IT-sikkerhed

Computervirus
Hacking
Spyware
Back-up
Lovgivning
og meget andet

www.noah2900.dk

Indholdsfortegnelse

Indledning

Emnet "**IT-sikkerhed**" omhandler mange forskellige forhold:

- Virus og antivirus
- Hacking, trojanske heste og firewall
- Spyware, overvågning og kryptering
- Økonomisk kriminalitet, frihedskæmpere og drengestreger
- Adgangskontrol og passwords
- Back-up (sikkerhedskopi) af data

IT-sikkerheden er i dag den største udfordring i udviklingen og brugen af informationsteknologi. Det moderne samfund og de private IT-brugere er utrolig sårbare overfor truslerne især fra Internettet, som stort set binder alle computere sammen. En stor del af den "almindelige" kriminalitet er nu flyttet ud på Internet, og i USA mener man faktisk, at omsætningen indenfor denne slags kriminalitet overstiger narkokriminaliteten nu ...

Alle har vel ting liggende på deres **private** computer, som de meget nødigt vil miste: digitalbilleder, skoleopgaver, private oplysninger (budgetter, minder, sange, taler, breve o.lign.), informationer vedr. netbank o.s.v. Og man kan meget let få følelsen af, at ens private grænser bliver overtrådt, hvis "fremmede" pludselig er inde og rode ved ens sager ... Desuden kan din private computer **misbruges** til kriminelle formål.

Samfundet og virksomhederne er også sårbare både i forhold til vigtige informationer og penge:

- Det kan f.eks. have alvorlige konsekvenser for patienterne, hvis journal-systemet på et stort hospital bliver angrebet af virus og sat ud af spil
- En virksomhed kan lide både økonomiske tab og få et dårligt image, hvis deres IT-systemer bliver angrebet: hackere laver sabotage mod deres hjemmeside og foretager pengeafpresning, informationer om kunder bliver afsløret og misbrugt, andre virksomheder udøver "industri-spionage" o.s.v.

Det er nødvendigt at sikre sig bedst muligt mod disse trusler – idet vi i alle dele af samfundet er blevet så "afhængige" af computere og netværk !

:-) Søren Noah, febr. 2006 (www.noah2900.dk)

Computervirus

Udtrykket ”computervirus” (eller ”malware”) bruges i dag bredt om alt muligt, som er skadeligt eller irriterende for vores computere, vores arbejde og vores privatliv, men den **oprindelige definition** på en computervirus er:

- et lille program som gemmer sig i et andet program (værtsprogrammet)
- når værtsprogrammet installeres og derefter benyttes, så installeres virussen også – og så kan den foretage sig de ting, som den er programmeret til at gøre

Den ”**gammeldags virus**” er altså afhængig af et andet program, som man selv skal vælge at benytte, før virussen kan smitte computeren !! Sådan er det ikke med de forskellige trusler, som vi ser i dag.

Den første computervirus dukkede op i starten af 1980’erne, kom rigtigt i omløb i 1986 og i 1988 dukkede det første antivirus-program op for at fjerne virussen ”Brain”, som smittede gennem brugen af disketter. Spredningen af virus foregik trods alt ret langsomt på denne måde – helt anderledes end i dag, hvor virus spredes med lynets hast gennem netværk – især over Internettet.

Siden 1986 er antallet af computervirus vokset eksplosivt – især i de seneste år – og man anslår, at der i dag findes langt over 100.000 virusser i omløb, hvoraf de fleste dog er varianter af andre. Skadevirkningen af en computervirus kan være enorm – alene ”I Love You”-ormen (maj 2000) anslås at have kostet 8,75 milliarder dollars.

I det følgende gennemgås de mange irriterende ting, som i daglig tale omtales som ”computervirus”, selv om de fleste altså ikke rigtig har noget med virus at gøre. Men det er måske også lige meget ... hovedsagen er, at det alt sammen er enten skadeligt eller irriterende. Og vi er nødt til at forholde os yderst kritisk og tage vore forholdsregler.

PS: Ifølge **Dansk Sprognævn** er både "virus", "virusser" og "vira" korrekte flertalsformer af "virus" på dansk. Så man kan altså selv vælge !

Traditionelle virus

En virus kan programmeres til at gøre forskellig skade (kaldet ”payload”):

- formatere harddisken, slette, overskrive eller kopiere filer og mapper
- ændre dato, attributter, størrelsesangivelse navn og type for en fil.
- stille om på opsætningen af programmer
- forhindre computeren i at starte eller få den til at slukke
- forhindre Internetforbindelsen i at virke
- udsende e-mails via ens mailprogram (evt. med falsk afsenderadresse)
- drille: CD-skuffen kører pludselig ud og ind – eller skærmen opfører sig ”morsomt” og usædvanligt

Div. karaktertræk ved forskellige virus

- **Boot-virus:** når en computer tændes, så siger man, at ”den booter”. Først startes der bestemte programmer, som computeren har brug for for at starte – og disse programmer ligger i et område på harddisken, som kaldes ”boot-sektoren”. En boot-virus lægger sig sammen med disse opstarts-programmer og er derfor ”levende” inden f.eks. Windows og dit antivirus-program startes ... Boot-virus kan dog godt fjernes alligevel !

- **Stealth-virus:** forsøger at gøre sig selv ”usynlige” (lige som Stealth-fly som ikke kan ses på radar el.lign.), indtil den bliver aktiveret på et bestemt tidspunkt.

- **Time-bomb:** Virus som er programmeret til et bestemt tidspunkt. F.eks. virussen ”Chernobyl” som vågner op og gør skade på årsdagen (natten mellem 25. og 26. april) for atomkraftulykken på atomkraftværket i Chernobyl i 1986

- **Dropper:** Et program som installerer en virus på systemet

- **Polymorfe virus**: Er i stand til at omprogrammere sig selv ... de muterer en smule og gør det sværere for antivirusprogrammerne at genkende dem. Meget almindelig egenskab i moderne virus-typer !

- **Fil-virus:** sætter sig fast på programfiler af f.eks. typen .exe, .com

Ormevirus (worms)

Kaldes også for mail-virus, da ormene ofte spredes via vedhæftede filer i e-mails. En orm minder om en virus, men ormen er et selvstændigt program, som ikke har brug for et andet program for at blive spredt. Den indeholder sit eget ”postvæsen” (SMTP-engine), som automatisk kan sende ormen videre og smitte andre maskiner på netværket – på et internt netværk (intranet) eller via Internet. Den misbruger ofte alle mail-adresserne i dit Outlook-kartotek.

Ormen spreder sig ved at udnytte huller i sikkerheden i Windows, på servere, i din browser eller ved at udnytte, at mange stadig ikke har lært at være forsigtige, når de modtager en fil med en spændende titel som for eksempel ”who_shot_JFK.vbs”. Du kan også blive angrebet, hvis du surfer forbi en suspekt **hjemmeside**, der er inficeret af en orm.

Når ormen har inficeret en maskine, spreder den sig selv ved udsende e-mails, der indeholder kopier af ormen, ofte til alle i dit adressekartotek, eller ved at benytte din Internetforbindelse til at søge efter andre maskiner med huller i sikkerheden, som den kan inficere.

Ligesom virus kan orme også forvolde store skader ved at slette filer o.s.v., men en anden kedelig egenskab er, at de mest aggressive orme spreder sig i så store mængder, at de får dele af Internettet til at køre langsommere eller helt lammer en virksomheds kommunikation, fordi mailserverne overbelastes.

Mange moderne orme installerer endvidere en såkaldt "**skjult bagdør**" (**trojansk hest**) på din computer, som så kan benyttes af en ondsindet hacker, hvis du ikke har den nødvendige beskyttelse. Ved hjælp af en "trojansk hest" kan fremmede faktisk overtage kontrollen med din maskine, uden at du ved det.

Trojanske heste

Udtrykket "**trojansk hest**" stammer naturligvis fra den græske mytologi, hvor Odysseus & Co. havde belejret byen Troja i 10 år, og nu var de ved at være trætte af det.

De lavede derfor en kæmpestor træ-hest, som de om natten placerede udenfor byporten til Troja. Og den var fyldt med soldater ...

Indbyggerne trak selv hesten indenfor næste morgen – de troede det var en slags gave fra guderne, og at Odysseus & Co. var forsvundet. Men det var de ikke ... om natten kravlede de ud af hesten, åbnede byporten indefra og lukkede så hele deres hær ind. Troja blev fuldstændigt udslettet – og krigeren Achilleus blev slået ihjel, men det er en anden historie.

En trojansk hest er IKKE en virus – men den er yderst farlig. Når en virus eller en orm installerer en trojansk hest på offerets computer, er der skabt en "**bagdør**", som kan udnyttes til at **fjernstyre** computeren udefra.

Den trojanske hest kan også (hemmeligt) installere sig selv samtidig med et andet program, som man f.eks. finder gratis på Internet. Der ligger et spændende gratis spil på nettet, lige til at hente og installere. Men måske får man altså samtidig skabt en "hemmelig spion" på maskinen ...

