IT-sikkerhedskoordinator.
I HS er man ikke mindst meget opmærksom på de generelle problemer, der i stigende omfang konstateres med sårbare webapplikationer, som kan muliggøre indtrængen af hackere.

3.5. Telekommunikation – TDC

For få år siden var TDC's IT-infrastruktur synonym med IT-infrastrukturen herhjemme. Det er ikke tilfældet længere. Monopolet er brudt og en række teleselskaber har oprettet egne IT-infrastrukturer. Denne udvikling har i sig selv reduceret sårbarheden, idet infrastrukturen ikke længere kun indeholder ét, men flere "points of failure". Den nye struktur er til gengæld sårbar i de knudepunkter, hvor de forskellige netværk er sammenknyttet, pointerer TDC's IT-sikkerhedschef, der finder, at der er et akut behov for at kortlægge samtlige knudepunkter og afdække de sårbarheder, som disse repræsenterer.

TDC har opbygget et distribueret netværk, hvor nedbrud enkelte steder ikke påvirker resten af netværket. Et nedbrud medfører blot at trafikken bliver omdirigeret. Uagtet, at der findes nødstrømsgeneratorer i TDC's systemer, anser TDC en afbrydelse af strømforsyningen for at være blandt de værst tænkelige scenarier. Uvedkommende indtrængen i TDC's netstyring med efterfølgende kontrol over kommunikationen i IT-infrastrukturen er også et worst case scenarium. Af samme årsag har TDC høj fokus på IT-sikkerheden og har bl.a. haft et uafhængigt revisorfirma til at gennemgå koncernens sikkerhedsrutiner.

3.5.1. TDC: IT-sikkerhed er først og fremmest et ledelsesansvar i virksomheden

TDC's IT-sikkerhedschef understreger, at det er TDCs holdning, at det generelt er vigtigt at sikre, at IT-sikkerhed er en integreret del af enhver virksomhed – og at alle virksomheder bør have mulighed for at indføre en IT-sikkerhedspolitik, som harmonerer med virksomhedens egne behov og præmisser.

TDC støtter gerne forskellige nationale og internationale initiativer, som kan begrænse sårbarheden i IT-infrastrukturen og skabe sikrere Internetkommunikation. Men i TDC mener man ikke, at et nationalt initiativ skal føre frem til, at virksomhederne pålægges den ene IT-sikkerhedsmæssige byrde efter den anden: Der er forskel på virksomhedernes behov, og eventuelle nationale initiativer skal

implementeres med respekt for virksomhedens egen ansvarsudfoldelse på IT-sikkerhedsområdet. Virksomheder som TDC med en særlig forpligtelse til at sikre infrastrukturen vil selvsagt også have et særligt ansvar for IT-sikkerheden inden for sit virkefelt. Men IT-sikkerhed er først og sidst et ledelsesansvar i den enkelte virksomhed – sådan bør det være i dag og fremover, pointerer TDC's IT-sikkerhedschef.

3.6. Transportsektoren – SAS

SAS' IT-sikkerhedschef fremhæver, at luftfarten generelt omfatter tre forskellige aktører, som sikkerhedsmæssigt skal spille sammen: Lufttrafik kontrolsystemerne, der er statsligt drevne, lufthavnenes IT-miljøer og de kommercielle flyselskabers IT-systemer.
Det er hans overordnede vurdering, at luftfartens IT-systemer generelt er robuste. Han vil ikke kommentere SAS' sårbarhed over cyberterrorisme, men peger i stedet på et worst case scenarium: En situation, hvor det lykkes udefra kommende at lamme både SAS' Internet Infrastruktur og tele-infrastrukturen i Skandinavien.

IT-sikkerhedschefen understreger, at SAS konstant har fokus på det IT-relaterede trusselsbillede. Selskabet bruger megen tid på informationshentning og sårbarhedsanalyser for at kunne gennemføre de nødvendige IT-mæssige opdateringer af soft- og hardware. Desuden bliver der brugt mange kræfter på at holde selskabets antivirus forsvar up-to-date. Dog erkender IT-sikkerhedschefen, at SAS – ligesom enhver anden IT-bruger – ikke kan sige sig helt fri for sårbarhed. Uanset ressourceforbruget er det ikke muligt at lave en 100 procent effektiv forebyggelse. Det skyldes ikke mindst tempoet i den teknologiske udvikling, herunder den frekvens hvormed nye softwareprodukter og systemer lanceres. Hastigheden betyder, at der løbende kommer nye sårbarheder frem, som typisk først opdages efter et stykke tid. Her gælder det så om at få lukket eventuelle huller hurtigst muligt, lyder det fra SAS.

3.6.1. SAS: Beskyttelse af IT-infrastrukturen bør være en "totalforsvarsopgave"

SAS' IT-sikkerhedschef peger på, at stort set alle brancher i dag er dybt afhængige af en velfungerende IT-infrastruktur. Den offentlige sektor er også godt på vej mod en tilsvarende afhængighed og det samme er borgerne. På den baggrund mener han, at der er et udtalt behov for en koordineret, landsdækkende beskyttelsesindsats på dette område. Beskyttelse af IT-infrastrukturen bør være en "totalforsvarsopgave" helt på linie med beskyttelse af fx el- og varmeforsyningen, mener han.

3.7. Den offentlige sektor

Den offentlige sektors forskellige serviceydelser er i stigende grad afhængig af IT. Og med visionen om "digital forvaltning" i den offentlige sektor, som nu udbredes med stor hast, vokser også kommunernes, amternes og statslige institutioners sårbarhed over for angreb via Internettet markant.

