

Nr. 183 | marts 2003

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

## Dårlig sikkerhed til hjemme-pc'en

**Private Internet-brugere må selv beskytte sig mod vira og hackere fra cyberspace**

**Forbrugeren er sin egen IT-chef**

> På trods af, at private Internetbrugere oplever flere og alvorligere problemer med computervira og hackere, er Internetudbydere ikke underlagt lovkrav om, at de skal oplyse deres kunder om, eller beskytte kunderne mod, virusangreb eller hackere.

**Internetudbydere tøver**

> Internetudbydere servicere deres virksomhedskunder med central virus- og hackerbeskyttelse, men langt de fleste tøver med at tilbyde privatkunderne en tilsvarende service.

**Der skal stilles krav til udbydere**

> Danske IT-sikkerhedseksperter mener, at Internetudbydere nu bør tage et medansvar for privatkundernes sikkerhed på Internettet, men de finder det ikke formålstjenligt at lovgive på området.

*Dette nyhedsbrev ser på IT-sikkerhed fra den private Internetbrugers synsvinkel. Teknologirådet har igangsat et projekt om "IT-infrastrukturens sårbarhed", som behandler sikkerhed generelt.*

Private virksomheder og offentlige systemer er dybt afhængige af, at IT og elektroniske netværk fungerer. Sikkerheden i den elektroniske kommunikation er alfa og omega for aktiviteterne på stadig flere samfundsområder. Men også borgernes IT-sikkerhed får stadig større betydning i takt med eksplosionen i antallet af private, der er koblet op til Internettet og benytter elektronisk kommunikation. Regeringen har en vision om at indføre "digital forvaltning" i den offentlige sektor. Målet er at forbedre den offentlige service ved at tilbyde borgerne øget selvbetjening og udveksling af informationer via Internettet. En af forudsætningerne for at dette kan realiseres er, at borgerne har tillid til, at den elektroniske kommunikation med det offentlige kan ske på betryggende vis. Og at der generelt i samfundet er tryghed og tillid om brugen af IT og elektronisk kommunikation. Dette er imidlertid ikke situationen i dag.

### Virusproblemerne vokser

Problemerne med computervira og hacking vokser i takt med, at flere mennesker tilslutter sig Internet, og i takt med, at de altid "åbne" bredbåndskoblinger til Internettet vinder udbredelse. Sidst-

nævnte sker ikke mindst som følge af hjemme-pc-ordningen, der gør det muligt for en virksomhed at stille en skattefri bredbåndsforsikring til rådighed for sine ansatte.

Siden Internettet for alvor slog igennem på privatmarkedet herhjemme i 1997, er der observeret ca. 60.000 forskellige vira af den traditionelle slags, som typisk er vedhæftet en email og spredt sig via computernes adresselister. I de seneste år er der fremkommet nye, langt mere avancerede og skadevoldende vira – de såkaldte "orme", der ligeledes er vedhæftet en email. Et eksempel er den såkaldte "I love you"-orm, der i 2001 ramte ca. 50.000 danske virksomheder og et ukendt antal private Internetbrugere.

Computervira og hackere er den første store, erkendte ulempe ved Internettet – en ulempe, som man har god mulighed for at gardere sig imod, når det gælder de traditionelle vira. Derimod er der eksempler på, at de mere udspekulerede ormevira, på trods af virusbeskyttelse, trænger ind i computere med omfattende ødelæggelser til følge. En ormevirus har den effekt, at den tager magten over modtagerens computer og fx sletter hele eller dele af harddisken. Samtidig vil ormen typisk åbne en bagdør til

computeren, så hackere uhindret kan trænge ind og fx bruge computeren som platform for yderligere kriminelle aktiviteter.

Ifølge danske IT-eksperter bliver disse ormevira stadig mere ondsindede og ødelæggende – og vurderingen er, at problemet vil fortsætte med at vokse i de kommende år.

## Hver tredje udsat for computervirus

3 millioner danskere har i dag adgang til Internet. Nye tal viser, at 30% af de private brugere har haft virusangreb. Tallene stammer fra en undersøgelse Danmarks Statistik har foretaget for Ministeriet for Videnskab, Teknologi og Udvikling. Af undersøgelsen fremgår også, at 74% af de private brugere har installeret antivirusprogrammer, mens 27% har installeret firewall. Mange af dem, der ikke benytter en sikkerheds-løsning, begrundet det med, at det er for svært at installere eller at de ikke forstår vejledningen. Undersøgelsen er offentliggjort af Rådet for IT-sikkerhed:

[http://www.videnskabsministeriet.dk/cgi-bin/doc-show.cgi?doc\\_id=154020&doc\\_type=35&leftmenu=2&topbar=none&topmenu=0](http://www.videnskabsministeriet.dk/cgi-bin/doc-show.cgi?doc_id=154020&doc_type=35&leftmenu=2&topbar=none&topmenu=0)

Danmarks Statistiks virksomhedstal fra januar 2003 viser, at 43 procent af danske virksomheder har været udsat for virusangreb i 2002. De sidste tre år har virusangreb kostet danske virksomheder 4 milliarder kr.