Den trojanske hest kan nu enten sende besked ud i verden, så en ondsindet person får at vide, at computeren er klar til at blive overtaget, eller den kan blot sætte sig til at vente og lytte. Enhver med den trojanske hests styreprogram vil herefter kunne få fuldstændig kontrol over computeren, og både starte programmer på den og overvåge, hvad der tastes på tastaturet v.h.a. en såkaldt **keylogger**. Hvis du altså ikke har installeret en såkaldt **firewall** på maskinen ...

Læs mere om firewall i afsnittet om "Hacking" !!

Kombinationer
Der er intet til hinder for, at en orm kan indeholde både en virus, som inficerer dine programmer og sender orm ud i verden, OG en trojansk hest, som åbner for fjernstyring udefra. Kun virus-programmørernes ubarmhjertige kreativitet sætter grænserne – og grænserne flyttes hele tiden.

Læs mere om den trojanske hest i afsnittet om ”Hacking” !!

Makrovirus

Makrovirus skjuler sig (og spreder sig) i filer, som kan indeholde **makroer** – f.eks. filer oprettet med Word og Excel. Men hvad er en makro ??

Eksempel:
Makroer er små programmer, som man kan lave i mange forskellige programmer f.eks. Word og Excel for at udføre en række handlinger på en lettere måde. Hvis man f.eks. har brug for at udskrive den aktuelle side i et langt Word-dokument, så skal man bruge en række klik med musen i menuer og dialogbokse ... ved at ”indspille denne række handlinger” som en makro, så kan man blot ved at klikke på en enkelt knap få udskrevet den aktuelle side i dokumentet.

Dette kan benyttes til at skjule en makro-virus i f.eks. et Word-dokument eller et Excel-regneark. **Effekten** af denne virus kan være hvilken som helst.

Smitten foregår f.eks. ved, at man modtager en Word-fil sammen med en e-mail. Når man åbner den vedhæftede fil i Word, så smittes programmet Word. Og derefter smittes alle andre dokumenter, som oprettes med dette program. Sender man så selv Word-dokumenter rundt til folk, så bliver de også smittet.

Spyware

Spyware har intet med virus at gøre – men det er ret irriterende og KAN være direkte skadeligt, idet der kan opsnappes vigtige informationer, som sendes videre til fremmede med skumle hensigter.

Spyware er en bred betegnelse for små **spionprogrammer**, der indsamler informationer om brugerens interesser, adfærd og vaner på Internettet – og evt. også på brugerens harddisk omkring netbank, kortnumre, passwords m.v.

Spyware sender informationer tilbage til bagmændene, som enten selv bruger oplysningerne til økonomisk kriminalitet eller i reklame-øjemed - eller de sælger dem videre til andre.

Altså en form for **overvågning** og udnyttelse.

Spyware installeres typisk på computeren sammen med et andet program, som man f.eks. downloader gratis via Internet. Måske står der endda i "betingelserne", at det sker – men hvor mange af os læser disse betingelser, som ofte er på engelsk og fylder 8 sider med små bogstaver ...?

Cookies

En såkaldt "cookie" (= småkage) er faktisk en mekanisme, som indsamler information om en Internetbruger og gemmer informationen på brugerens egen computer. En cookie er blot en lille tekstfil, som indeholder nogle oplysninger vedr. en bestemt hjemmeside. Det er kun den hjemmeside, der kan "plantet småkagen", som kan bruge informationerne til noget.
Eksempel:
Mange hjemmesider giver dig mulighed for at "skræddersy" startsiden med præcis det indhold, som du ønsker. Det kunne f.eks. være nyheder indenfor bestemte emner, et bestemt design/farver på siden o.lign. Disse informationer (indstillinger) bliver oftest gemt i en cookie på din egen computer. Og næste gang du besøger hjemmesiden, så hentes informationerne frem og bruges til at vise siden, som du vil have den. Det er jo sådan set meget smart.

Cookies er **ikke farlige** (de kan IKKE indeholde virus) – og de kan faktisk være praktiske og nyttige. Men de kan også misbruges til at indsamle informationer, som du ikke aner noget om. Og du aner heller ikke, hvad de bliver brugt til !!

De fleste websites skjuler sjældent, at de benytter cookies, og brugeren kan selv fravælge adgang til cookie-informationer. Men hvis et site benytter cookies og ikke fortæller brugerne om dette, så kan man betragte disse cookies som en form for spyware, fordi det foregår i det skjulte.

Adware og pop-up reklamer

Udtrykket **adware** er engelsk og det er en sammentrækning af ordene **ad**vertisement (= annonce) og soft**ware**. Må ikke forveksles med "Ad-Aware", som er et glimrende program, som netop bekæmper adware !!

Adware-programmer er mere harmløse end spyware, da de ikke sender information tilbage til bagmændene. Adware kan vise **pop op-vindue**r med reklamer, ændre indstillinger i browseren (f.eks. startsiden), installere uønskede søgemenuer eller tilføje bookmarks i browseren. Hvis et adware-program sender information tilbage om brugerens Internetvaner, er det spyware.

Browser hijacking

Browser hijacking (kidnapning af browseren) forveksles tit med spyware. Browser hijacking sker, hvis man bliver ført til en anden hjemmeside end forventet, selv om man har indtastet den korrekte web-adresse. Denne form for hijacking er svær at beskytte sig imod. Her gælder det om at bruge sin sunde fornuft og vurdere, om websitet ser rigtigt ud. Evt. kontakte firmaet.

En anden form for hijacking er, når personer opretter domænenavne, som til **forveksling** ligner andre hjemmesiders web-adresser:

Hvis man skriver www.it-borger.dk uden bindestreg (www.itborger.dk), kan man risikere at ende på et helt andet website med skjulte hensigter. Som domæne-ejer kan man undgå dette problem ved at købe flere næsten enslydende domæner, som ligner hinanden. I denne form for browser hijacking spekuleres der altså i, at brugerne ikke staver web-adressen korrekt.

Browser hijacking hænger sammen med begrebet "**phishing**", som behandles senere.

Spam (junkmail)

På engelsk betyder det "hakket skinkekød på dåse" – en slags ubestemmelig fars, som måske nok mætter men ikke smager særlig godt. I forbindelse med computeren er SPAM udtryk for de irriterende e-mails med reklamer, som vi ikke har bedt om at få.

Langt hovedparten af spam kommer fra udlandet (især USA og Asien) og er på engelsk, hvilket gør det relativt let for os danskere at genkende dem. De fleste reklamerer for lån, produkter, uddannelser og porno. Foreningen "Børns Vilkår" har imidlertid påpeget, at især børn og unge kan være meget sårbare overfor denne form for reklame, når de bliver tilbudt at bolle med Britney Spears, købe Viagra eller anabolske steroider o.s.v. Løsningen er at opdrage børn og unge til at være kritiske overfor de ting, som de ser og modtager via Internettet.

Normalt er spam-mails ganske ufarlige, hvis man blot sletter dem med det samme. Man skal endelig ikke **åbne** en spam-mail, man skal ikke **svare** på den eller forsøge at "**afmelde** sig" hos afsenderen, for så er bagmanden bare klar over, at der er liv på denne mail-adresse og fortsætter med at sende spam.

Der kan sagtens være vedhæftet en fil i en spam-mail, og den vedhæftede fil kan sagtens indeholde virus eller orm ... så der er god grund til at være på vagt.

I Danmark er det **forbudt** at udsende spam iflg. Markedsføringsloven §6a !! Hvis en spam-mail stammer fra et dansk firma, så kan man indbringe en klage til Forbrugerombudsmanden (dansk@spamklage.dk), som så vil tage sig af sagen – og der er allerede givet store bøder til danske spammere.

Men hvis der er tale om udenlandske spam-firmaer, så har man kun en meget lille chance i kampen ... oftest gælder der helt andre regler i det land, hvor spammen er udsendt.

Men hvordan pokker får de fat i vores e-mail adresser ?

Det er IKKE levende mennesker, der sidder og beslutter, at nu vil de sende en reklame-mail til dig. Det hele foregår v.h.a. computerprogrammer – såkaldte "robotprogrammer" – som konstant søger rundt på alle dele af Internettet og leder efter e-mail adresser på hjemmesider, i nyhedsgrupper, i gæstebøger o.lign. Og der findes endda programmer, som blot gætter på mail-adresser på kendte domænenavne – det koster jo næsten ingenting at sende disse spam-mails ud i millionvis, og hvis bare der kommer penge ud af 1% af dem, så er det en god forretning.

Orme-virus benyttes også som redskab til at "høste mail-adresser" rundt omkring ... til senere udsendelse af spam.

Man skal altså ikke skrive sin e-mail adresse alle vegne !!

HTML-virus

Web-sider på nettet er lavet i et kodesprog, som kaldes HTML (Hyper Text Markup Language). På visse hjemmesider benyttes endvidere et "script-sprog" hvor der kan gemmes skadelig kode – det betyder, at man faktisk kan blive smittet med skadelig kode (virus) gennem sin browser, blot ved at besøge en hjemmeside ... især hvis ens browser ikke er opdateret. Oftest er det på "**suspekte hjemmesider**", man kan støde på den slags (typisk porno og sider med mere eller mindre ulovlige produkter og ydelser).

