Fra rådet til tinget
TEKNOLOGIRÅDETS NYHEDSBREV TIL FOLKETINGET

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

Nr. 234 | januar 2007

It-kriminalitet overskrider grænser

International lovgivning skal styrke mindre virksomheders it-sikkerhed

It-kriminalitet er i voldsom og ukontrollabel vækst. Men på internationalt plan agerer politikere, politi, producenter og forhandlere af soft- og hardware og apparater med it-indhold generelt som om, der er helt styr på it-sikkerheden.
Hvis sikkerhedsniveauet for alvor skal forbedres, er der behov for international lovgivning og internationale mærkningsordninger. Og Danmark bør gå foran, mener en arbejdsgruppe under Teknologirådet.
Sårbarheder i soft- og hardware er det alvorligste it-sikkerhedsproblem anno 2006. Her er der brug for en international model som sørger for, at alle brugere straks får opdateret deres sikkerhed, når sikkerhedshuller bliver opdaget. Benchmarking, mærkningsordninger og digitale identiteter til alle borgere er andre forslag fra arbejdsgruppen.

Dette nyhedsbrev tager afsæt i Teknologirådsprojektet "It-sikkerhed på tværs af grænser". Projektet har resulteret i en rapport med samme titel, der udkom den 25. januar 2007. Rapporten kan downloades aratis fra www.tekno.dk.

Hvis vi i Danmark skal udnytte vores globale, digitalt baserede handelspotentiale fuldt ud, skal kommunikationsvejene være sikre. Det indebærer, at borgere og virksomheder skal beskyttes – og beskytte sig – bedst muligt mod den stadig mere udbredte it-kriminalitet. Danmark er dog ikke i stand til alene at nedkæmpe og forebygge den it-kriminalitet, der rammer os, da den typisk er grænseoverskridende og på grund af den globale forbundenhed via it-netværk involverer flere lande på én gang. Omfanget af handel, kommunikation og udveksling af personlige oplysninger via nettet vokser dag for dag – og flere og flere produkter er tilsluttet internettet. Den stigende sammenkobling øger risikoen for sårbarhed i soft- og hardware. Disse og andre it-relaterede sikkerhedsproblemer kan ikke løses nationalt, men nødvendiggøre europæisk og globalt samarbejde.
Specifikt for Danmark er større it-sikkerhed simpelthen en forudsætning for, at vi kan realisere målene i regeringens globaliseringsstrategi, om at fastholde og udbygge vores position som et førende innovativt videns- og iværksættersamfund.

It-kriminalitet løber løbsk

Blandt analyseinstitutter og politimyndigheder verden over er der udbredt enighed om, at problemerne med it-kriminalitet er et hastigt voksende globalt problem. Det er imidlertid ikke det indtryk, man får ved at iagttage den nuværende danske og internationale indsats til forebyggelse og bekæmpelse. Politikere, politi, producenter og forhandlere af it-udstyr og apparater med it-indhold m.fl. agerer generelt som om problemerne er under kontrol. Den såkaldte IP-ficering af samfundet, som betyder, at it indgår i stadig flere produkter og er nervetråde i det globalt forankrede digitale servicesamfund, har gjort os mere og mere sårbare over for it-kriminalitet. Det bekræfter en undersøgelse foretaget af bl.a. FBI (2006), som viser, at 60 pct. af USA's virksomheder anser it-kriminalitet for at koste dem flere penge end fysisk kriminalitet. The Computer Economics

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

Malware Report (2006) afdækker, at malware som computervirus, orme og spyware på globalt plan kostede virksomheder 85 mia. kr. i 2005. En international undersøgelse (Eurostat, 2006) hævder, at 24 pct. af alle danske virksomheder og 35 pct. af danske borgere har været udsat for et virusangreb i 2005. Og Danmark mærker også konsekvenserne af utilstrækkelig it-sikkerhed på andre felter: Hvidvaskning af penge via internettet, organiserede indbrud på betalingsterminaler, destruktion af webbutikker via "botnet" og identitetstyveri ved hjælp af "phishing" er blot nogle af de seneste eksempler.

Hvad er "phishing" og "botnet"?
Begrebet "phishing" er dannet af ordene "fishing" og "phony" (falsk) og betyder at aflure personlige identiteter/adgangskoder fx via email med falske afsendere, "smarte" softwareprodukter eller falske "look a like-hjemmesider". En mulig konsekvens af phishing er, at en virksomhed ikke kan eller tør sende email til deres kunder – og at kunderne mister tilliden til virksomhedens internettjenester. "Botnet" er et andet eksempel på it-kriminalitet, som indebærer store økonomiske gevinstmuligheder for it-forbrydere, der ved at true med angreb kan pengeafpresse webbutikker og lignende. Et botnet består af et netværk af ofte tusindvis af pc'er, der uden deres ejeres viden bliver brugt til at udsende fx spam og phishing mail.