## Sin egen IT-chef

Myndighederne herhjemme anbefaler, at såvel virksomheder som private Internetbrugere garderer sig mod vira ved hjælp af antivirusprogrammer. De fleste mellemstore og store virksomheder har etableret en IT-afdeling, som bl.a. har til opgave at forhindre, at vira og hackere trænger ind i virksomhedens systemer. Når det gælder private Internetbrugere, er situationen i dag den, at man må være sin egen IT-chef og sørge for at anskaffe, installere og ikke mindst opdatere antivirussoftware og en firewall. En ny undersøgelse viser, at tre fjerdedele private brugere har installeret antivirus programmer. Kun meget få udbydere af Internetforbindelser herhjemme og i udlandet tilbyder i dag kunderne central beskyttelse mod hackere samt de vira, som kan overføres via de email, der kanaliseres til forbrugeren via udbydernes mailserver.

## Udbyderne bør tage et ansvar

Danish Computer Emergency Response Team (DK-CERT) overvåger sikkerheden på det danske forskningsnet, som leverer højhastighedsforbindelser til forskningsverdenen, og på sektornettet, som 2.800 danske uddannelsesinstitutioner bruger. I DK-CERT erkender man, at det kan synes absurd, at hver eneste private Internetbruger verden over skal investere i egen software til beskyttelse mod truslerne fra

cyberspace. DK-CERT mener, at tiden er inde til at Internetudbyderne påtager sig opgaven med at sikre kunderne virusfri email. Ifølge DK-CERT er der i dag ikke noget som rent teknologisk forhindrer Internetudbyderne i at tilbyde denne service.

Dog understreger man i DK-CERT, at udviklingen inden for vira er uforudsigelig, og at et antivirus-system derfor aldrig kan være 100 procent sikkert – også selv om det opdateres dagligt. Derfor er det urealistisk at forestille sig, at udbyderne på nuværende tidspunkt kan give en ansvarspådragende garanti for, at email ikke indeholder vira. Eller en garanti for, at udbyderens virusprogrammer ikke bremser email, som ikke indeholder virus. På den baggrund mener man i DK-CERT ikke, at udbyderne via lovkraft kan tvinges til at virusbeskytte brugerne. Det skal ske ad frivillighedens vej, så virusbeskyttelse bliver et konkurrenceparameter udbyderne imellem.

Der findes i dag ingen lovgivning, som forpligter Internetudbydere til at oplyse om eller beskytte deres kunder mod virus eller hacking. I Ministeriet for Videnskab, Teknologi og Udvikling (MVTU) mener man på linie med DK-CERT ikke, at Internetudbydere ved lov skal pålægges at virusbeskytte kunderne. Fra ministeriets side lyder dog en opfordring til udbyderne om at etablere en tæt dialog med brugerne om sikkerhedsspørgsmål.

Det er klart i udbydernes egen interesse og det bør hellere ske i dag end i morgen, hedder det fra ministeriet, hvor man understreger, at ansvaret for borgernes IT-sikkerhed ideelt set skal løftes af udbydere, butikker som sælger pc'er og brugerne i fællesskab. Tal fra Danmarks Statistik, efteråret 2002, viser, at 80 procent ikke blev vejledt om IT-sikkerhed, da de købte deres pc.

Et konstruktivt og gensidigt samarbejde for at højne IT-sikkerheden er helt centralt for at samfundet samlet set kan få et højere sikkerhedsniveau. Hvis ikke alle interessenter medvirker til at gøre anvendelsen af elektronisk kommunikation tillidsvækkende og trygt, så stimulerer det en udvikling som alle vil tabe ved, fastslår man i MVTU.

## Antivirus er "big business"

Kombineret antivirussoftware og firewall til beskyttelse af hjemmecomputeren mod virus og indtrængen af hackere kan i dag erhverves for mellem 400 til 600 kr. Beløbet inkluderer typisk en daglig eller ugentlig online opdatering, som giver beskyttelse mod de nyeste vira. På trods af, at der også findes flere gratis antivirusprogrammer og firewalls, som kan downloades via Internettet, er antivirus/firewall blevet big business. På verdensplan kæmper ca. 15 store leverandører om adgangen til millioner af virksomheders og private Internetbrugeres pengepunge.