Mange mennesker tillader, at deres e-mail program kan benytte **HTML-mail**. Det betyder, at man f.eks. kan formatere sine egne mails med forskellige skrifttyper, farver o.s.v. Og man kan indsætte billeder og kulørte baggrunde. Samtidigt tillader man også de samme ting i de indgående mails, som bliver vist som en slags webside i stedet for "ren tekst". Og straks er der altså risiko for smitte **uden** at klikke på nogen vedhæftede filer !!

Hoax

En hoax er en **falsk** virusadvarsel, som spredes via e-mail.

En typisk hoax indeholder f.eks. en skrækhistorie om en ny virus, som vil slette data på ens computer. Afsenderen påstår også, at advarslen blev udsendt "for en uge siden" fra et stort firma som IBM eller Microsoft. Der er dog aldrig et link til en artikel om den farlige virus med, og man kan heller ikke finde noget hos de store antivirus-firmaer om virussen. Beskeden opfordrer altid til, at du hurtigst muligt sender den videre til alle, du kender – en almindelig hoax kan nemlig ikke sende sig selv videre automatisk ligesom en orm.

De **godartede** af slagsen har blot samme formål som et kædebrev, hvilket vil sige, at de bare spilder folks tid og belaster mailserverne med unødvendige mails.

De mere **ondsindede** forsøger ikke blot at narre dig til at sende advarslen videre (og få dig til at fremstå som et fjols), men lokker dig også til at slette bestemte filer på din harddisk. På denne måde bliver du faktisk selv til en virus ... hvis du altså hopper på den. En hoax skal du ikke sende videre, du skal ikke gøre andet end at slette den med det samme !!

Friends-greetings virus

En e-mail, der umiddelbart ligner en hilsen fra en ven eller bekendt, men i virkeligheden opfører sig som en mellemting mellem virus og spam.

Den såkaldte "Friendgreetings"-virus ankommer som en e-mail med f.eks. følgende indhold: "X has sent you an E-Card - a virtual postcard from FriendGreetings.com. You can pickup your E-Card at FriendGreetings.com by clicking on the link below."

Brugeren skal så godkende at installere et lille program for at åbne hilsenen, hvilket mange gør uden at læse det med småt først. Og det er netop det, som denne hilsen udnytter. For læser man programmets licensaftale, står der, at det er reklame for f.eks. porno, man i virkeligheden henter ned. Derudover siger man ja til at sende e-mailen videre til kontaktpersonerne i ens adressekartotek. Siden man selv har klikket **ja tak** til at hente programmerne er kampagne-typen ikke (som man skulle tro) ulovlig.

Mange kalder "Friendgreetings-kampagnen" for en virus, men antivirusselskaberne betegner den ikke som en virus i egentlig forstand. I modsætning til gængse virus er formålet at ikke at øve hærværk mod computeren, men at spamme brugerne med uønsket internetreklame.

Blandings-misbrug

Noget af det luskede og besværlige ved alle disse ting er, at de forskellige metoder ofte kombineres af skurkene:

- En makrovirus kan slippe en orm løs
- En orm installerer en trojansk hest og sender sig selv videre
- En spam-mail eller hoax kan sagtens medbringe en vedhæftet fil, som indeholder skadelig kode

Der er al mulig grund til at være på vagt, bruge sin sunde fornuft og styre sin nysgerrighed – et forkert klik med musen kan gøre forskellen ...

Eksempel (Bagle-worm)

Bagle ormen spreder sig med enorm hast og installerer trojansk hest

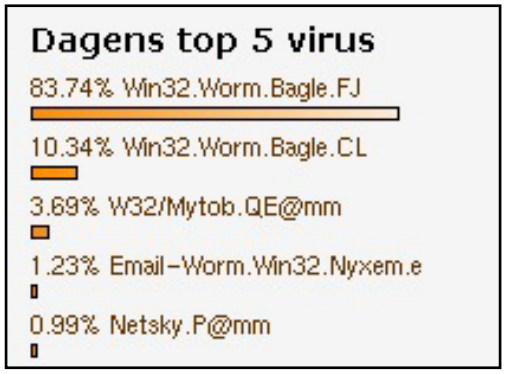
(Kilde: www.csis.dk og www.comon.dk, 7-2-2006)

En variant af ormen **Bagle** (også kaldet **W32.Worm.Bagle-FJ**), som blev sendt i omløb d. 2. februar 2006, er ved at få en ny opblomstring. Sikkerhedsfirmaet CSIS har opfanget et betydeligt antal, og den udgør det seneste døgn over 83% af alle virus-infektioner i DK.

I lighed med andre Bagle orme er denne kode yderst skadelig. Den formerer sig via e-mail og indfanger på den måde nye zombie-maskiner i Bagle-forfatterens spind af spam- og bagdørs-inficerede maskiner. At ormen først i dag for alvor er begyndt at sprede sig, kan ikke forklares. De fleste antivirus-firmaer har for længst frigivet opdateringer, som klarer denne trussel, ligesom flere kan fange den via heuristisk teknologi.

Ormen ankommer via e-mail med følgende indhold:

Fra: [Spoofet/forfalsket afsender adresse]



Emne: [en af følgende kombinationer]

- Delivery service mail
- Delivery by mail
- Registration is accepted
- Is delivered mail
- You are made active

Indhold: [en af følgende kombinationer]

- Thanks for use of our software.
- Before use read the help

Vedhæftet fil: [en af følgende kombinationer]

- wsd01.zip
- viupd02.zip
- siupd02.zip
- guupd02.zip
- zupd02.zip
- upd02.zip
- Jol03.zip

Hvis den vedhæftede fil åbnes, så droppes en kopi af ormen til den lokale harddisk, og den ændrer dernæst i registreringsdatabasen med det formål, at ormen og bagdøren aktiveres ved en genstart af systemet. Når en pc bliver ramt, bliver den til en zombie-pc, som fjernstyres af bagmanden fra det østlige Rusland. Selvom myndighederne har haft ham under lup de sidste to år, så har man endnu ikke kunne røre ham.

”Man opdager ikke, at ens pc er blevet til en zombie, fordi det foregår i baggrunden. Almindelige folks computere samles et zombie-netværk, hvor forfatteren til virussen kan bruge zombie-computerne til for eksempel at angribe hjemmesider med eller sende spam med,” siger **IT-sikkerhedsekspert Peter Kruse fra CSIS**.

Virussen spreder sig via mail og peer-to-peer-programmer. Man skal som altid **ikke** åbne vedhæftede filer fra folk, man ikke kender. Hvis man er bange for at ens computer er inficeret, så kan man mange steder på nettet gratis scanne sin PC og få fjernet zombie-virussen. Se f.eks. under links sidst på disse sider !!

Virussens historie

1981-82	Rich Skrenta's "Elk Cloner" program inficerer Apple II disketter uden at slette data – og for hver 50'ende gang dukker der et digt op på skærmen. Professor Len Adleman indfører udtrykket "virus" til beskrivelse af "selv-kopierende programmer".
1986	Computervirus bliver kendt i den større offentlighed med virussen Brain, som smitter PC'en via disketter
1988	Den første antivirus kommer på banen for at fjerne Brain-virussen
1990	IBM og McAfee introducerer de første antivirus-programmer, og man abonnerer på opdateringer på diskette, da Internet ikke er så udbredt endnu.
1992	Michelangelo-virussen bliver et populært emne - dog mest i medierne. De første værktøjer og programmer til at "bygge" computervirus med kommer på markedet. Bl.a. Dark Avenger Mutation Engine (DAME)
1995	Makrovirus begynder at udnytte Microsoft Office-programmer
1998	Alverdens computere angribes af den første "trojanske hest" kaldet Back Orifice, som kan fjernstyre PC'er
1999	Melissa-virussen spredes med lynets hast til ca. 1 mio. PC'er. Melissa aktiveres ved at åbne en vedhæftet fil i e-mail – og den sender sig selv videre via adressekartoteket.
2000	Computervirus spredes hurtigt i stort tal via e-mail. Bl.a. virussen LoveBug (I love you)
2001	Nimda og Anna Kournikov, nye virus med stor spredning
2002	Virus spredes bl.a. i billedfiler (jpg) og via fildelingstjenester som f.eks. Kazaa. Virus og hacking begynder at smelte sammen.
2003	Virussen Hammer slår alle rekorder i hurtigt spredning. På 10 minutter smitter den 75.000 computere. Virussen SoBig.F slår til med voldsom styrke i august-september. Alene i Danmark smitter den ca. 1,3 mio. computere. Der tales nu om risiko for virus i mobiltelefoner.
2004	Slagsmål mellem de 3 virusser MyDoom, NetSky og Bagle. Motivet bag disse virus er at skabe en bagdør, som kan misbruges til "anonym" udsendelse af spam samt deltagelse i DOS-angreb. Forsøger at slå antivirusprogrammer ud – og forsøger i øvrigt at ødelægge og udkonkurrere hinanden.
2005	De såkaldte "botnet" vokser i omfang. Private computere tages som gidsler og misbruges til kriminelle formål

Virus-forebyggelse og helbredelse

Det er lettere (og mindre smertefuldt) at forebygge end at helbrede. Og dette gælder især i forhold til computervirus o.lign.