Med henblik på at fremme indførelsen af digital forvaltning i den offentlige sektor oprettede bl.a. Ministeriet for Videnskab, Teknologi og Udvikling, Finansministeriet og Amtsrådsforeningen i 2001 "Den digitale Taskforce," som er underlagt det fælles statslige/kommunale "Projekt Digital Forvaltning". Den Digitale Taskforce beskæftiger ca. 20 mennesker, der kommer fra forskellige ministerier, Kommunernes Landsforening og Amtsrådsforeningen. Taskforcen har bl.a. til opgave at identificere og afklare tekniske og herunder sikkerhedsmæssige problemstillinger vedrørende digital forvaltning.

Regeringen har på Finansloven for 2003 afsat 50 mio. kr. til udbredelse af den digitale signa-tur til borgere, myndigheder og private virksomheder. Målet med digital forvaltning er at forbedre den offentlige service ved at tilbyde borgerne øget selvbetjening og udveksling af informationer via Internettet.
I erkendelse af, at også private borgeres IT-sikkerhed er en trussel for stabiliteten i samfundet – og en direkte hindring i forhold til indførelse af digital forvaltning – anser det nye,

uafhængige Rådet for IT-sikkerhed det som et af sine hovedfokusområder at sikre, at private opnår størst mulig sikkerhed ved brug af Internettet. Vejen frem er oplysning til borgerne om sikkerhed, mener man i Rådet for IT-sikkerhed – oplysning, som kan medvirke til at højne borgernes fokus på sikkerhedsspørgsmål.

Sikkerhedseksperter i DK-CERT vurderer, at den digitale signatur på længere sigt vil kunne anvendes til at højne IT-sikkerheden i forhold til bl.a. hackere, idet den vil give mulighed for at oprette lukkede virtuelle miljøer, hvortil adgangen er stramt kontrolleret. Men det ligger en del år ude i fremtiden.

3.7.1. Amtsrådsforeningen efterlyser fælles sikkerhedsstandarder

Amterne er stærkt involveret i udviklingen af Danmark som netværkssamfund – digital forvaltning (De Digitale Amter), digital signatur og elektronisk sags- og dokumenthåndtering er nogle af de områder, hvor amterne er aktive. Konkret har amterne bl.a. fokus på udvikling af portalløsninger såsom Sundhedsportalen.

Amterne har i de senere år øget opmærksomheden på IT-sikkerhed markant. Ifølge Amtsrådsforeningens IT-ansvarlige, er de amtslige IT-systemer opbygget med forskellige grader af sikkerhed alt efter datas følsomhed. Sikkerhedsmaskerne er tættere i systemer, som skal håndtere fx personfølsomme eller finansielle oplysninger – end i systemer, som behandler data, hvor der ikke er en tilsvarende, potentiel risiko for misbrug.

Ifølge Amtsrådsforeningen er sikkerhedsniveauet på den ene side et spørgsmål om, hvor mange ressourcer, man vil bruge på rent teknisk at sikre sine data. På den anden side er sikkerheden i høj grad afhængig af de sikkerhedsprocedurer, man i en given virksomhed har for omgangen med data. Teknikken kan ikke forhindre uhensigtsmæssige arbejdsgange – og derfor bør der i høj grad også fokuseres på brugernes omgang med systemer og data, fastslår Amtsrådsforeningen.

Diskussionerne i amterne om IT-sikkerhed er præget af de forskellige politikområder, hvor IT-sikkerhed indgår som en afgørende faktor. Der er bestemte udfordringer på sundhedsområdet, andre udfordringer på teknik/miljø-området osv. I øjeblikket fokuserer amterne primært på de sikkerhedsmæssige udfordringer i relation til den kommende Sundhedsportal. Det omhandler bl.a. sikkerhedsudfordringer i de systemer, som Sundhedsportalen vil give adgang til – fx den såkaldte "personlige elektroniske medicinprofil", som er under udvikling, og Elektronisk Patientjournal.

I Amtsrådsforeningen finder man det vigtigt at fastsætte et realistisk IT-sikkerhedsniveau, som er inden for organisationernes og virksomhedernes rækkevidde. Man finder også, at det skal være brugerne af systemerne, ikke leverandørerne, der skal formulere såvel sikkerhedsniveauet som de fællesstandarder, fremtidens IT-infrastruktur bør bygge på. Samtidig fastslår Amtsrådsforeningen, at tiden er inde til at udvikle nogle konkrete sikkerhedsstandarder, som eventuelt kan gradueres alt efter sikkerhedsbehovet i det enkelte system – standarder, som alle leverandører skal basere deres systemer på, så man har sikkerhed for, at disse systemer også rent sikkerhedsmæssigt spiller i sammen toneart.

Det værst tænkelige scenarium for den IT-ansvarlige i Amtsrådsforeningen er uden tvivl en situation, hvor IT-systemerne er kommet til at hænge sammen på en sådan måde, at en cyberterrorist, hvis denne først er indenfor IT-murerne, har adgang til en hel række forskellige systemer, der sikkerhedsmæssigt dermed vælter som dominobrikker. En udvikling i den retning skal man ifølge Amtsrådsforeningen bl.a. imødegå ved at lave fællesregler og fælles standarder for sikkerheden i de offentlige IT-infrastrukturer.

3.7.2. CSC: Behov for at sikre samfundskritiske systemer

IT-virksomheden CSC Danmark er en af de største leverandører af IT-løsninger til den offentlige sektor herhjemme. CSC leverer drift og udvikling af en række centrale IT-systemer som

fx CPR-registeret, politiets systemer og skattesystemerne. Gennem statens DataNet leverer CSC endvidere netværksadgang til bl.a. EU's intranet for store statslige virksomheder. CSC samarbejder derudover med mere end 130 kommuner og en lang række amtslige og statslige institutioner om realiseringen af det digitale Danmark.

I fremtiden vil information og interaktion forløbe elektronisk, hvilket giver de offentlige myndigheder nye unikke muligheder for at samarbejde interaktivt med borgere og virksomheder i Danmark. I CSC mener man, at digitaliseringen af det offentlige er det IT-lokomotiv, som vil bringe Danmark i den absolutte informationsteknologiske front og samtidig påvirke den måde, hvorpå alle andre dele af samfundet fungerer.