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

## **Lovgivningen er klar: Hacking og virus-spredning er strafbart**

Straffeloven §263, stk.2 omtales ofte som "hacker-paragraffen". Heraf fremgår det bl.a., at paragraffen "giver hjemmel til at straffe den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling. Denne bestemmelse kan anvendes såvel ved målrettet indtrængen i IT-systemer, som ved ulovlig aflytning af den kommunikation, der sker via hjemmesider, og strafferammen er bøde eller fængsel indtil 6 måneder."

Spredning af computervirus er strafbart efter straffelovens §291 – den såkaldte "hærværksparagraf". Her fremgår det, at "den, som ødelægger, beskadiger eller bortskaffer ting der tilhører en anden, straffes med bøde eller hæfte eller med fængsel indtil 1 år."

I maj 2002 foreslog EU-kommissionen indførelse af nye fællesregler for cyberkriminalitet.

Ifølge forslaget skal spredning af vira og hacking fremover koste op til fire års fængsel. Forslaget, der er fremlagt som en del af det politimæssige samarbejde mellem EU-landene, Danmark også deltager i, behandles p.t. i de enkelte medlemslande.

## **De fleste Internetudbydere tøver**

En rundspørge, som Teknologirådet har foretaget til en række af de største Internetudbydere på det danske marked, viser, at udbydere generelt tøver med at tilbyde privatkunderne central beskyttelse mod hackere og vira. Når det gælder virksomhedskunderne er situationen derimod den, at udbydere tilbyder central beskyttelse – og at mange virksomheder gør brug af denne service. Udbydere overvejer jævnligt at tilbyde private Internetbrugere en tilsvarende service, men de vurderer, at omkostningerne aktuelt er højere end de private brugere er villige til at betale. Flere af udbydere forventer dog, at brugerens interesse for at betale sig fra beskyttelse vil vokse i de kommende år. Sikkerhedsaspektet vil blive et konkurrenceparameter udbydere imellem og på et tidspunkt vil denne service formentlig indgå som en integreret del af ethvert Internetabonnement.

En af udbydere i Teknologirådets rundspørge tilbyder allerede i dag via sin hjemmeside at brugeren kan tilmelde sig en centralt styret virusskanning samt en central firewall, som man kan benytte på tre forskellige sikkerhedsniveauer. Omkring en fjerdedel af dial-up kunderne (modem- eller ISDN-forbindelser) benytter denne service, som på nuværende tidspunkt er gratis. Udbyderens private ADSL-kunder tilbydes en lignende service for en merpris på abonnementet. 10 procent af den pågældende udbyders private ADSL-kunder er i øjeblikket villige til at betale denne merpris.

## **Individuel beskyttelse er altid et must**

I DK-CERT påpeger man, at den private forbruger – uanset om forbrugers Internetudbyder vælger at indføre central virusbeskyttelse – alligevel skal sikre sig individuelt mod vira og hacking. Det skyldes bl.a., at vira kan nå den private forbrugers computer ad andre veje end via udbyderen – fx gennem brug af webmail-tjenester som fx "Hotmail" eller ved installation af materiale fra diskette eller CD-rom. Samtidig er det i dag reelt ikke muligt for en Internetudbyder at oprette en central firewall, som beskytter kunderne mod indtrængen af hackere, mener man i DK-CERT. Teknologien er godt nok til stede – og denne service tilbydes virksomhedskunder – men problemet er, at privatkundernes ønsker til, hvad de skal kunne få adgang til og downloade fra Internettet, er meget forskellig. En mulighed er det dog at graduere sikkerheden og åbne for, at privatkunderne kan tilmelde sig flere sikkerhedsniveauer, hvad en enkelt udbyder på det danske marked da også i dag tilbyder. En sådan sikkerhedsmæssigt graderet, central firewall vil dog langt fra imødekomme alle private Internetbrugeres ønsker om at kunne bevæge sig frit på Internettet.

I dag kan den private bruger, ifølge DK-CERT, kun beskytte sig optimalt mod vira og uvedkommende indtrængen ved også at benytte eget antivirusprogram og en firewall. Erfaringerne viser imidlertid, at de private danske Internetbrugere har været – og til dels stadig er – relativt langsomme til at indse, at virusbeskyttelse og brug af firewall er en nødvendighed i dag. I DK-CERT vurderer man, at "mange og stadig flere" private Internetbrugere anvender virusbeskyttelse, mens "kun få" har installeret en firewall. Sidstnævnte betyder reelt, at et uvist antal private danske computere er ubeskyttede og dermed åbne for hackere.