Antivirus-programmer

Det er et absolut MUST at have et godt antivirus-program installeret på computeren, hvis man vil være bare nogenlunde sikker på at kunne have sine ting i fred !! Med mindre man aldrig kobler sig på Internet eller sætter en fremmed diskette/CD i ... Forsøg har faktisk vist, at en ny og helt **ubeskyttet** computer er voldsomt inficeret efter blot 20 minutter på nettet – og stort set vil gå i stå, hvis man fortsætter ret meget længere ...

Og det er nødvendigt at **opdatere** programmet mindst en gang om ugen – eller helst lade programmet gøre det automatisk.

Et antivirus-program kan nemlig kun bekæmpe de virus, som det "kender" – og da der dukker nye varianter og virus op dagligt, så er det nødvendigt at opdatere listen. Dette gøres via producentens hjemmeside – og et godt antivirus-program klarer selv dette **automatisk**, så man ikke behøver at tænke på det !!

Der findes masser af firmaer, som laver antivirus-programmer. Visse af dem kan levere en hel "sikkerhedspakke" mod både virus, hacking og spyware. Her er et kendt udvalg:

- www.symantec.dk (laver Norton-programmerne. 479 kr pr. år)
- www.panda.dk
- www.drsolomon.com
- www.trendmicro.com
- www.nai.com (tidligere McAfee)
- www.norman.com
- www.bitdefender.com

De fleste af dem tager penge for det efter en prøveperiode på 1-2 måneder, men der findes også programmer, som er 100% gratis at bruge for privatpersoner. Her vil jeg blot anbefale programmet **Avast** fra Tjekkiet, som virker aldeles glimrende og gratis for private: www.avast.com

På min hjemmeside kan du finde det direkte link, så du kan downloade programmet. Og der ligger også en **vejledning** i, hvordan du skal gøre og hvordan du indstiller programmet til at fungere bedst muligt bagefter.

Ligeledes er der links til nogle steder på nettet, hvor man gratis kan få scannet sin computer "**online**". Det tager lidt tid, og det kan ikke erstatte et antivirus-program – men man kan se det som et godt supplement.

Krav til dit antivirus-program

- Programmet skal konstant (resident) beskytte mod indkommende mail, som indeholder virus (f.eks. i vedhæftede filer). Programmet skal stoppe disse og give dig mulighed for at slette dem, inden de åbnes og smitter
- Programmet bør også opdage de kendteste trojanske heste
- Programmet skal også holde øje med virus, når du surfer på Internet
- Programmet skal scanne disketter, som sættes i maskinen
- Programmet skal scanne filer som åbnes (inkl. exe-filer) – det tager lidt ekstra tid, men det er en god idé !
- Der skal være mulighed for, at man selv kan sætte programmet i gang med at scanne hele harddisken for virus - eller scanne en fil man har downloadet, inden man åbner den
- Programmet bør kunne fjerne en virus, som den finder
- Programmet skal sørge for at opdatere sig selv automatisk via nettet
- OBS: Du skal kun have ét antivirusprogram installeret. Det giver ikke dobbelt sikkerhed at installere to – de kommer nemlig op og slås med hinanden og beskylder hinanden for at indeholde virus ... :-)

Hvis skaden er sket

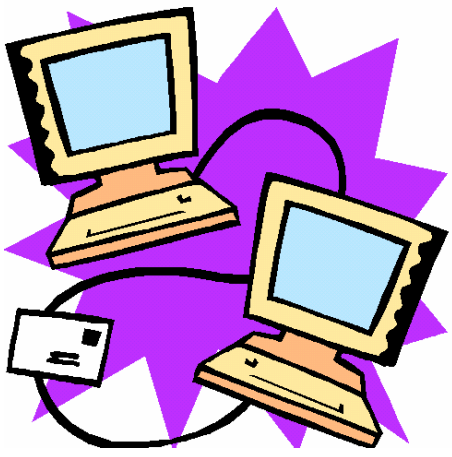
- Hvis dit antivirus-program finder en virus, så skulle det gerne kunne fjerne virussen helt.
- Man kan evt. forsøge med en af "online-scannerne" eller et program som "Stinger" fra NAI (tidligere McAfee). Der er links til disse på min hjemmeside !!
- Hvis virussen er særlig besværlig, så har mange af antivirus-firmaerne specielle værktøjer (removal tools) liggende til fri download på deres hjemmeside. Disse værktøjer er lavet til specifikke (svære) virus og giver en forklaring på, hvordan virussen fjernes.
- I værste fald kan du være nødt til at formatere din harddisk for at slippe helt af med virussen – og så er det, man er glad for en virusfri back-up af sine data. Og du vil være nødt til at installere alle dine programmer igen ...

Tro mig ... det er langt lettere at forebygge end at helbrede :-)

Hvorfor laves der virus ?

Oprindelig har virus nok mest været udtryk for **hærværk** på lige fod med graffiti på gade og vej. Og det har været en **udfordring** at kunne lave en virus, som blev spredt til hele kloden meget hurtigt – og måske med omtale i medierne. Men i de senere år er virus blevet en del af den **økonomiske kriminalitet** på Internettet – og overlapningen mellem virus og hacking er konstant voksende:

- Virus benyttes som" transportmiddel" for andre skadelige programmer, som installeres på vore computere – uden at vi ved det
- Trojanske heste og spyware kan tjene til at aflure tastetryk, personlige oplysninger og koder vedr. netbank o.s.v.
- Trojanske heste kan overtage kontrollen med din PC og gøre den til en såkaldt "zombie" ... som styres udefra. Din PC kan f.eks. benyttes som udgangspunkt for hacking på andre computere på nettet
- Din PC's harddisk kan misbruges til opbevaring af ulovlige ting (piratkopier af film og software, mp3-filer, børneporno o.lign.)
- Din PC kan misbruges til udsendelse af spam-mails
- Din PC kan misbruges i de såkaldte DOS-angreb (Denial-of-Service), hvor et stort antal computere på samme tidspunkt får ordre udefra om at bombardere en bestemt server (hos et bestemt firma) med data. Med det resultat at serveren på et tidspunkt bliver overbelastet og giver op. Firmaer som Microsoft, Yahoo, Symantec og den amerikanske pladebranche's organisation RIAA har oplevet den slags.



Disse netværk af smittede computere (**botnet**) kan ligefrem lejes ud til skumle formål. Virus er ikke længere kun hærværk – der er store penge at tjene !

Dem der laver virus er interesserede i at få spredt virus til flest mulige computere. Derfor leder de bevidst efter sikkerhedshuller i de mest brugte programmer, som fx Windows, Internet Explorer og Outlook/Outlook Express. I dag findes der programmer, som automatisk scanner Internettet for computere med de sårbarheder, hackeren ønsker at udnytte.

Microsoft udsender én gang om måneden opdateringer til ovennævnte programmer (samt Office-pakken) for at lukke nye sikkerhedshuller. Og det er både godt og skidt ... men mest godt. Der er bare stadigvæk mange mennesker, som ikke får installeret disse opdateringer – og det ved hackerne godt, så de kan gå målrettet efter de maskiner, som stadigvæk er sårbare.

Og de virus, som man fyrer af sted, er præcis programmeret til at udnytte de sikkerhedshuller, som Microsoft detaljeret har beskrevet ... Såå øh, husk lige at opdatere Microsoft-programmer den 2. tirsdag i hver måned, når der kommer besked om det !!

PS: Det er mest Microsoft, som skurkene elsker at hade – men andre programmer går heller ikke fri. Der er også virus til Linux, Mac og Netscape/Mozilla-programmerne Firefox og Thunderbird m.fl. selvom omfanget er langt mindre.

Beskytter vi os godt nok ?

I det nyeste nummer af computerbladet "**Komputer for alle**" (nr. 2/2006) refereres en læserundersøgelse, hvor 5462 læsere havde svaret på en række spørgsmål. Den viser, at 98% af læserne har installeret et antivirus-program derhjemme, og mindst 92% opdaterer det hver uge eller lader programmet klare det automatisk. 75% har selv oplevet at have virus på deres PC.

80% lader Windows opdatere automatisk, når der udkommer nye opdateringer fra Microsoft.

Eksperter vurderer, at ca. 75% af alle e-mails er spam. Derfor har 62% af læserne installeret et "spam-filter" – hvilket betyder, at hele 65% af læserne modtager under 10 spammails om ugen. Ca. 10% af læserne modtager over 40 spammails om ugen – og det er jo nok dem, som ikke har installeret noget spamfilter ...

65% har haft "spyware" på deres PC – og 75% har derfor installeret et program, som fjerner den slags. 45% har oplevet "popup-reklamer" med anstødeligt indhold ...

Rådet for IT-sikkerhed fortæller i deres Årsberetning fra 2005, at 93% af de borgere, som er koblet på Internet, har installeret et antivirus-program – og 80% har opdateret det indenfor den sidste måned. 70% har installeret en firewall.

Tabellen herunder viser, hvor mange pct. der har oplevet tab af data eller tid som følge af virusangreb. Blandt borgerne ser tallene desværre ud til at stige – mens det går bedre i virksomhederne og i det offentlige.

	Borgere	Virksomheder	Offentlige sektor
2002	-	46 pct.	59 pct.
2003	29 pct.	32 pct.	58 pct.
2004	31 pct.	24 pct.	43 pct.
2005	35 pct.	-	-

Rådet for IT-sikkerhed gennemførte i maj-juni 2005 en undersøgelse via telefoninterviews, hvor 74% mente, at de havde ret godt styr på IT-sikkerheden. Men når man gik dem nærmere på klingen og spurgte om, hvordan man genkender trusler i e-mails samt på usikre websites, så havde 63% faktisk en utilstrækkelig viden ...

