Fra rådet til tinget
TEKNOLOGIRÅDETS NYHEDSBREV TIL FOLKETINGET

Nr. 190 | Februar 2004

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

ISSN: 1602-4311

Infrastruktur åben for cyberterror?

Eksperter anbefaler at få overblik over Danmarks it-relaterede sårbarhed

Manglende viden om Danmarks it-sårbarhed >

Vitale samfundsfunktioner kan lammes via internettet >

Der er behov for en bredt favnende undersøgelse >

Der er behov for at skabe overblik over it-infrastrukturens sårbarhed i det stadig mere digitaliserede Danmark.
Dag for dag vokser risikoen for internetbaseret sabotage af vitale samfundsfunktioner. Det kan koste store summer og i yderste konsekvens menneskeliv. Teknologirådets arbejdsgruppe ønsker en omfattende undersøgelse, der kan skabe opmærksomhed om problemerne og angive løsninger, som begrænser Danmarks it-relaterede sårbarhed. Læs arbejdsgruppens øvrige anbefalinger sidst i nyhedsbrevet.

Dette Fra rådet til tinget uddrager essensen af Teknologirådets arbejdsgruppe om it-infrastruk-turens sårbarhed og en workshop, der blev til-rettelagt i samarbejde med Forsvarets Forsknings-tjeneste.

It spiller en stadig større rolle i Danmarks kritiske infrastruktur – det vil sige de samfundsstrukturer, som er afgørende for, at nationen kan fungere på alle niveauer. Den kritiske infrastruktur omfatter mange forskellige områder fra energi- og vandforsyning og kommunikation til sygehusvæsen, finanssektor og centraladministration. It-infrastrukturen udgør en voksende del af teleområdet, netværk (fra det åbne internet til lukkede og dedikerede netværk) og tilhørende it-systemer og går således på tværs af de traditionelle sektorer.
Internettet har uvurderlige fordele, men nettets udbredelse gør også samfundet mere sårbart og stiller nye sikkerhedskrav til it-infrastrukturen. Sårbarheder som det danske samfund ikke har overblik over – og krav, som vi sjældent er i stand til at honorere.

Truslerne fra cyberspace

Private og offentlige virksomheder i Danmark prioriterer traditionel sikkerhed i form af lås på dørene og effektive tyverialarmer langt højere end it-sikkerheden. Digitaliseringen af samfundet vokser og vokser, men samtidig er vores it-systemer ofte pivåbne for uautoriseret indtrængen af vira, orme eller hackere til personfølsomme og andre kritiske data.
Den manglende it-sikkerhed koster hvert år samfundet et ukendt milliardbeløb. Det er ikke gået op for danskerne, hvilke konsekvenser, vi risikerer at løbe ind i, hvis vi ikke begynder at tage it-sikkerheden langt mere alvorligt end i dag, lyder det fra Danish Computer Emergency Responce Team (DK-CERT), der er en offentlig it-sikkerhedsorganisation.
Nationalt Efterforskningsstøttecenter under Rigspolitichefen har i de seneste 4-5 år registeret fortsat vækst i antallet af anmeldelser af hacking. Og i DK-CERT er man ikke i tvivl om, at egentlig cyberterrorisme er i vente. Ved at lamme internettet i kortere eller længere tidsrum og dermed få al internetbaseret dataudveksling til at bryde samme, kan fremtidens digitale terrorangreb få vitale samfundsfunktioner til at bryde sammen.
Risikoen stiger og nye trusler opstår i takt med realiseringen af visionen om Det Digitale Danmark, hvor information og viden kan flyde frit. Den offentlige

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

ISSN: 1602-4311

sektor vil servicere borgerne elektronisk, internetbanker vinder frem, kommunikationssøgning, nyhedsformidling og kontakt mellem mennesker sker i stigende grad via internettet.
I de senere år er der talrige eksempler på, at it-sikkerheden har spillet fallit, når indtrængende vira og orme har lagt tusinder af computere ned i både private og offentlige virksomheder. Et af de seneste eksempler er ormen "Sobig.F", der i august 2003 ramte store dele af statsadministrationen, herunder Folketinget, der fik blokeret sin emailkommunikation. Danske virksomheder og institutioner bliver kontinuerligt angrebet via internettet. En typisk konsekvens er, at virksomhedens servere bliver overbelastet og "går ned", eller at vira trænger ind og ødelægger eller sletter data.