Men en succesfuld offentlig digitalisering forudsætter bl.a., at sikkerheden er i top. Og her er billedet ikke entydig positivt, mener Account Manager i CSC Public Sector. Han pointerer, at de IT-folk, der sidder i staten, amterne og kommunerne generelt gør et stort og godt arbejde. Men rent sikkerhedsmæssigt er billedet meget fragmenteret og hullet – og det bekymrer. Mange har lært at håndtere vira, og man sørger for at tage backup – men når det kommer til beskyttelse mod egentlig cyberterrorisme, så er kun de færreste offentlige institutioner tilstrækkelig godt forberedt, siger CSC-chefen.

CSC har i eget hus opbygget en sikkerhedsinfrastruktur, som på alle væsentlige områder vil kunne modstå cyberterrorisme. De IT-systemer, som CSC driver for offentlige og private virksomheder, er fx placeret 10 meter under jordoverfladen. Medarbejdere med adgang til de vitale, offentlige systemer er oftest clearet af PET/FE, og omkring en række af systemerne er der opbygget en adgangsvej til data, som går gennem tre lag af firewalls, som er opbygget efter tre forskellige principper. Virksomheden investerer løbende i forbedringer af sikkerheden i infrastrukturen. På globalt plan har CSC bl.a. udviklet programmer, der kan finde huller i netværk, og ansat et team af hackere, der løbende tester IT-systemerne.

CSC-chefen fastslår dog, at intet system er 100 procent sikkert – og at CSC i øvrigt leverer det sikkerhedsniveau som kunden ønsker at betale for. Dog har CSC nogle mindstekrav på sikkerhedsområdet, der skal være opfyldt for at virksomheden accepterer ansvaret for driften af en applikation. Desværre er det en gennemgående tendens, at de nyeste sikkerhedsydelser ikke efterspørges forretningsmæssigt – før det er for sent, siger han.

Som lovgivningen er i dag, har fx en offentlig forvaltning ikke pligt til at anvende hverken virusskanning af indgående post, katastrofe backup (dobbelt drift af systemet) eller særligt aflukkede driftsafsnit med særligt betroet personale. Generelt er dette ikke et stort problem, men for en håndfuld IT-systemer udgør det en sårbarhedsrisiko, mener man i CSC, hvor holdningen er, at tiden er inde til, at langt flere private og offentlige virksomheder begynder at tage truslerne alvorligt og investerer i den nødvendige sikkerhed.

CSC fastslår videre, at man som udgangspunkt for at minimere sårbarheden i den offentlige IT-infrastruktur, skal definere de systemer, som er kritiske for driften af det danske samfund – et initiativ, der allerede burde have været indført i forbindelse med terrorlovgivningen i kølvandet på 11. september, mener CSC-chefen. Samtidig påpeger han, at det er helt afgørende, at der bliver udviklet og lovfæstet fællesregler for disse kritiske systemers drift og for adgangen til dem. Fællesregler for IT-sikkerheden i kritiske systemer vil medføre, at man opnår konvergens i sikkerhedsniveauerne mellem de forskellige systemer, fordi disse i dag specificeres af forskellige ministerier, og derefter leveres af forskellige leverandører med forskellige holdninger til sikkerhed. Det vil bl.a. medføre en mindre sårbarhed end i dag, mener CSC-chefen, der sætter spørgsmålstegn ved, om den undersøgelse fra Danmarks Statistik og Ministeriet for Videnskab, Teknologi og Udvikling fra foråret 2003, som viste, at bl.a. den offentlige sektor var plaget af virus, er udtryk for, at der er en markant sårbarhed. CSC er selv udsat for flere tusinde angreb om ugen i form af bl.a. portscanninger, men formår at beskytte sig mod indtrængen. CSC har i hvert fald endnu ikke

haft hændelser, som har berørt nogle af de vitale offentlige systemer, virksomheden driver.

3.7.3. Rigsrevisionen påpeger alvorlige sikkerhedsproblemer i staten

Staten er opdelt i ca. 250 "virksomheder" – en virksomhed kan fx være et departement eller en styrelse under et ministerium. Rigsrevisionen har to hovedopgaver – dels at udføre forvaltningsrevision – det vil sige undersøge, om disse statslige virksomheder bruger deres penge fornuftigt, dels at gennemføre finansiel revision af samme. Under sidstnævnte hører IT-revision, hvor Rigsrevisionen kortlægger og vurderer IT-håndteringen.

Ifølge Rigsrevisionens kontorchef med ansvar for IT-revision i statslige virksomheder, tegner der sig generelt et positivt billede af de statslige virksomheders håndtering af IT-sikkerhed. En meget stor andel har formået at imødekomme de hidtidige sikkerhedsmæssige udfordringer. På den anden side er kun et fåtal rustet til at møde de omfattende sikkerhedsmæssige udfordringer i det stadig mere digitaliserede statsapparat. Når papir bliver fortid og informationerne i stedet er digitale, indebærer det, at virksomhedernes korrespondance med borgere og andre virksomheder – fx afgørelser på sager og andre sagsakter, elektroniske bilag og fakturaer, kalender- og mødeaktiviteter m.v. – forsvinder, når systemerne går ned. Det vil sige, at tilgængeligheden til informationerne bliver endnu mere kritisk end det er tilfældet i dag. Kontorchefen peger på, at det netop er besluttet, at al skriftlig kommunikation indenfor staten fremover skal foregå elektronisk via e-mail. Det vil reelt betyde, at alle processer i staten bliver afhængige af, at Internettet og den enkelte institutions interne systemer, er "oppe at køre". Hvis nettet eller de interne systemer af den ene eller anden årsag – fx strømforsyningssvigt eller sabotage – bryder sammen, så kan statsapparatet ikke fungere uden væsentlige vanskeligheder.