Den skadelige orm fra udlandet

I forbindelse med udarbejdelsen af dette nyhedsbrev har det vist sig yderst vanskeligt at overtale virksomheder til at tale om deres it-sikkerhed – og i særdeleshed deres problemer med samme.

It-sikkerhedsfirmaet, Neupart A/S, har accepterede at deltage. Adm. direktør Lars Neupart, der også er medlem af Teknologirådets ekspertarbejdsgruppe i projektet "It-sikkerhed på tværs af grænser", er ikke bange for at fortælle, at hans virksomhed i enkelte tilfælde har haft ubudne it-gæster. For ingen kan beskytte sig 100 pct. mod it-kriminalitet. Det ville i givet fald kræve så store ressourcer og indebære så massive foranstaltninger, at man ikke kunne drive forretning. Men man kan gøre utrolig meget både fra samfundets side og internt i virksomheden, pointerer han.

En langsomt fungerende hjemmeside tilbage i 2004 indikerede, at noget var galt. Ved at analysere aktiviteterne på webserveren fandt man ud af, at trafikken fra og med et ganske bestemt tidspunkt var øget markant. Det viste sig, at serveren var blevet inficeret med en computerorm af udenlandsk oprindelse (en orm er et skadeligt program på linie med virus og spyware) og at ormen straks var gået i gang med at bruge webserveren som platform for nye angreb.
Men hvordan kunne ormen trænge gennem virksomhedens beskyttelsesforanstaltninger? Forklaringen var, at man ikke havde opdateret en softwarekomponent med den seneste sikkerhedsrettelse. Den ansvarlige medarbejder var holdt op en måned tidligere og der var ikke sket en overdragelse af ansvaret for denne softwarekomponent.

"Man kan sige, at hullet i vores overdragelsesrutine skabte et sikkerhedshul, som blev udnyttet af en it-kriminel. Heldigvis opdagede vi relativt hurtigt computerormen, fik stoppet dens it-forurening og undgik alvorligere konsekvenser som nedbrud af vores webserver, hvilket ville have været problematisk, da en stor del af vores kundekontakt foregår via hjemmesiden. Man kan også sige, at vi var heldige, at skaberen af ormen ikke havde gjort den endnu mere destruktiv," fremhæver Lars Neupart.

Eksemplet viser, at der kan ske sikkerhedsbrister selv i virksomheder med maksimal opmærksomhed på it-sikkerhed, hvilket mere end antyder, at andre virksomheder og private brugere er ringe stillet. Problemet er, at det er vanskeligt at beskytte sig mod fx sikkerhedshuller i software. It-industrien er international og software er typisk udviklet i udlandet – og man kan af bl.a. konkurrencehensyn ikke stille særlige nationale sikkerhedskrav. Derfor kræver det internationale løsninger, hvis sikkerhedsniveauet skal løftes for alvor.

"It-kriminalitet er i dén grad globalt funderet og der er brug for internationale initiativer, hvis vi skal nedbringe risikoen for at blive ramt. I tilfældet med vores computerorm ville tvungen autoopdatering af software have forhindret angrebet, der inden for kort tid ramte utallige andre virksomheder verden over, som ikke havde gennemført sikkerhedsrettelsen," siger Lars Neupart.

Han er medlem af Dansk Industris It-sikkerhedsudvalg og har herigennem erfaret, at små og mellemstore virksomheder gennemsnitligt klare sig dårligere end de store på it-sikkerhedsfronten. Hvis disse virksomheder fik bedre styr it-sikkerheden, ville Danmarks samlede it-infrastruktur blive mindre sårbar – og det kan netop blive resultatet af en international indsats.

"Der er ingen tvivl om, at de internationale initiativer, vi foreslår i rapporten, vil kunne afhjælpe en lang række af de it-sikkerhedsproblemer, som mange små og mellemstore virksomheder og private brugere døjer med i dag," siger Lars Neupart.

It-sikkerhed - et politisk spørgsmål

Han undrer sig ikke over, at det politiske system i Danmark og internationalt generelt ikke udviser den store interesse for it-sikkerhed.

"Det er en udbredt opfattelse og misforståelse, at it-sikkerhed udelukkende handler om teknik – og at problemerne derfor skal løses af teknikere. Samtidig er det nok et resultat af, at udviklingen er gået hæsblæsende hurtigt. Graden af samfundets it-afhængighed er eksploderet på ganske få år, og det har øget behovet for it-sikkerhed tilsvarende. Jeg er ikke tilhænger af skingre råb om at "ulven kom-

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

mer", men der er ingen tvivl om, at tiden nu er inde til, at politikerne vågner op til dåd på det her område. Hvis danske virksomheder ikke er i stand til at anvende it effektivt og sikkert, kan det påvirke vores konkurrenceevne negativt og dermed velfærdssamfundets overlevelsesevne. Vi er nødt til at sætte ind med en kombination af effektfulde nationale og internationale initiativer, som kan forebygge og bekæmpe it-kriminalitet. Og Danmark er vidensmæssigt rustet til at tage teten og høste den forretningsmæssige "first mover" effekt," siger han.