Det kunne tyde på, at folk mangler viden !! Det er ikke nok at installere div. sikkerhedsprogrammer, hvis man ikke også har en viden om truslerne. Antivirus-programmet kan ikke beskytte én mod virus, hvis man selv lukker virus ind ved at begå dumme (menneskelige) fejl.

I virksomhederne viser det sig også, at selvom man har installeret div. sikkerhedssoftware, så sker der netop "menneskelige fejl" i håndteringen af IT-systemerne.

Politisk vil man gerne lægge en større del af ansvaret over på Internet-udbyderne ... som til gengæld helst vil tørre ansvaret af på brugerne selv.

Under alle omstændigheder ser det ud til, at det offentlige fortsat bør køre **oplysningskampagner** om disse ting – ligesom man i virksomhederne skal huske på sikkerheden i forhold til hjemmearbejdspladser og uddannelse af medarbejderne.

Der er masser af gode **informationsmaterialer** at hente på nettet, f.eks:

- www.it-borger.dk
- www.raadetforitsikkerhed.dk
- http://sikkerhed.tdconline.dk

Gode våben mod spam og spyware

Der findes adskillige programmer mod disse ting – og i en større virksomhed med mange computere og medarbejdere må man naturligvis vælge et yderst pålideligt produkt. Det koster både tid og penge at kæmpe med disse problemer !! Men private har det lidt lettere:

- Spam kan bremses ganske effektivt med det danske program **SPAMfighter**, som er gratis for private. Det lægger sig som en del af mail-programmet Outlook og filtrerer al spam fra. Det bliver dog lagt over i en speciel mappe, som man kan checke og slette med mellemrum.

- Adware, dårlige cookies, browser hijackers, spyware m.v. kan fjernes ved at bruge programmet **Ad-Aware**, som også er ganske gratis til privat brug.

OBS: Der er naturligvis links til disse programmer på min hjemmeside !!

Læs evt. mere om spyware, programmer mod den slags o.lign. på hjemmesiden: www.spywarefri.dk

Checkliste mod virusproblemer

- Installer et anerkendt antivirus-program, som kører i baggrunden hele tiden (resident) og scanner alle filer, som kommer udefra (Internet, mail, disketter, CD-ROM o.s.v.) – og evt. scanner filer som åbnes og ændres. Det er sikrest at installere programmet fra CD el.lign., INDEN man kobler computeren på nettet, hvis dette kan lade sig gøre.

- Straks efter at du har installeret antivirusprogrammet, så skal du opdatere det via producentens hjemmeside.

- Og dette skal du gøre ofte (helst hver uge), hvis ikke programmet kan indstilles til at gøre dette automatisk, mens du er online.

- Sørg for at lave en startdiskette i Windows. Og sørg for at lave en "Rescue Disk" via dit antivirusprogram, hvis dette er muligt. Og gør dette, INDEN det er for sent !! Hvis din harddisk bliver voldsomt medtaget og "går i sort", så kan du nemt få brug for disse ting.

- Lav back-up disketter eller CD med dine vigtigste datafiler ! Og sørg for, at filerne er fri for virus, inden du laver din back-up ...

- Pas på e-mails med vedhæftede filer !! Især hvis mailen kommer fra folk, som du ikke kender - eller hvis emne-linjen ikke er på dansk.

- Hvis den vedhæftede fil er af fil-typen:
  exe, com, bat, vbs, pif, scr, js, zip eller har dobbelt filtype i slutningen (f.eks: very_good_offer.txt.vbs) – så er der ekstra grund til at være på vagt. Er du i tvivl om den slags, så slet mailen (lad være med at klikke og åbne den !!) og kontakt evt. afsenderen på anden vis, hvis det er en du kender.

- Sørg også for at opdatere Windows (inkl. Internet Explorer og Outlook) via Windows Update funktionen: i browseren klikker du på Funktioner > Windows Update. Sørg for at du også fremover bliver gjort opmærksom på nye opdateringer, som lukker sikkerhedshuller i dit system.

- Visse typer virus (f.eks. gemt i vedhæftede filer eller skjult HTML-kode) kan "aktiveres", hvis blot man åbner mailen, så den kan læses i "indholdsruden" (det hedder det i Outlook).
  Man kan derfor med fordel **lukke for indholdsruden !!**

  I **Outlook 2000 og XP** gøres det således:
  Sørg for at "Indbakke" er valgt. Klik så på Vis og "sluk" for punktet "Indholdsrude".

  I **Outlook 2003** gøres således:
  Sørg for at "Indbakke" er valgt. Vælg: Vis > Læserude > Deaktiveret

Nu risikerer du ikke, at smittebærende filer installerer sig selv automatisk, du kan vælge at slette mailen uden at åbne den, hvis den ser suspekt ud – eller du kan dobbeltklikke på den for at læse den.

- Ofte ligger der virus i lydfiler (via tjenester som Kazaa o.lign) samt de forskellige morsomme ”greeting-cards” som man kan sende fra div. websider.

- Lad være med at besøge ”suspekte” hjemmesider, da der KAN ligge ondsindet kode, som via browseren hopper over på din computer og udføres, uden at du er klar over det.

- Lad være med at åbne programfiler fra nettet med det samme. Gem dem f.eks. på ”Skrivebordet” og kør et viruscheck på dem, inden du dobbeltklikker og installerer noget nyt.

- Lad være med at opgive personlige oplysninger på Internet – med mindre det er strengt nødvendigt og virker troværdigt.

- Såkaldte ”hoax” (falske kædebreve med advarsler eller opfordringer om dit og dat) skal du IKKE sende videre. Bare slet dem med det samme!

- Sørg evt. for at følge lidt med i udviklingen omkring disse emner – ved at abonnere gratis på et eller flere nyhedsbreve via mail. Der findes flere gode danske steder på nettet. F.eks. www.virus112.dk og hos TDC på http://sikkerhed.tdconline.dk

- Brug din sunde fornuft – og lad være med at tage unødige chancer ...

Hacking

Definitionen på hacking er: indtrængen (indbrud) på elektroniske dataområder og systemer, som man ikke har lovlig adgang til.

I Danmark benytter vi som regel kun udtrykket ”hacker”, fordi det er ulovligt alt sammen – men i udlandet (og især i hacker-kredse) benyttes ofte to udtryk: **hackere**, som er de ”gode”, og **crackere**, som er de ”onde” ... Hackerne ser ned på crackerne og vil helst ikke sammenlignes med dem !

Hvorfor bli’r man hacker ?

Der er ingen tvivl om, at spændingen er en afgørende faktor: Kan det lade sig gøre ? Det er en intellektuel udfordring at forsøge at hacke sig ind på ”besværlige steder” med stor prestige som f.eks. NASA, Det Hvide Hus, Microsoft o.s.v.

Der er mange, som mener, at hackere har en dårlig moral og lever et isoleret og asocialt liv blandt colaer og tomme pizzabakker ... men så enkelt er det nok ikke ... Der er nemlig mange forskellige motiver for at hacke – og der er stor forskel på disse folk samt deres dygtighed.

Man kan groft sagt opdele disse personer i 3 grupper:

Script Kiddies

Betegnelsen "script kiddies" bruges typisk om drenge/unge mænd, som ikke kender konsekvensen af den kode, de laver og spreder. På Internettet er det let at finde værktøjer, som man kan bruge til at skrive virus og ”hacke” uden nogen erfaring med programmering. De er næsten lige nemme at bruge som et tekstbehandlingsprogram. Derfor kan mange af dagligdagens IT-problemer kan sagtens skyldes disse "script kiddies" – altså glade **amatører**, som evt. finder skadelig kode på nettet og slipper den løs uden at tænke over konsekvenserne. Denne type ”hackere” udgør langt den største del – og de er ikke farlige, hvis man blot følger de gode råd vedr. beskyttelse af computeren.

Crackere

At bryde kopibeskyttelsen på et program (f.eks. Microsoft Office-pakken eller et spil) kaldes at ”cracke”. Og så kan man pludselig distribuere ”piratkopier” af disse ting – evt. tjene store penge på det.

Crackere laver deres aktiviteter for egen vindings skyld eller for at blære sig. De ødelægger data, stjæler data og forsøger ofte at sælge tingene bagefter. Efter indbrud i virksomheder kan de finde på at forsøge at lave pengeafpresning. De er ikke specielt dygtige og efterligner de ”ægte” hackere’s metoder.

Man må tro, at det er ”cracker-typen” som i dag benytter sig af virus for at inficere computere til div. formål (DOS-angreb, udsendelse af spam, opsnapning af bankoplysninger, industri-spionage o.lign.)

Hackere
De ”ægte” hackere er ekstremt dygtige til at programmere og udtænker selv deres metoder. Denne type er meget svære at kæmpe imod – til gengæld er der meget få af dem i forhold til de 2 andre typer (script kiddies og crackere). Hvis han giver sig tid til det, så kan den dygtige hacker sagtens snige sig udenom en firewall på computeren – og han kan (stort set) slette alle sine spor efter sig, så det er meget svært at finde ham bagefter.