Rigsrevisionen udførte i 2002 IT-revision af 34 statslige virksomheder. Selvom det som nævnt generelt er et positivt billede, der tegner sig i de statslige institutioner, så er der også på nogle områder konstateret behov for at forbedre IT-håndteringen. I mere end halvdelen af de undersøgte institutioner, havde Rigsrevisionen anbefalinger på følgende områder:

IT-styring: Der er behov for, at ledelserne i langt højere grad end det sker i dag fokuserer på de risici, der også er forbundet med IT-anvendelsen. Udviklingen fra dengang hvor IT var en lille fritstående maskine i hjørnet af økonomiafdelingen og til i dag, hvor virksomhedens drift og udvikling afhænger af IT systemerne, er foregået over en meget kort årrække. Den erkendelse er ikke slået igennem på alle direktionsgange. Der er bl.a. behov for, at den enkelte ledelse kortlægger risici og tager stilling til og implementerer det ønskede sikkerhedsniveau, lyder det fra Rigsrevisionen.

Adgangskontrol: Der er behov for, at den enkelte virksomhed tilrettelægger procedurer med klare retningslinier for, hvem der kan få adgang til systemer og data. Dette har man ikke i tilstrækkelig omfang i dag, hvor situationen er den, at de statslige virksomheder ikke sikrer, at alle bruger-id'er er personlige. Samtidig er man ofte for rundhåndede med at uddele administratorrettigheder, hvilket indebærer, at nogle har rettigheder i systemerne, som er unødvendigt store i forhold til de opgaver, de skal løse. Endelig udfører man ikke i tilstrækkelig omfang periodisk opfølgning på, om brugerrettighederne stadigvæk er korrekte, lyder det fra Rigsrevisionen.

Eksterne dataforbindelser: Statslige virksomheder mangler ofte at udarbejde overordnede politikker for, hvordan de styrer deres eksterne dataforbindelser – det vil bl.a. sige Internetforbindelser, dataudveksling mellem servere og kommunikation mellem hjemmearbejdspladser og virksomhed. Med udgangspunkt i en risikovurdering skal virksomheden tilrettelægge procedurer med klare retningslinier for periodisk opfølgning på sikkerhedsniveauet, så man hele tiden matcher de nye risici, der opstår i kølvandet på den teknologiske udvikling. Ifølge Rigsrevisionens IT-revisionschef overlades vurderingen af sikkerheden i eksterne dataforbindelser i dag ofte til virksomhedens tekniske personale.

Overvågning af netværk: Rigsrevisionen konstaterer, at de statslige virksomheder kun i et begrænset omfang overvåger driften af deres netværk for unormale hændelser. Det betyder, at man ofte reelt ikke ved, hvad der foregår i systemerne. Kontrol af såkaldte "logs" – det vil sige aktiviteter i systemerne – er ofte fraværende, hvorfor man ikke altid opdager unormale hændelser. Rigsrevisionens IT-revisionschef omtaler en statsinstitutions IT-systemer, der i 2002 blev misbrugt til ulovlig udveksling af filer til musik og spillefilm. Misbruget kunne finde sted, fordi institutionen ikke gennemførte en systematisk overvågning af sit netværk.

Beredskabsplaner: Endelig er virksomhederne generelt ikke omhyggelig nok med at udarbejde beredskabsplaner. Virksomheden bør tage stilling til, i hvor lang tid man kan acceptere at være uden IT – og beredskabsplanerne skal udarbejdes i overensstemmelse hermed. Manglende beredskabsplaner kan medføre nedbrud, som ligger langt ud over det acceptable for virksomhedens drift og samfundsmæssige opgave.

Rigsrevisionens IT-revisionschef mener overordnet, at der er behov for en koordineret, national indsats, som kan øge sikkerheden i de offentlige IT-systemer. Han peger på, at Ministeriet for Videnskab, Teknologi og Udvikling har udsendt et høringsforslag til en standard for IT-sikkerhed i statslige institutioner. I Rigsrevisionen finder man dette initiativ nødvendigt, og man håber, at det kan være en forløber for udvikling og implementering af fælles standarder for IT-sikkerhed i hele den offentlige sektor. Rigsrevisionen offentliggør i december 2003 en tværgående undersøgelse af de statslige virksomheders IT-anvendelse.

4. Flere holdninger og initiativer på IT-sikkerhedsområdet

4.1. To vurderinger af Internetsikkerhed samt anbefalinger

4.1.1. Dansk rapport: Internettet er et godt og sikkert kommunikationsnet

Enhver risiko kan opgøres ud fra en samlet vurdering af trusler, sårbarheder og konsekvenser i tilfælde af, at en bestemt hændelse indtræder. For væsentlige risici bør der træffes afværgeforanstaltninger, som kan reducere eller i bedste fald eliminere risikoen – hedder det i rapporten, "IT-sikkerhedsrådets udredning om Internet sårbarhed", der blev udsendt i februar 2000. Ifølge rapporten bør enhver Internetforbindelse underkastes en risikovurdering med henblik på at iværksætte de rette sikkerhedsforanstaltninger i form af firewalls, routere, kryptering, sikkerhedspolitikker, overvågning m.v. Hvis man træffer de rigtige forholdsregler og beskytter sig mod de sårbarheder, Internettet rummer, er Internettet, konkluderer rapporten, et godt og driftsikkert kommunikationsnet. Når det gælder ISP'er, der repræsenterer knudepunkter på IT-infrastrukturen, anbefaler rådet, at der dels udarbejdes detaljerede nød- og beredskabsplaner, dels etableres alternative driftscentre og knudepunkter, der kan tages i brug i tilfælde af fysisk ødelæggelse af en installation.