Lars Neupart fremhæver ligeledes en række pointer, der også er omtalt i arbejdsgruppens rapport og således afspejler holdning i Teknologirådets arbejdsgruppe: For det første behovet for øget forskning og statistik på it-sikkerhedsområdet – som afsæt for at opnå større indsigt i problemerne med it-kriminalitet. Mængden af videnskabelige undersøgelser og offentligt tilgængeligt statistisk materiale om it-kriminalitet er i dag stærkt begrænset, ligesom konkrete initiativer til forebyggelse og bekæmpelse af it-kriminalitet er præget af manglende ressourcer og fokus.

"Der er akut behov for forskning, som kan synliggøre omkostningerne ved ikke at prioritere it-sikkerhed. Samtidig skal vi opbygge et nuanceret statistisk grundlag for initiativer på it-sikkerhedsområdet. For at kunne måle effektiviteten af initiativerne, vil det også være en god idé at benchmarke enkeltlande og regioner i forhold til deres it-sikkerhedsniveau," siger han.

It-sikkerhedsproblemer – og løsninger

Teknologirådets arbejdsgruppe fremhæver, at tiden er inde til konkrete, målrettede skridt i form af international lovgivning og internationale certificerings- og mærkningsordninger. Det har været målet med projektet at præsentere internationalt orienterede, praktisk realiserbare løsningsforslag på de grænseoverskridende it-sikkerhedsmæssige problemområder, gruppen anser for at være de vigtigste netop nu og i de kommende år. Nedenstående løsninger skal igangsættes hurtigst muligt og simultant på de nævnte problemområder, mener arbejdsgruppen. Se venligst rapporten for samtlige problemområder og uddybning af såvel problemer som løsninger.

Sårbarheder i soft- og hardware er det alvorligste it-sikkerhedsproblem anno 2006.

- Udvikling af en international model, som sikrer, at sikkerhedsopdateringer i software bliver installeret hos brugerne straks efter et sikkerhedshul er opdaget.
- EU-lovkrav om, at forhandlere af elektronisk, netværksbaseret udstyr som computere, telefoner, MP3-afspillere, tyverialarmer m.v. leverer produkter med den nyeste sikkerhedsopdatering.
- EU indfører en "whitelist"-ordning for soft- og hardware. Den offentlige sektor går foran og benytter kun whitelistede it-produkter.
- Certificeringsordning for Internet Service Providere (ISP'er) i EU, der pålægges at leve op til en adfærdskodeks.

Forbrugerne kan ikke skelne mellem sikre og usikre it-produkter og -services.

- Udvikling af et EU-koncept for mærkning af internetforbundne produkter. Der benyttes mærkning som i bilverdenens "crashtest-ordning".

Begrænset international politiindsats og retsforfølgelse på it-kriminalitetsområdet.

- Anerkendelse af it-kriminalitet som et nyt politispeciale, udnævnelse af mindst én it-kriminalitetsansvarlig i hver af de nye politikredse og etablering af en central myndighed, der kan håndtere komplekse sager om it-kriminalitet professionelt – nationalt og internationalt.
- Politimæssig kompetenceoprustning hele vejen rundt – fra uddannelse af specialister på de enkelte it-kriminalitetsområder til kompetenceudvikling af anklagemyndighed og dommere.
- Videreudvikling af internationale samarbejdsaftaler, som skal sikre en mere effektiv håndtering af grænseoverskridende it-kriminalitet.

Mangel på sikker identifikation, hvilket hæmmer et frit informationsflow i EU.

- Danmark etablerer en langsigtet strategi om at videreudvikle den nuværende digitale signatur til et "borgerservicepas" i form af en "digital identitet". Målet på længere sigt er, at hver borger i EU har en sådan interoperabel, digital identitet, der kan øge integrationen og minimere risikoen for misbrug af personlige oplysninger.

Arbejdsgruppen bag projektet

Teknologirådets arbejdsgruppe i projektet "It-sikkerhed på tværs af grænser", ledet af projektleder Bjørn Bedsted, bestod af:

- Preben Andersen, chefkonsulent i Uni-C, leder af DK-CERT.
- Brian Birkvald, Security Principal & Manager i IBM's Security Group.
- Lars Neupart, adm. direktør for Neupart A/S.
- Morten Storm Petersen, adm. direktør for Signaturgruppen A/S.
- Carsten Stenstrøm, Teknologisikkerhedschef i Danmarks Radio.

- Christian Wernberg-Tougaard, Director i Unisys, medlem af ENISA's rådgivende ekspertudvalg om "Awareness Raising".

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

De sidste 5 numre af Fra rådet til tinget er:
Nr. 233: Biobrændstoffer til transport
Nr. 232: Gratis offentlig transport
Nr. 231: Ønskes: En ny privacy-politik
Nr. 230: Uddannelse til globalt marked
Nr. 229: Bedre sundhed hvis færre røg

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