Han ødelægger som regel ikke noget, men vil oftest blot bevise, at der ER huller i sikkerheden. Og så selvfølgelig bevise overfor sig selv og ”de andre”, at det godt kunne lade sig gøre. De ser sig selv som en slags Robin Hood-agtige frihedskæmpere – og en del af deres filosofi er, at alle informationer skal være frit tilgængelige ... En lidt mystisk tankegang.

En lille sammenligning med den virkelige verden
Amatør-hackerne løber ind på et fyldt fodboldstadion og skyder vildt omkring sig med et maskingevær. Samtlige blandt publikum har en risiko for at blive ramt - det er i hvert ret sandsynligt, at NOGEN bliver ramt, men det er helt tilfældigt. Og der er også en stor chance for at fange gerningsmanden, hvis nogen altså prøver på at fange ham !

De ”proff” hackere ligger på lur, studerer offeret (f.eks. præsidenten) og lærer alle detaljer udenad gennem længere tid, og kunsten består i at nedlægge offeret med eet "clean shot" lige i panden. Ingen andre kommer til skade, og hackeren er forsvundet sporløst bagefter. Og han er meget svær at finde - men det er ikke totalt umuligt, for der er måske altid nogle spor ...

I det lille eksempel her kunne "præsidenten" f.eks. være det danske forsvarsministerium, Pentagon eller Microsoft eller ... Men hr. og fru Jensen er næppe interessante for den type hackere - der er ingen grund til at "skyde" dem - og der er absolut ingen prestige i det i hackerkredse.

Men der er kommet penge med ind i billedet nu, så det betaler sig at ramme så mange som muligt. Hvis man kan opnå at få kontrol over en masse computere og deres Internet-forbindelse, så er der mange muligheder. Læs videre !!

Hvorfor bliver private computere hacket ?

Der er naturligvis en lang forklaring på den slags - så dette er den korte Pixibogs-version, som er nogenlunde til at forstå for de fleste (?) - det håber jeg i hvert fald.

Private computere bliver hacket, fordi det er nemt ! Alt for mange har slet ingen eller mangelfuld beskyttelse af deres computer med Internet-forbindelse. Derfor er de lette ofre.

Det er såmænd slet ikke en person, som sidder og udvælger netop DIG som offer. Det er oftest blot et computerprogram, som automatisk finder de lette ofre – dem som ikke har opdateret deres styresystem, deres antivirusprogram o.s.v.

I den lille sammenligning med fodboldstadion svarer maskingeværet til ... **ormevirus** spredes over hele verden til tilfældige menneskers computer. En orm kan f.eks. installere en skjult **bagdør** på computeren – også kaldet en "**trojansk hest"** – så fremmede kan fjernstyre computeren udefra og f.eks. opsnappe vigtige informationer vedr. netbank, pinkoder og passwords, som så automatisk sendes videre til bagmanden. En slags tyveri og svindel i Cyberspace.

Et formål med at hacke private computere kunne også være at overtage **kontrollen** med computeren og benytte den til at arrangere større angreb fra mange computere samtidig mod udvalgte mål ... De såkaldte "**Denial-of-Service**" (DoS) angreb, som kan lamme en webserver hos nogen, man gerne vil genere - f.eks. et firma, en politisk modstander eller en person.

Et andet formål er simpelthen at score din e-mail adresse og net-forbindelse, som så SÆLGES videre til folk, som udsender **SPAM** til sagesløse computer-brugere på Internettet. Og så breder det sig ligesom kædebreve - uden at folk ved noget eller gør noget. SHIT !! Eller din computer kan benyttes som udgangspunkt (base) for hacking af andre computere – så bagmanden slører sin egen identitet.

Et tredje formål kunne være at overtage **kontrollen med din harddisk** og evt. bruge den til at opbevare store mængder data, som andre så kan downloade hemmeligt. Det kunne være ulovligt materiale som musik, film, programmer, børneporno o.lign.

OBS: Alle disse ting kan stort set stoppes ved at installere en såkaldt **firewall** på computeren. Mere om det senere !!

Identitet og IP-adresser

Hvis man som privat person har en Internet-forbindelse med alm. modem, så betaler man typisk for det antal minutter, som man er koblet på nettet (online). Det betyder for de fleste, at man kun er koblet på, når det er nødvendigt (de fleste af os er vel lidt sparsommelige). Ellers bliver det simpelthen for dyrt.

Det betyder, at hackere kun har relativt kort tid til at "finde dig" og gøre et indbrud på din computer klar - og evt. finde ud af, om det er umagen værd at genere dig. Hvis du ikke er "online", så er der ingen umiddelbar risiko for fremmed indtrængen fra Internet !!

Din computer's identitet på Internet består af en såkaldt IP-adresse - på en måde kan man kalde det computeren's CPR-nummer eller "adresse", mens man er online på nettet.

Det fungerer på 2 måder: en dynamisk (skiftende) IP-adresse eller en permanent (fast) IP-adresse.

Hvis du har en forbindelse med **modem**, så får du automatisk tildelt en IP-adresse af din Internet-udbyder, når du kobler dig på nettet. Men det er blot en midlertidig IP-adresse - også kaldet en **dynamisk IP-adresse**. Næste gang du kobler dig på, så får du en anden adresse. Dette gør, at din identitet "sløres" for hackeren. Han har betydelig sværere ved at finde lige præcis DIG næste gang, fordi du "skifter adresse". Man er altså på en vis måde lidt anonym - i hvert fald statistisk set ...

Din Internet-udbyder har et vist antal IP-adresser, som kan deles ud til kunderne, mens de er online. Men der holdes 100% styr på, HVEM der har de forskellige adresser på et hvilket som helst tidspunkt, og disse oplysninger kan politiet f.eks. gøre krav på i efterforskning af mere alvorlige sager.

Hvis du har en "fast" forbindelse (f.eks. **bredbånd** med ADSL eller kabelnet), så får du oftest tildelt en **permanent IP-adresse**, som du altid kan identificeres på - den ændres altså ikke. Det betyder samtidig, at hackeren kan vende tilbage til dig, hvis han (jo, det er vist oftest hankøn) først een gang har fundet frem til dig og din IP-adresse - og evt. har fundet dig "interessant" at genere, misbruge eller udnytte økonomisk.

Dette sammenholdt med, at folk med bredbåndsforbindelse oftest er online i langt højere grad (det koster jo ikke ekstra at være "på" uafbrudt), gør dig til et langt mere udsat offer for hacking !! Der er trods alt forskel på, om man lader hoveddøren stå åben i 3 minutter - eller om man lader den stå åben, mens man er på ferie i 3 uger ...

OBS: I forbindelse med "traditionel hacking" gælder ovenstående naturligvis – men i forbindelse med truslen fra virus (som kan benyttes til at få adgang til ens computer), så er det lige meget, om man har den ene eller anden form for Internet-forbindelse. Bortset fra, at man måske er mindre "aktiv" på nettet med en langsom og dyr modem-forbindelse ...

Hvordan finder hackerne frem til os ?

Der er i dag 2 helt forskellige metoder:

- Visse hackere benytter sig at virus til at sprede og installere trojanske heste (bagdøre) på folks computer, så de kan overtage kontrollen
- De mere "traditionelle" hacker-metoder, som gennemgås herunder

Hackere benytter sig af særlige "værktøjer" (= computer-programmer) - og visse af disse programmer er lige så nemme at bruge som Word. Det kræver altså ikke nødvendigvis teknisk dygtighed for amatør-hackerne at bruge dem.

Det er som regel v.h.a. disse programmer, at tilfældige privatpersoner bliver hacket af en af de tusindvis af amatør-hackere: Først undersøger programmet automatisk et nærmere bestemt område af IP-adresser. En IP-adresse ser således ud: xxx.xxx.xxx.xxx - altså 4 gange 3 cifre (tal) eller f.eks. 217.254.083.371 (nullet foran 83 kan udelades).

Hvis der er respons på en eller flere IP-adresser, så laves der en såkaldt "**port-scanning**" på disse adresser for at se, om der skulle være en indgang (port), som står åben. Hvis der er det, så er hackeren ret let inde i systemet og kan evt. lave ravage, alt efter hvor dygtig han er. Porte svarer (lidt nemt forklaret) til forskellige typer "døre og vinduer", som computeren benytter til diverse former for data-trafik og processer.

Lad os lave en lille sammenligning for forståelsens skyld:
Hvis du nu var indbrudstyv i den virkelige verden, så ville du være glad for et "redskab" (f.eks. et computer-program), som automatisk kunne ringe op til alle telefonnumre indenfor et bestemt område (f.eks. i Valby). Nogle af telefonnumrene ville sikkert slet ikke være i brug, og på nogle af numrene var der optaget eller nogen tog telefonen. Men nogle steder var der bare ingen hjemme, så straks tager du (indbrudstyven) ud til adressen og checker, om der skulle være døre eller vinduer, som ikke er lukket og låst. Og det KUNNE jo godt være, at man havde glemt et eller andet, da man tog hjemmefra.

I dette tilfælde ville det være praktisk med en voldgrav rundt om huset fyldt med sultne krokodiller ... Tyvene ville ret hurtigt skride igen.