I DK-CERT fastslår man, at de private computeres "åbenhed" i stigende omfang bliver udnyttet af personer, som trænger ind på og anvender computerne som platforme for nye ulovligheder – fx såkaldte portscanninger, hvor hackeren afslører andre computere, som er sårbare overfor indtrængen. Ved at operere med afsæt i en fremmed computer – eller et netværk af sådanne – kan hackeren sløre sin egen identitet ved forsøg på indtrængen i fx virksomheders IT-systemer. Hackerer vil således ikke efterlade sin egen IP-adresse (alle Internetbrugere registreres og kan spores via deres "virtuelle fingeraftryk" – eller Internet Protocol adresse), men den computers IP-adresse, hvorfra ulovlighederne udøves.

Udover at hackere anvender private computere som platforme, har hackeren adgang til alt, hvad der befinder sig på den enkelte computers harddisk – alle data, informationer, passwords osv. Afhængig af harddiskens faktiske indhold, kan adgangen misbruges på forskellig vis – fx til opsamling af kreditkortnumre, opkald fra computeren til dyre cybersexnumre og hærværk på harddisken. Ifølge DK-CERT vil enhver Internetbruger, der har installeret

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

en firewall på sin private computer, erfare, at problemet er særdeles udbredt: En firewall vil hyppigt registrere portscanninger og afværge uautoriseret indtrængen.

## Digital signatur

Digital signatur er populært sagt en elektronisk underskrift til brug til sikker kommunikation på Internettet – fx ved udveksling af informationer mellem offentlige myndigheder (såsom Told og Skat) og borgere eller virksomheder. Den digitale signatur består af en "offentlig nøgle" og en "privat nøgle", som begge er beskyttet med passwords.

Det er tanken, at den digitale signatur skal erstatte papirgange og øge borgernes selvbetjening i en fuldt digitaliseret offentlig sektor. Samtidig forventer man, at signaturen vil fremme en effektiv og målrettet IT-anvendelse i private virksomheder, herunder at signaturen vil øge sikkerheden ved og dermed brugen af e-handel.

## Rådgivning til borgerne om sikkerhed

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 Rådet for IT-sikkerhed under MVTU, der begyndte sit arbejde i januar 2003, det for 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.

Modsat det tidligere IT-sikkerhedsråd, der ophørte i 2002, får det nye råd adgang til at udføre konkrete opgaver såsom igangsættelse af kampagner og rådgivning af MVTU i forhold til normer og standarder for IT-sikkerhed.

Regeringen har på Finansloven for 2003 afsat 50 mio. kr. til udbredelse af den digitale signatur til borgere, myndigheder og private virksomheder. Signaturen stilles gratis til rådighed for alle.

I DK-CERT forventer man, at udbredelsen i samfundet vil ske meget hurtigt i løbet af de kommende år. Sikkerhedseksperter i DK-CERT vurderer, at signaturen 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.

## Kilder

- ❖ Preben Andersen, chefkonsulent i Uni-C og leder af DK-CERT.
- ❖ Yih-Jeou Wang, kontorchef i Ministeriet for Videnskab, Teknologi og Udvikling.
- ❖ Danish Computer Emergency Response Team (DK-CERT) – [www.cert.dk](http://www.cert.dk).
- ❖ Ministeriet for Videnskab, Teknologi og Udvikling – [www.vtu.dk](http://www.vtu.dk).
- ❖ Rådet for IT-sikkerhed – [www.vtu.dk](http://www.vtu.dk).
- ❖ Uni-C – [www.uni-c.dk](http://www.uni-c.dk).
- ❖ Internetudbydere på det danske marked: TDC, Uni2, Get2Net, Cybercity.

*Fra Rådet til tinget udgives af Teknologirådets sekretariat.*

*Dette nummer er skrevet af freelancejournalist Jakob Vedelsby, research Bjørn Bedsted.*

*De sidste fem numre Fra rådet til tinget er:*

*182: EPJ også patientens værktøj*

*181: Effektiv overvågning af havmiljøet*

*180: Pensionsalderen til debat*

*179: Europa håber på Open Source*

*178: Kvælstof og landbruget*

*Udgivet marts 2003*

*ISSN: 1600-2105*

## Udgiver

Teknologirådet  
Antonigade 4  
DK - 1106 København K  
Tel. 33 32 05 03  
[rtt@tekno.dk](mailto:rtt@tekno.dk)

## Abonnement

Gratis pr. email  
Tilmelding på:  
[rtt@tekno.dk](mailto:rtt@tekno.dk)  
Tidligere nyhedsbrev findes på:  
[www.tekno.dk/rtt.htm](http://www.tekno.dk/rtt.htm)

ISSN: 1602-4311