4.1.2. Dansk rapport: Bedst mulige sikkerhed inden for en kalkuleret risiko

Af forsvarsministeriets rapport fra 2001, "Samfundets sårbarhed som konsekvens af IT-anvendelsen", fremgår det, at man som virksomhed, selvom der bliver truffet alle mulige teknologiske og fysiske beskyttelsesforanstaltninger, ikke kan beskytte sine data og IT-systemer 100 procent, når man åbner sit lokalnet op mod Internettet. På den baggrund må man bringe begrebet "Risk Management" på banen – det vil sige, at man søger at opnå den bedst mulige sikkerhed inden for en kalkuleret total risiko.
I rapporten anbefales det, at Danmark, for at styrke IT-sikkerheden på nationalt niveau, iværksætter en koordineret indsats mod IT-kriminaliteten. Det skal bl.a. ske ved at etablere en beredskabsorganisation til varetagelse af IT-sikkerheden på nationalt niveau.
Organisationen, som i rapporten kaldes "Koordinationscenter for beskyttelse af national IT-infrastruktur" skal bl.a. overvåge og indsamle erfaringer om mulig kriminel aktivitet på Internettet, ligesom den vil få til opgave at varsle de myndigheder, der indgår i beredskabet.
I rapporten foreslås det, at koordinationscentret sammensættes af repræsentanter fra DK-CERT, ISP'er m.fl., NALLA (National Long Lines Agency), PET, FE, Nationalt efterforskningsstøttecenter, Response Teams, en tværministeriel referencegruppe og interessenterne (de vitale samfundsområder såsom elforsyning, vandforsyning, telekommunikation m.v.).

4.2. DK-CERT: Indfør lovfæstede mindstekrav til IT-sikkerhed i det offentlige

Der er ikke et samlet overblik over, hvilke Internetbaserede netværk, der eksisterer i Danmark. Der er heller ingen koordinerende instans, som overvåger IT-infrastrukturen, og som man kan melde ind til, hvis man observerer problemer i form af vira og hackere. Ej heller findes der et decideret IT-sikkerhedsberedskab på alle vitale samfundsområder. Der bør snarest iværksættes initiativer på disse områder, mener man i DK-CERT.

Konkret peger man på, at der skal skabes overblik over IT-infrastrukturen på alle vitale samfundsområder – det vil bl.a. sige, at der skal skabes klarhed over, hvordan man skal handle, hvis der går noget galt i infrastrukturen. Samtidig skal det sikres lovgivningsmæssigt, at man er forpligtet til at melde vira/hackerproblemer til den centrale, koordinerende enhed, som herefter kan hjælpe med at forbedre sikkerheden i den pågældende virksomhed – og bevirke, at problemet ikke gentager sig i andre virksomheder.

I DK-CERT mener man videre, at der bør formuleres en officiel dansk strategi for IT-sikkerhed, som opstiller en række mindstekrav, der skal være opfyldt i offentlige virksomheder: For det første skal enhver pc eller server indeholde automatisk opdaterbart antivirusprogrammel samt være firewall-beskyttet. For det andet skal alle offentlige virksomheder registrere trafik og trafikmønstre ved hjælp af Intrusion Detection System (IDS), hvilket begrænser risikoen for, at virksomheden bliver hacket uden at man opdager det. For det tredje skal de ansætte en person, der forstår hvad Internetsårbarhed- og sikkerhed er, ligesom de skal have en stadig opdateret sikkerhedspolitik, som kontinuerligt tager højde for nye sårbarheder.

4.3. Rådet for IT-sikkerhed: Vi skal skabe en naturlig sikkerhedsadfærd

Emner som cyberterrorisme og IT-infrastrukturens sårbarhed står langt nede på dagsordenen hos Rådet for IT-sikkerhed. Eller rettere på det kommissorium, politikerne har formuleret og som udstikker rådets fokusområder. Øverst står udvikling af en informationsindsats, som er målrettet IT-sikkerheden hos private borgere og små- og mellemstore virksomheder. Det handler om at opbygge en egentlig IT-sikkerhedskultur i Danmark, som ikke mindst kan bidrage til at accelerere implementeringen af den digitale offentlige sektor.

Formanden for Rådet for IT-sikkerhed pointerer, at der generelt i Danmark er behov for at fokusere langt mere på IT-sikkerhed end det sker i dag. Det skyldes alene, at IT er noget relativt nyt, som langt fra alle danskere endnu har opbygget nogle naturlige sædvaner omkring. Vi skal udbrede en naturlig adfærd i forhold til IT-sikkerhed – fx at man opbevarer passwords fornuftigt, fastslår han.

Rådsformanden vurderer, at årsagen til, at rådet ikke er sat til at fokusere på emner som cyberterrorisme og beskyttelse af IT-infrastrukturen er, at et sådant arbejde så småt er ved at finde sin form i regi af en national sårbarhedsudredning. Formanden tøver dog ikke med at fastslå, at der efter hans mening er et stort behov for en koordineret og snarlig national samtænkning med henblik på at styrke IT-infrastrukturen i Danmark.
Ligesom en IT-afhængig virksomhed i dag skal have en IT-sikkerhedspolitik og -beredskabsplan, så skal samfundet selvfølgelig også have det i forhold til sine væsentligste sektorer. Der har i årevis været et lovfæstet beredskab på teleområdet. IT-infrastrukturen har i dag har mindst lige så stor betydning som tele-infrastrukturen, hvorfor der naturligvis skal laves tilsvarende planer for IT-området, fastslår formanden for Rådet for IT-sikkerhed.

4.4. Center for IT-sikkerhed: Danmark har brug for en national sikkerhedspolitik og en forebyggende indsats

Internettet har skabt et samfund, der på visse områder er mere sårbart end for 10 år siden. Tidligere skulle man tiltvinge sig fysisk adgang til en lokation for at forrette skade, i dag kan adgangen i mange tilfælde finde sted via Internettet. Samfundets sårbarhed over for cyberterrorisme vil blot vokse og vokse med tiden, forudser lederen af Center for IT-sikkerhed på Alexandra Instituttet i Århus.