Firewall

En firewall svarer lidt til voldgraven med krokodiller :-)

En firewall er et program, som holder øje med al indgående og udgående datatrafik mellem din computer og netværket (i dette tilfælde: Internettet).

Når du har installeret din firewall, skal du altså lære den hvilke programmer, der gerne må få adgang til Internettet. Fidusen er, at krokodillerne kan ”opdrages”, således at de lader bestemte ting slippe ind og ud – f.eks. vil du jo gerne kunne sende og modtage e-mails og surfe på nettet, hvilket også er datatrafik ind og ud via din netværksforbindelse.

Hver gang et nyt program forsøger at sende eller modtage data, vil firewallen bede dig om at godkende eller afvise trafikken. Du kan bede firewallen om at huske dine valg (”Remember this setting” el. lign.), så du slipper for at tage stilling hver gang, du for eksempel bruger dit mailprogram eller vil kopiere noget tekst fra nettet over i Word..

En firewall fås enten som hardware eller som software. For privatpersoner er software-udgaven mest relevant og kan skaffes helt gratis !! (se sidste side)

En firewall som er indstillet korrekt vil opdage alle de primitive hackertyper - og det er ca. 99% af dem. De sidste 1% af hackerne kan man som privatperson ikke stille så meget op imod - men de er sikkert heller ikke interesseret i at hacke os "almindelige" mennesker. De går efter de "store fisk" - og selv CIA og FBI har faktisk haft besøg af hackere utallige gange. Deres websites har fået udskiftet forsiden af hackere, som griner af dem: "Tag Jer nu sammen" o.s.v. De ser kun en ægte udfordring i at snyde en firewall - og de har teknisk viden og kunne til at gøre det.

Social engineering er en metode, som visse hackere benytter for at skaffe sig adgang til et IT-system. Man udgiver sig f.eks. for at være fra IT-afdelingen el.lign. og beder en medarbejder om at udlevere sit brugernavn og password, fordi der er nogle problemer. Hvis det lykkes at **snyde** vedkommende, så kommer man jo pludselig inden for firewallen og kan foretage sig handlinger, som systemet opfatter som lovlige og udført af en godkendt bruger.

Botnet og zombie-PC'er

Når en computer er blevet inficeret med en trojansk hest er der skabt en "bagdør" på maskinen, som kan udnyttes af skumle personer udefra. En inficeret kaldes en "zombie-PC", fordi den opfører sig "spøgelsesagtigt" og kan fjernstyres af fremmede. Hvis en hacker har opnået kontrol med et meget stort antal computere på denne måde, så kaldes disse computer tilsammen for et "botnet" (forkortelse af robot-net).

Dette botnet kan nu misbruges til skumle og ulovlige formål: udsendelse af spam, DOS-angreb (denial-of-service), udgangspunkt for videre hacking m.v.

Det opdaterede **antivirus**-program vil oftest stoppe den slags, inden det kommer indenfor dørene. Og en korrekt installeret **firewall** vil stoppe den ulovlige (hemmelige) datatrafik.

Phishing

Phishing er endnu et forsøg på at **lokke** f.eks. en banks kunder til at opgive fortrolige oplysninger, herunder numre på bankkonti, betalingskort og koder.

Typisk modtager man en e-mail fra bagmændene bag svindelnummeret, hvor der omtales et eller andet problem med ens konto. Man skal så klikke på et link, som kan føre én over på en **falsk hjemmeside**, hvor man skal indtaste diverse fortrolige oplysninger vedr. kontoen, som herefter kan misbruges eller tømmes for penge.

Et andet trick er, at man ved at klikket på linket i mailen kommer til at installere en grim form for **spyware** på computeren, som automatisk finder frem til informationer om ens bankkonto/netbank. Og informationerne sendes derefter til bagmanden.

Phishing har i efteråret 2005 for første gang ramt svenske kunder i en stor nordisk bank. Problemet har indtil nu været størst i Brasilien og England, men har fået en vis omtale i danske medier i 2005, og det må forventes at dukke op i dansk sammenhæng i løbet af 2006.

En ormevirus i efteråret 2005 mindede lidt om det – masser af os modtog en mail fra FBI eller CIA, som påstod at vi havde foretaget os et eller andet, som skulle efterforskes. Mange blev noget forskrækkede over det, og klikkede uforsigtigt på den vedhæftede fil, som derefter installerede en trojansk hest og sendte sig selv videre via adressekartoteket i Outlook. Opdaterede antivirusprogrammer opfangede dog hurtigt disse mails, som man så bare kunne slette.

Rådet mod phishing er at udvise forsigtighed og være kritisk overfor den slags mails. Evt. kan man kontakte sin bank og spørge, om de har udsendt mails af den slags (hvilket de som regel ikke gør). Desuden vil et opdateret antivirusprogram samt et anti-spyware program som f.eks. Ad-Aware kunne hjælpe én. Men hvis man bliver ledt over på en falsk hjemmeside og indtaster fortrolige oplysninger, så er man lidt på spanden !! Så lad være med det ...

Kryptering og PGP

Kryptering betyder, at informationer og data ”kodes” (krypteres), så de bliver ulæselige/ubrugelige for personer, som ikke har lovlig adgang til dem. Til gengæld skal den korrekte modtager have en ”nøgle” som kan ”afkode” (de-kryptere) data, så de atter kan læses i normal form.

Kryptering kan være stærk (svært at bryde koden) eller svag (lettere at bryde koden). En stærk kryptering hedder i dag 128 bit, og det kræver betydelig computerkraft at bryde koden. I Outlook 2003 kan man faktisk kryptere indholdet i sine e-mails med 128 bit kryptering.

”Pretty Good Privacy” (**PGP**) er et af de kendte og gode programmer, som kan kryptere data. Det kan downloades på nettet, men den gratis version er en smule begrænset og kan ikke kryptere meget kraftigt. Så man må til lommerne, hvis man vil have den fulde version, som kan lave en meget kraftig kryptering. Programmet er fra USA, og i starten var det faktisk forbudt at eksportere programmet til andre lande, fordi det hindrede de amerikanske efterretningstjenester i at overvåge os – eller gjorde det meget besværligt i hvert fald. Men så slap det ud på Internet, og derefter var der ikke så meget at stille op. Man kan faktisk kryptere hele sin harddisk (eller dele af den), en diskette o.lign.

SSL (Secure Socket Layer) er en sikkerhedsstandard, som er indbygget i vores browsere. Teknikken benytter bl.a. kryptering ved overførsel af data. Det kan f.eks. være ved login på online-tjenester, e-handel, digital signatur m.v. Man kan se en lille "låst hængelås" nederst i browservinduet, når krypteringen er slået til – og webadressen skifter fra http:// til https://

Digital signatur

Digital signatur er ideen om, at man skal kunne "**skrive under** elektronisk og digitalt", så f.eks. dokumenter, kontrakter o.lign. kan gøres juridisk bindende.

Meningen er f.eks., at man skal kunne **legitimere sig** overfor bl.a. offentlige websites som "Told & Skat", kommunen, hvor man som borger kan lave forskellige former for selvbetjening. Endvidere sikrer brugen af den digitale signatur, at indholdet ikke bliver ændret/forvansket undervejs i dataoverførslen.

Digital signatur benytter sig naturligvis i høj grad af stærk kryptering, og den "officielle" digitale signatur leveres i Danmark af TDC. Mange banker har imidlertid udviklet deres egen digitale signatur bl.a. til brug ved netbank.

Brugeradgang og adgangskoder (passwords)

Mange steder skal man "logge på" med brugernavn og adgangskode (password). Brugernavnet er tit ret let at gætte sig frem til – så adgangskoden skal derfor være rimelig sikker, hvis man vil undgå, at fremmede personer uden lovlig adgang til systemet kan komme ind. Det kan være netværket på skolen eller arbejdspladsen – eller adgang til netbank eller selve ens egen computer.

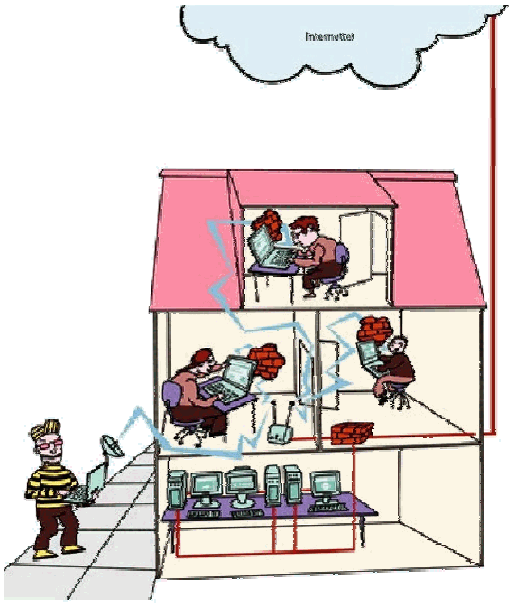
Brugerens **login** giver ligeledes nogle bestemte rettigheder og muligheder på systemet f.eks.:

- hvilke programmer, man har adgang til at benytte
- om man har mulighed for at downloade og/eller installere nye programmer
- hvilke områder (drev, mapper og filer) man har adgang til og hvilken type adgang, man har. Læseadgang (man kan kun kigge men ikke ændre) – skriveadgang (man kan både kigge, ændre og gemme) – eller måske slet ingen adgang.