Truslerne – og hvor de kommer fra

De mest almindelige trusler via internettet er skadevoldende programmer (virus, orme, trojanske heste, fjernstyringsprogrammer, spyware), skadelig kode på websider (ActiveX), portscanning (forsøg på at finde sårbare computere), hacking (overtagelse af kontrollen med computere), sniffing (opsamling af datapakker), Denial of Service angreb (offerets system sættes ud af drift), webgraffiti (websiders information ændres), falske advarsler via email (spilder tid, diskplads og båndbredde), spam (spilder tid, diskplads og båndbredde), misbrug af åbent mailrelæ (videresendelse af spam uden ejerens vidende).
Derudover kan truslerne mod it-infrastrukturen komme via fysisk adgang – og for eksempel involvere en medarbejder, en hacker, tyveri af it-udstyr eller opstå som følge af ildebrand, overgravning af kabler og lignende. Et nedbrud af it-infrastrukturen kan skyldes fejl, uheld eller en bevidst handling med et konkret formål. Konsekvenserne kan være afsløring af data (uvedkommende bryder fortroligheden), ændring af data (uvedkommende laver om på data), tab/ødelæggelse af data eller afbrydelse/nedlukning, hvor systemet holder op med at virke.
Kilde: OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), der er en beregningsmodel til brug ved risikovurdering.

Holland er godt i gang

På Teknologirådets workshop om it-infrastrukturens sårbarhed berettede Eric Luiijf, chefkonsulent i TNO – en hollandsk søsterorganisation til Forsvarets Forskningstjeneste i Danmark – om de hollandske initiativer på området. Den hollandske regering gennemførte i perioden 2000 til 2002 projekterne "Infodrome" om konsekvenserne af samfundets voksende afhængighed af it, og "KWINT", om sårbarheden af den hollandske del af internettet. Arbejdet mundede ud i tre konkrete tiltag: Etableringen af et "Computer Emergency Response Team" for statsadministrationen. En informations- og virus alarmservice rettet mod små og mellemstore virksomheden og private borgere. Endelig blev der fastsat konkrete evalueringskriterier for sikkerheden hos de hollandske leverandører af internetforbindelser (ISP'ere).
Samtidig satte den hollandske regering et nyt projekt i værk i regi af TNO, som skal munde ud i et regelsæt, der kan beskytte både den statslige og den private it-infrastruktur. Første trin i projektet var at identificere vitale samfundsområder og afdække deres kritiske processer og afhængigheder – for eksempel at nedbrud af strømforsyningen vil have konsekvenser på en lang række andre samfundsområder. Hollænderne har fundet i alt 11 kritiske sektorer, herunder energi, drikkevand, den finansielle sektor, sygehusvæsenet og transport. Hvert område er derudover opdelt i underområder – for eksempel er "transport" opdelt i transport på henholdsvis vej, jernbane, luft og vand samt transport i rørlinier. Også internettet defineres som en vital og kritisk infrastruktur – og afhængighederne på it-området vurderes at være særdeles komplekse og involvere mange aktører.
Andet og tredje trin i projektet, som er undervejs, går ud på at stimulere til samarbejde mellem den offentlige sektor og private virksomheder om at forbedre infrastrukturens sikkerhed. I trin tre gennemføres en trussels- og sårbarhedsanalyse, som skal afdække manglende sikkerhedsforanstaltninger. I en foreløbig konklusion hedder det blandt andet, at truslerne mod infrastrukturen hele tiden ændrer sig. Et samfund skal kunne reagere hurtigt på nye trusler, der skal forebygges via et tæt samarbejde mellem offentlige og private aktører, mener man i TNO.

Forslag fra workshoppen

På Teknologirådets workshop om IT-infrastrukturens sårbarhed diskuterede deltagerne forskellige aspekter af emnet. Afslutningsvis fremkom deltagerne med individuelle forslag til initiativer, som de mente ville kunne mindske sårbarhederne. Nogle deltagere foreslog, at enhver virksomhed bør indføre løbende overvågning med og egenkontrol af sårbarheder og sikkerhedsniveau. Virksomheder bør også indføre nødprocedurer og et lokalt beredskab i tilfælde af strømsvigt.
For at sikre, at alle virus- og hackerangreb bliver indberettet, skal man kunne gøre dette anonymt, lød et tredje forslag på workshoppen. Flere deltagerne mente, at samfundet overordnet set bør vedtage fælles it-standarder, fælles it-terminologi og en fælles praksis for it-sikkerhedsregnskaber. Andre fremførte, at der bør vedtages en lovgivning, som fastsætter minimumskrav til it-sikkerhed i offentlige og private virksomheder.