Han mener, at Danmark med fordel kunne sætte ind på tre områder: Iværksætte en forebyggende indsats på uddannelsesområdet, udarbejde en national sikkerhedspolitik og etablere en synlig, national IT-sikkerhedschef. Han vurderer videre, at informationskampagner over for brugere, IT-ansvarlige og ledere er absolut nødvendige.
Hvad angår indsatsen på uddannelsesområdet, så peger han på, at IT-sikkerhed i højere grad

skal indgå i de eksisterende IT-uddannelser inden for netværk og systemudvikling. Men endnu vigtigere finder han det, at IT-sikkerhed vinder indpas på det ledelsesmæssige plan, så beslutningstagere i private og offentlige virksomheder er bevidste om deres ansvar og roller på dette område – at de ikke kun betragter IT-sikkerhed som et teknisk problem, men er klædt på til at stille krav til IT-afdelinger og leverandører.

Lederen af Center for IT-sikkerhed mener videre, at Danmark har brug for en national IT-sikkerhedschef. En person, der refererer passende højt op i samfundssystemet, og som kan sikre fokus på og koordinerer arbejdet med IT-sikkerhed – og vigtigst af alt – sørger for at skabe synlighed om, at IT-sikkerhed er sat højt på samfundets dagsorden og er noget, der skal tages alvorligt. Han fastslår dog samtidig, at han finder det problematisk, at der i Danmark ikke er foretaget en overordnet samfundsmæssig risiko-konsekvensanalyse i forhold til IT-sikkerhed, som afdækker både aktiver og hvor galt det kan gå. Kun ved at gennemføre en sådan analyse kan man sikre, at samfundet og virksomhederne ikke spilder ressourcer på de forkerte områder, pointerer han.

4.5. Hvidbog om IT-arkitektur: Struktureret håndtering af IT-sikkerheden er en helt afgørende parameter for udbredelse af digital forvaltning

Det koordinerende Informationsudvalg – et tværoffentligt koordinationsorgan på det IT-faglige område – udsendte i juni 2003 "Hvidbog om IT-arkitektur". Formålet med hvidbogen, der er et led i udbredelsen af digital forvaltning herhjemme, er at "opnå et generelt kvalitetsløft af den proces, hvorunder offentlige IT-systemer udvikles."

En specifik diskussion af IT-sikkerhedsspørgsmål udgør kun en meget begrænset del af hvidbogen. Det fremgår dog bl.a., at en struktureret håndtering af IT-sikkerheden vurderes som en helt afgørende parameter for udbredelse af digital forvaltning. Sikkerheden er imidlertid ikke blot noget, som kan tilsættes den færdige løsning, hedder det, sikkerhedskravene må være indarbejde i arkitekturprocessen lige fra visionsstadiet.

Ifølge hvidbogen er det en forudsætning for sammenhæng på sikkerhedsområdet, at krav og løsninger beskrives udfra et fælles koncept og koordineres på det overordnede plan. Samtidig fremgår det, at en grundig risikoanalyse bør være afgørende for valget af sikkerhedsarkitektur og sikkerhedsløsninger, og det anbefales, at det offentlige benytter fælles principper for denne analyse.

4.6. IT-sikkerhedsekspert: En ulige og konstant kamp mod hackere og vira

Det er i praksis en umulig opgave at afdække alle sikkerhedshuller i et komplekst IT-system. IT-systemer omfatter typisk produkter fra mange forskellige leverandører, der hver især skal være ufejlbarlige. Der kan være fejl i hardware, fejl i systemsoftware, fejl i applikationer og fejl i selve den valgte sikkerhedsmodel. Og der findes ikke en generel test, der med sikkerhed kan fastslå, at et IT-system er sikkert, forklarer en IT-sikkerhedsekspert fra firmaet MindSoft.

Han understreger, at en IT-sikkerhedsafdelings arbejde derfor på mange måder er en ulige kamp mod hackere og lignende: Mens sikkerhedsafdelingen skal sikre, at ethvert tænkeligt hul i sikkerheden lukkes, skal en hacker blot finde et eneste hul for at bryde sikkerheden. En sikkerhedsafdeling har en begrænset mængde ressourcer, mens hackere findes i ubegrænset antal. Dertil kommer, at der findes et meget stort antal frit tilgængelige Internetsider, der løbende publicerer fundne sikkerhedshuller i standardsoftware, hardware, firewallprodukter og lignende. Dette gør det ofte til en triviel opgave for ukyndige at få adgang til IT-systemer, der ellers har været tiltroet stor sikkerhed.

Implementering af sikkerhed er ressourcekrævende og intet sikkerhedssystem er 100 procent sikkert. Jo større grad af sikkerhed, der ønskes, des flere ressourcer kræves der for at håndhæve sikkerheden. Valg af sikkerhedsniveau for et IT-system vil derfor altid

være en afvejning mellem prisen (cost) og fordelene (benefit), pointerer IT-sikkerhedseksperten og understreger, at niveauet for et IT-systems sikkerhed afspejler dets evne til at modstå enhver trussel, der kan påvirke dets kvalitet, anvendelse og funktionalitet. Jo større sikkerheden i et IT-system er, des mindre sårbart er systemet overfor truslerne – det vil bl.a. sige forsøg på at få adgang under falsk identitet, hacking, indførsel af virus eller virusorme, der kan gøre systemet utilgængeligt eller medføre skadelige ændringer af applikationer.

For at mindske sårbarheden skal alle de trusler, der er mod IT-systemet, afdækkes. Det sker ved at gennemføre en risikovurdering, hvor truslerne identificeres og hvor der sker en vurdering af konsekvenserne i form af fx økonomisk tab, hvis de fundne trusler realiseres. Risikovurderingen skal løbende – og proaktivt – revideres i takt med at nye trusler opstår og identificeres. En revidering af trusselsbilledet skal straks afspejles i fastlagte standarder og best practices og herefter hurtigst muligt implementeres i de berørte IT-systemer, fastslår han.

4.7. Internationalt samarbejde om IT-sikkerhed

Kommunikations- og informationstjenester udbydes i dag på tværs af landegrænser – og virus- og hackertrusler er ligeledes verdensomspændende. På den baggrund fremhæver Rådet for IT-sikkerhed, at effektive sikkerhedsfremmende løsninger nødvendigvis må bygge på internationale standarder. Derfor mener man, at en styrkelse af det internationale samarbejde, herunder et arbejde frem mod fælles standarder inden for IT-sikkerhed, vil være til gavn for hele det danske samfund.

En dansk IT-sikkerhedsekspert peger i den forbindelse på, at internationale standarder indebærer en ny risiko, nemlig at huller i disse fælles beskyttelsesforanstaltninger vil åbne for, at hackere og vira kan trænge ind overalt, hvor standarderne er implementeret.

"Riskoen for cyberangreb vokser, og efter den 11. september er der stigende risiko for alvorligere angreb," sagde EU-kommissær Erkki Liikanen, da EU's ministerråd i slutningen af 2002 vedtog at styrke koordinationen og samarbejdet i EU om IT-sikkerhed. Konkret sker det ved at oprette et center for IT-sikkerhed kaldet "Network Security Agency". Centret, der skal stå klar i 2004, får til opgave at koordinere det IT-sikkerhedsarbejde, der foregår i medlemslandene. De nationale Computer Emergency Reponse Teams (CERT) vil spille en central rolle som bl.a. videnindsamlere og koordinatorer i de enkelte lande.

DK-CERT er formand for et udvalg under EU, som har fået til opgave at udvikle et "Early Warning System", som skal sikre, at alle vitale samfundsområder og formentlig også virksomheder i EU-landene modtager en hurtig advarsel, hvis der fx konstateres en ny virus/orm undervejs. I DK-CERT understreger man, at advarselssystemet ikke vil kunne foregribe begivenhedernes gang, men at man meget hurtigt kan melde ud, hvis der sker noget på området. Herefter kan de enkelte virksomheder og institutioner skride til hurtig handling med henblik på at undgå eller begrænse den potentielle skadevirkning. Med en advarsel fra systemet vil der typisk også følge informationer om, hvordan den enkelte virksomhed handler optimalt i situationen, forklarer man i DK-CERT, der sammen med EU-udvalget skal aflevere et komplet "Early Warning System" i januar 2004.

4.8. En national dansk sårbarhedsudredning undervejs

Folketinget igangsatte i 2002 arbejdet med at udforme en national sårbarhedsudredning på en lang række samfundsområder. Det overordnede formål er at kortlægge samfundets sårbarhed og give en vurdering af den civile sektors beredskab i forhold til de konstaterede sårbarheder. Udredningen fokuserer på områder, som er af væsentlig betydning for samfundets sikkerhed og stabilitet, herunder bl.a. IT-infrastrukturen. Arbejdet foregår i regi af Indenrigs- og Sundhedsministeriet, mens sårbarhedsudredningens sekretariat ligger hos Beredskabsstyrelsen.
Den nationale sårbarhedsudredning er inspireret af tilsvarende arbejder, som har fundet sted i både Sverige og Norge i de senere

år. I Sverige under overskriften "Säkerhet i en ny tid" og i Norge "Samfunnssikkerhet – Veien til et mindre sårbart samfunn".

"Underudvalget vedrørende el, naturgas- og teleforsyning samt IT-forhold" er et af en række udvalg under den nationale sårbarhedsudredning. Underudvalget har til opgave at udarbejde en delrapport, som beskriver områdets sårbarhed og de beredskabsmæssige tiltag, der findes i dag – og ikke mindst giver en vurdering af, hvor de væsentligste udfordringer findes. Den samlede nationale sårbarhedsudredning skal foreligge den 14. april 2004.

Når el, naturgas, tele og IT er lagt sammen skyldes det, ifølge formanden for udvalget, at de er indbyrdes afhængige af hinanden: Fx kan el- eller gasforsyningen ikke fungere uden tele og IT, ligesom hverken tele-infrastrukturen eller IT-infrastrukturen kan fungere uden el.
I udvalget vil man dels fokusere på sårbarhederne på de enkelte områder, dels på sårbarhederne de steder, hvor der optræder gensidig afhængighed og finder overlapninger sted mellem dem. Der er dannet henholdsvis en IT-, tele, gas- og el-beredsskabsgruppe.

I forlængelse af sårbarhedsudredningen vil man i IT-sikkerhedskontoret under IT- og Telestyrelsen arbejde videre i retning af at komme med anbefalinger til den opbygning af et egentligt IT-beredskab i staten, som man i høj grad mener, at der er behov for. Chefen for IT-sikkerhedskontoret oplyser, at man følger og bidrager til arbejdet på IT-sikkerhedsområdet i EU – også med henblik på at skabe koordination mellem de nationale tiltag og de tiltag, der gennemføres på EU-niveau.