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyhedsbreve findes på:
www.tekno.dk/rtt.htm

ISSN: 1602-4311

Ingen koordineret dansk indsats
I Danmark er Politiets Efterretningstjeneste national sikkerhedsmyndighed – også på it-området. PET har til opgave at forebygge angreb på danske it-systemer, som har betydning for landets sikkerhed. Forsvarets Efterretningstjeneste udfører også opgaver inden for it-sikkerhed og varsling. Endelig har Nationalt Forskningsstøttecenter under Rigspolitichefen til opgave at overvåge organiseret og kompliceret it-kriminalitet. Derudover påhviler ansvaret for it-sikkerhed i dag den enkelte minister (i henhold til Beredskabsloven) og den enkelte virksomhed i samfundet. Der eksisterer ikke et nationalt beredskab, som koordinerer de beredskaber, der måtte være på lokalt niveau hos myndigheder eller virksomheder.
Kilder: DK-CERT og Forsvarets Forskningstjeneste.

Overordnet set demonstrerede workshoppen en fælles erkendelse af, at kompleksiteten i it-infrastrukturen hele tiden bliver øget. Det giver problemer med teknisk gennemskuelighed og placering af ansvar i virksomhederne. Den indbyrdes afhængighed på tværs af offentlige og private sektorer vokser – og dermed øges sårbarheden over for uønskede hændelser. It-kontrolmulighederne svækkes af outsourcing, globalisering og hurtig udvikling af digital forvaltning.
Der er behov for flere møder på tværs af sektorer for at afdække indbyrdes afhængighed og sårbarheder – og for at arbejde for løsninger til fælles bedste. Det er vigtigt ikke kun at fokusere på centralt dirigerede løsningsforslag på it-infrastrukturens sårbarhed, lød det på workshoppen.

Flere veje til større it-sikkerhed i Danmark

I dag findes der intet samlet overblik over Danmarks it-relaterede sårbarhed. Inden for det seneste år har it-nedbrud i blandt andet den finansielle sektor herhjemme aktualiseret en problemstilling, der både koster samfundet dyrt og i værste fald kan være direkte livstruende for borgerne – for eksempel hvis nedbrud sker i hospitalsvæsenet. Teknologirådet har bedt en række danske nøglepersoner på it-sikkerhedsområdet om deres bud på, hvad der skal til for at starte en udvikling hen imod at begrænse it-infrastrukturens sårbarhed mest muligt.
I betragtning af, hvor mange samfundsaktører, der er afhængige af en sikker og stabil it-infrastruktur, finder Kjell Hermansson, it-sikkerhedschef i Danske Bank, det underligt, at der endnu ikke er iværksat en koordineret indsats for at styrke den internetrelaterede it-sikkerhed på landsplan. Niels Nygaard, Security Manager i SAS, er enig. Han mener, der er et udtalt behov for en koordineret, landsdækkende indsats for at beskytte it-infrastrukturen. Det bør være en "totalforsvarsopgave" helt på linie med beskyttelse af for eksempel el- og varmeforsyningen, siger han og bliver bakket op af Christian Wernberg-Tougaard, Account Manager, Public Sector, CSC Danmark A/S. Der er behov for, at samfundet formulerer regler for driften af og adgangen til samfundskritiske it-systemer. Ensartede regler og sikkerhedsniveauerne vil reducere sårbarheden markant, pointerer CSC-chefen.
Preben Andersen, chefkonsulent I UNI-C og leder af DK-CERT, mener ligeledes, at der er behov for at etablere en koordinerende instans, som overvåger it-infrastrukturen. Samtidig pointerer han behovet for at etablere et IT-sikkerhedsberedskab på alle vitale samfundsområder. Endelig bør der formuleres en officiel dansk strategi for it-sikkerhed, som opstiller en række mindstekrav, som skal være opfyldt i offentlige virksomheder, siger han og får støtte hertil af Jørn Knudsen, it-sikkerhedskoordinator i Hovedstadens Sygehusfællesskab. Jørn Knudsen peger på, at digitaliseringen af den offentlige sektor stiller store krav til it-infrastrukturen i Danmark. Jo større samfundsbetydning og -integration internettet får, jo større bliver behovet for en koordineret indsats, som kan optimere sikkerheden, siger han.
Der skal gennemføres en risiko-konsekvensanalyse i forhold til it-sikkerheden i Danmark. Kun på den baggrund kan man sikre, at samfundet og virksomhederne ikke spilder ressourcer på de forkerte områder i relation til IT, fastslår Per B. Hansen, afdelingschef i TDC og leder af Center for it-sikkerhed ved Alexandra Instituttet. I forlængelse heraf mener Lars Hagerup, kontorchef i Amtsrådsforeningen med ansvar for it-sikkerhed, at tiden er inde til at udvikle konkrete sikkerhedsstandarder, som alle it-leverandører skal basere deres systemer på. Det skal sikre, at alle systemer spiller i samme toneart rent sikkerhedsmæssigt, siger han.