5. Kilder

- "*How to Own the Internet In Your Spare Time*," 2002. Forfatter: Bl.a. Nicholas Weaver, UC Berkeley, USA. Kan downloades fra www.uritytopics/security/holes/story/0,10801,75315,00.html.
- "*Samfundets sårbarhed som konsekvens af IT-anvendelsen*". Rapport fra Forsvarsministeriet, september 2001. Intern rapport – forespørgsel til IT-fagligt Center i Ministeriet for Videnskab, Teknologi og Udvikling.
- "*IT-sikkerhedsrådets udredning om Internet sårbarhed*". Rapporten kan downloades fra www.videnskabsministeriet.dk/fsk/publ/2001/itsikker/ren.htm.
- "Hvidbog om IT-arkitektur", juni 2003, kan downloades fra www.oio.dk/arkitektur/hvidbog.
- "*Information Security in Europe*". Rapporten er udarbejdet af KPMG IT Risk Management og kan downloades fra IT- og Telestyrelsens hjemmeside – www.itst.dk.
- Kommissorium for en national sårbarhedsudredning samt Kommissisorium for udvalget vedrørende el, naturgas- og teleforsyning samt IT-forhold – www.im.dk
- Danmarks Statistik: "Den offentlige sektors brug af IT, 2002". "Danske virksomheders brug af IT, 2002". "Befolkningens brug af Internet, 4.kvartal 2002".
- Den svenske sårbarheds- og sikkerhedsudredning, del 1 og 2 samt bilag og udtalelse fra Statsministeriet kan downloades fra:
  http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41a.pdf
  http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41b.pdf
  http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41c.pdf
  http://www.statskontoret.se/pdf/remissvar/2001227.pdf
- Den norske rapport "Samfunnssikkerhet – Veien til et mindre sårbart samfunn" kan downloades fra: http://odin.dep.no/jd/norsk/publ/stmeld/012001-040015/index-dok000-b-n-a.html.
- Info. om internationalt seminar om IT-sikkerhed afholdt af IT- og Telestyrelsen i april 2002 – www.itst.dk/wimpprint.asp?page=tema&objno=98571563.
- Rådet for IT-sikkerhed (et uafhængigt råd, der er nedsat af Ministeren for Videnskab, teknologi og udvikling) – www.videnskabsministriet.dk.
- IT-sikkerhedskontoret (under IT- og Telestyrelsen) – www.itst.sk.
- Kommissorium for en national sårbarhedsudredning. Indenrigs- og Sundhedsministeriet – www.im.dk/Index/dokumenter.asp?o=7&n=0&d=1762&s=4
- Danish Computer Emergency Response Team (CERT) – www.cert.dk.
- Den centrale CERT-organisation – www.cert.org.
- TDCs CERT-organisation – www.csirt.dk.
- EU-kommissionen. Vedr. Internet- og informationssikkerhed. www.europe.eu.int.
- Den digitale Taskforce – http://e.gov.dk.
- FIRST (Forum of Incident Response and Security Teams) – en international organization, som har DK-CERT som medlem. www.first.org.
- System Administration, Networking and Security (SANS) - forsknings- og uddannelsesinstitution, som arbejder for at holde verden ajour med ny viden og erfaring og nye løsninger på IT-sikkerhedsproblemer. Se bl.a. top20-liste over sårbarheder på www.sans.org/top20.
- US Department of Homeland Security – www.dhs.gov/dhspublic.
- www.forbrugersikkerhed.dk.
- ITEK – Dansk Industris branchefællesskab for IT-virksomheder – www.itek.dk.
- Deloitte & Touche – interviewundersøgelse af 242 danske virksomheder om IT-sikkerhed. Undersøgelsen kan rekvireres på www.deloitte.dk.
- "Beretning om revision af statsregnskabet for 2002" – www.rigsrevisionen.dk.
- DIFO (Dansk Internet Forum) – www.difo.dk.
- WebTrust – info og links på www.fsr.dk/Site/FSRInfo.nsf/no/01001000.

- IDC – IDC Directions 2003 – www.idc.dk.
- DK Hostmaster A/S – www.dk-hostmaster.dk.
- Symantec – www.symantec.dk.
- Artikler i Computerworld, Jyllands Posten, Politiken, Berlingske Tidende og på IT- og Telestyrelsens hjemmeside.

- **Notatet er endvidere baseret på interview med følgende eksperter:**
- Kjell Hermansson, IT-sikkerhedschef i Danske Bank.
- Lars Engbro, IT-chef i NESA.
- Ryan Schnipper, IT-chef i Energi E2.
- Jesper Vedelsby, IT-sikkerhedsekspert, MindSoft.
- Jørn Knudsen, IT-sikkerhedskoordinator i Hovedstadens Sygehusfællesskab.
- Per Verdelin, IT-sikkerhedschef i TDC Koncernen, formand for Dansk Industris IT-sikkerhedsudvalg.
- Per B. Hansen, leder af Center for IT-sikkerhed, Alexandra Instituttet, afdelingschef i TDCs Erhvervsdivision med ansvar for sikkerhedsrådgivning af erhvervsvirksomheder.
- Niels Nygaard, Security Manager i SAS.
- Preben Andersen, chefkonsulent i Uni-C og leder af DK-CERT.
- Freddie Drewsen, leder af Kommunikations- og Informationssektionen (CIS), Forsvarets Forskningstjeneste.
- Allan Fischer-Madsen, formand for Rådet for IT-sikkerhed.
- Henrik Brodersen, chef for IT-sikkerhedskontoret, IT- og Telestyrelsen. Formand for "Underudvalget vedrørende el-, naturgas- og teleforsyning samt IT-forhold" under den Nationale Sårbarhedsudredning.
- Lars Hagerup, kontorchef i Amtsrådsforeningen med ansvar for IT-sikkerhed.
- Christian Wernberg-Tougaard, Account Manager i Public Sector, CSC Danmark A/S.
- Steen Bernt Jensen, kontorchef i Rigsrevisionen med ansvar for IT-revision i statslige virksomheder.

Teknologirådet

Antonigade 4
1106 København K

Telefon 33 32 05 03
Telefax 33 91 05 09

tekno@tekno.dk
www.tekno.dk

Giro 8 51 07 68

Teknologirådet har til opgave at:

fremme
teknologidebatten

vurdere teknologiens
muligheder og konsekvenser

rådgive folketinget
og regeringen