Aktuel analyse af it-infrastrukturen

I efteråret 2003 igangsatte IT- og Telestyrelsen projektet "Statsligt it- og teleberedskab", som skal danne baggrund for udvikling af et moderne beredskab for elektronisk kommunikation i Danmark. Beredskabet skal sikre tilgængelighed til de offentligt udbudte taletelefoni-, internet- og datatjenester i en beredskabssituation, for eksempel ulykker, katastrofer, krig og terrorhandlinger – inklusive cyberterrorisme.
Ifølge Karin Ingrid Kubista fra IT- og Telestyrelsen indeholder projektet blandt andet en national analyse af sårbarheder i it-infrastrukturen, kortlægning af et integreret it- og teleberedskab og en samfundsøkonomisk konsekvensvurdering. Målet er dels at sikre koordination af it- og teleberedskabet på tværs af samfundets sektorer, dels at formulere eventuelle krav til såvel offentlige myndigheder som private virksomheder. Endelig skal projektet komme med forslag til vejledninger på it-sikkerhedsområdet, der er målrettet både borgere, virksomheder og offentlige myndigheder. Arbejdet indledes i februar 2004 og en rapport med analyser og anbefalinger skal ligge klar i juni 2004. IT- og Te-

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

ISSN: 1602-4311

lestyrelsen forventer, at der vil blive truffet politisk beslutning om beredskabet i begyndelsen af 2005.

Opfordring til grundigere undersøgelse

Teknologirådets arbejdsgruppe om it-infrastrukturens sårbarhed mener ikke, at IT- og Telestyrelsens projekt er tilstrækkeligt i forhold til at løse de øjeblikkelige problemer med it-sårbarhed i Danmark. Alene den begrænsede tid, der er afsat til opgaven – 3-4 måneder – vil gøre det særdeles vanskeligt at nå et resultat, som imødekommer behovene, mener arbejdsgruppen.
Teknologirådets arbejdsgruppe mener derimod, at der er behov for en langt grundigere, bredt favnende undersøgelse, som involverer både politiet, forsvaret og civile. Arbejdsgruppen lægger vægt på, at også selve *gennemførelsen* af en sådan undersøgelse er utrolig vigtig. Undersøgelsen vil betyde, at der bliver skabt opmærksomhed om problemstillingerne i alle dele af samfundet – og dét er der et akut behov for, fastslår arbejdsgruppen.

Arbejdsgruppens fem anbefalinger

Teknologirådets arbejdsgruppe kan på baggrund af egne diskussioner på en lang række arbejdsmøder i perioden maj 2003 til januar 2004, samt arbejdet med oplæg til workshop ("Notat om it-infrastrukturens sårbarhed") og resultaterne fra workshoppen, præsentere følgende fem anbefalinger:

- **Arbejdsgruppen anbefaler, at der iværksættes en bredt favnende undersøgelse af it-infrastrukturens sårbarhed i Danmark. Undersøgelsen skal dels skærpe danskernes opmærksomhed i forhold til, *hvor* usikre it-forholdene faktisk er i dag, dels resultere i løsningsmodeller, der begrænser Danmarks it-relaterede sårbarhed mest muligt. Undersøgelsen forudsætter videnindsamling, et indgående analysearbejde og en prioriteret forskningsindsats inden for de forskellige sektorer.**
- **I arbejdet med at afdække it-infrastrukturens sårbarhed bør Danmark være opmærksom på udenlandske erfaringer. Holland er et af de lande, som har været en lignende proces igennem, hvorfor det vil være fornuftigt blandt andet at trække på erfaringerne herfra.**
- **Som resultat af den danske undersøgelse bør der iværksættes initiativer, som skaber opmærksomhed og viden i samfundet om it-sårbarhed og it-sikkerhed. Arbejdsgruppen lægger her særlig vægt på, at der bliver skabt opmærksomhed om *den menneskelige faktors* afgørende betydning i den forbindelse.**
- **Arbejdsgruppen finder det endvidere vigtigt, at der bliver skabt en fundamental viden i samfundet om it-sikkerhed og it-sårbarhed. Dette bør blandt andet ske ved at sikre, at der bliver sat større fokus på disse emner i regi af såvel grunduddannelserne som de videregående uddannelser.**
- **Med henblik på fremover at opnå en situation med størst mulig it-sikkerhed overalt i samfundet, anbefaler arbejdsgruppen endelig, at der i forlængelse af undersøgelsen opstilles forskellige it-sikkerhedsmæssige krav til forskellige sektorer alt efter hvor betydningsfulde for samfundet de er.**

Kilder til yderligere information

- Notat om it-infrastrukturens sårbarhed (Teknologirådet) – www.tekno.dk/pdf/projekter/p03_it_infrastruktur_rapport.pdf.
- Rådet for it-sikkerhed. www.videnskabsministeriet.dk.
- IT- og Telestyrelsen. www.ITst.dk.
- Information om projektet "Statsligt it- og beredskab" på Offentlig Information Online. www.oio.dk/itsikkerhed/saarbarhedsanalyse.
- Teknologidebat nr. 4/2003 – tema om "sårbarhed i cyberspace". Kan bestilles hos Teknologirådet. www.tekno.dk.
- DK-CERT. www.cert.dk.
- It-sikkerhedsrådets udredning om Internet sårbarhed. www.videnskabsministeriet.dk.
- Hvidbog om it-arkitektur, juni 2003. www.oio.dk.
- Kommissorium for udvalget vedrørende el, naturgas, teleforsyning samt it-forhold (den nationale sårbarhedsudredning). www.ITst.dk.
- Den Digitale Taskforce. http://e.gov.dk.
- Beretning om revision af statsregnskabet for 2002 (omhandler bl.a. IT-sikkerhedsproblemer i staten). www.rigsrevisionen.dk.
- Critical Infrastructure Protection in the Nederlands: A Quick Scan. Af Eric Luiijf m.fl. http://www.tno.nl/instIT/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf
- TNO (Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek), Holland. www.tno.nl/homepage.html.
- Introduktion til det hollandske "Infodrome" projekt. www.infodrome.nl/english.

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

ISSN: 1602-4311

- Om det hollandske "KWINT" projekt (på hollandsk). www.kwint.org.
- Den svenske sårbarheds- og sikkerheds-udredning del 1. og 2. http://forsvar.regeringen.se.
- Den norske rapport "Samfunnssikkerhet – Veien til et mindre sårbart samfunn." http://odin.dep.no.
- OCTAVE-modellen. Udviklet ved Software Engineering Institute, Carnegie Mellon University. www.sei.cmu.edu.

Den eksterne arbejdsgruppe bag Teknologirådets projekt

- Freddie Drewsen, leder af Kommunikations- og Informationssektionen (CIS), Forsvarets Forskningstjeneste. fd@ddre.dk. Tlf. 39 15 17 95.
- Preben Andersen, chefkonsulent i UNI-C og leder af DK-CERT. preben.andersen@uni-c.dk. Tlf. 35 87 88 87.
- Knud Mose, TDC. knmo@tdc.dk.
- Peter Christensen, Catpipe Systems. pc@catpipe.net.
- Sten Christophersen, Hovedstadens Sygehusfællesskab. sc@hsd.hosp.dk.

Fra rådet til tinget udgives af Teknologirådets sekretariat. Redaktør Ida Leisner.
Dette nummer er skrevet af freelancejournalist Jakob Vedelsby.

De sidste fem numre Fra rådet til tinget er:
189: Hold hus med elforbruget
188: Drop ja eller nej til GMO
187: Dansk energi-vision efterlyses
186: IT-privacy skal forbedres
185: Mens vi venter på ulykken