Sikkerhed i trådløse netværk (WLAN)

Et trådløst netværk (WLAN = Wireless Local Area Network) transporterer data via "radiobølger" i stedet for kabler. Og det er jo smart, at man ikke behøver at trække kabler, men samtidig betyder det en øget **risiko** for, at uvedkommende får adgang til netværket.

Der er alle de sædvanlige fordele (og ulemper) som ved netværk i al almindelighed: man kan deles om data, internetforbindelse, printer m.v.



Radiobølgerne sendes ud fra en basisstation (også kaldet "access point") og kan modtages af computere, som indeholder et "trådløst netkort", og det gør f.eks. alle bærbare computere, som bliver solgt i dag. Og man kan naturligvis også sende tilbage til basisstationen.

Rækkevidden er typisk mellem 50-100 meter og stoppes ikke af mure eller hegn, selvom den slags godt kan nedsætte rækkevidden.

Der er forskellige **standarder** indenfor trådløs data-overførsel, og udviklingen vil gøre, at der kommer nye til. I øjeblikket benyttes hovedsageligt 2 standarder:

- **802.11b** som er en ældre standard med mindre rækkevidde, hastighed og understøtter kun den ældre (svagere) WEP-kryptering
- **802.11g** som er nyere og med forbedringer: større rækkevidde, højere hastighed og understøttelse af stærkere kryptering: WPA og WPA2

Det bedste er naturligvis at anskaffe udstyr, som understøtter BEGGE standarder.

Den øgede risiko består i, at uvedkommende måske også kan modtage radiobølgerne og således "benytte ens internetforbindelse" (hvorved hastigheden falder) og evt. "hacke sig ind" på ens personlige område og stjæle eller ødelægge data.

Det er man naturligvis ikke interesseret i – og derfor må man være på vagt og **aktivt** tage visse forholdsregler, når man installerer sit trådløse netværk. Det er nødvendigt med det lille private netværk derhjemme – og det er nærmest livsnødvendigt, hvis det handler om virksomhed med masser af følsomme og værdifulde oplysninger, som ikke må falde i de forkerte hænder !!

Gode råd vedr. sikkerheden i trådløse netværk?

- Brug kryptering (WEP eller WPA)
- Slå broadcast-meddelelser fra
- Skift standard passwordet på basisstationen
- Skift SSID
- Brug en firewall
- Brug filtrering på MAC-adresser
- Vær opmærksom på persondatalovens bestemmelser, hvis du håndterer personfølsomme data f.eks. i et firma eller en forening !

Fagudtryk vedr. trådløse netværk:

- SSID: Service Set Identifier (navnet på et trådløst netværk – som regel kan man selv bestemme navnet)
- Broadcast-meddelelse: Information fra et trådløst netværk om navnet på det trådløse netværk (SSID), datahastighed og kryptering.
- WEP: Wired Equivalent Privacy er den krypteringsprotokol, der bruges i de fleste ældre trådløse netværk af typen
- WPA og WPA2: Wi-Fi Protected Access - nyere krypteringsstandard, der anvender dynamiske nøgler og er langt mere sikker end WEP-standarden
- MAC-adresse er et unikt identifikationsnummer på det trådløse netkort. Hvis man kun tillader adgang for bestemte MAC-adresser, så er man vældig godt beskyttet mod fremmedes indtrængen på netværket.
  PS: Det har altså intet at gøre med ”Mac-computere” ...
- VPN: Virtuelt Privat Net - en tjeneste, som laver en virtuel (kunstig) datatunnel fra punkt til punkt for de tilsluttede brugere, så uvedkommende ikke lige kan ”komme ind”
- Wi-Fi: blot en anden betegnelse for trådløse netværk

Checkliste mod hackerproblemer

- Hackere benytter sig ofte af de såkaldte ”trojanske heste” til at få adgang til din computers harddisk. Ved at holde sig opdateret imod virus, så hjælper det faktisk også mod hacking, idet disse ting ofte spredes v.h.a. ormevirus.

- Hvis du er meget på nettet – eller f.eks. har en fast forbindelse (med fast IP-adresse), så bør du afgjort installere en såkaldt **Firewall**. Det er et program, som fungerer som en slags pas-kontrol mellem Internettet og dit eget system.

- Sørg for at sætte dig lidt ind i, hvordan din Firewall fungerer, og indstil den korrekt. Tillad kun trafik, som du er helt sikker på !

- Firewall’en skal ligesom antivirusprogrammer opdateres en gang i mellem. Visse programmer kan gøre dette automatisk. Jeg kan varmt anbefale ”Zone Alarm” som (for private brugere) kan hentes gratis på nettet (www.zonelabs.com).

- Trådløse netværk bør sikres som beskrevet på foregående side. IT- og Telestyrelsen har udgivet et par glimrende gratis foldere om problemerne – og de kan også hentes på nettet: www.it-borger.dk > Sikkerhed

- Lad være med at sløse med personlige oplysninger og adgangskoder. En god adgangskode indeholder både små og store bogstaver samt tal. Og den bør indeholde mindst 8 tegn.

Her er en Top-10 over de DÅRLIGSTE passwords, du kan finde på:

- Ingenting (= intet password)
- Password (altså ordet ”password” som kodeord)
- Navnet på dit barn eller din kæreste/kone (eller tæt familie)
- Navnet på dit kæledyr (”Pusser” eller ”Trofast”)
- En tegneseriefigur, fodboldhold, spiller, popstjerne o.lign.
- Dit stjernetegn (eller din kones stjernetegn – det er let at finde frem til)
- Bandeord eller ”frække ord”
- Science fiction – eller fantasyfigur
- Firmanavn o.lign.
- Fødselsdatoer og telefonnumre

Afbryd din net-forbindelse, hvis du ikke skal bruge den. Blot fordi du har en fast forbindelse (til fast og billig pris), så behøver hele butikken jo ikke stå åben døgnet rundt !! Hvis du ikke er online – så er der lukket for hackere o.lign.

Overvågning

Overvågning er mange ting. Vi kender den slags, som foregår med **videokamera** på offentlige eller private steder (f.eks. i virksomheden, i Seven-Eleven kiosken eller hjemme i indkørslen). På private steder skal der være tydeligt skiltning om, at der er videoovervågning.

I dag kan man overvåge et område via satellitkamera eller fra fly ... men det er stort set kun militære myndigheder og efterretningstjenester, der har adgang til den slags. Og de skilter ikke med det ...

Rocker-krig, terrorisme og "11. september" har øget ønsket om at kunne overvåge visse grupper uden at skulle have en dommerkendelse først.

Overvågning privat

Alle de nye digitale former for kommunikation kan meget let overvåges med de rette programmer og tilstrækkelig computerkraft. Telefoner, mobiltelefoner, e-mail, Internet-surf, fax-beskeder m.v. kan overvåges/aflyttes og gemmes, men det er der naturligvis en masse love og regler om. Det er ikke tilladt at foretage denne form overvågning/aflytning, med mindre myndighederne har kraftig mistanke om noget kriminelt og er i gang med en vigtig efterforskning.

Rockerloven og Terrorloven i Danmark
Den danske regering har de senere i flere omgange skærpet lovene, straffene og mulighederne for overvågning i det danske samfund i forbindelse med kriminelle grupper af forskellig slags og IT-kriminalitet i det hele taget.

I slutningen af 2006 var der bl.a. forslag fremme om at forbyde mobiltelefoner med taletidskort, fordi man ikke kan identificere folk, som benytter disse. Man kan sagtens aflytte telefonen, men man kan ikke spore, hvem der ejer den. Du kan finde det sidste nye via min hjemmeside.

Echelon
Globalt overvågningssystem styret af UKUSA-landene (Storbritannien, Australien, Canada, New Zealand og USA) – men helt klart med USA som "generalen". Der har været megen debat om Echelon, idet der har været utallige afsløringer af ulovlig overvågning af firmaer, borgere, politikere o.s.v.

Det er et omfattende emne at beskrive, så her henvises ligeledes til min hjemmeside, hvor der er yderligere information samt links til spændende artikler m.m.

Overvågning på jobbet

Det er alt for nemt at overvåge medarbejderes mails, data og telefonsamtaler på jobbet. Det mener flere fagforeninger og eksperter, som advarer mod de nye teknologiske overvågningsmuligheder og efterlyser lovgivning på området, fordi medarbejdernes retssikkerhed er truet.

”Den teknologiske udvikling gør, at der er brug for meget klare retningslinier for, hvad man må og ikke må. Lige nu er det en jungle, og det må både være i medarbejdernes og virksomhedernes interesse, at der bliver strammet op,” siger advokat i hovedorganisationen FTF, Helle Bang Hjort.

Som et eksempel på en ny teknologisk overvågningsmulighed fremhæver IT-fagforeningen Prosa den slags software, der kan omsætte tasteklik til ren tekst – også kaldet tastatur-loggere.

”De nye programmer læser alt, hvad dit tastatur laver, så de er giftige. De giver chefen entydig adgang til data, som læses udenfor sammenhæng og uden, at den ansatte har mulighed for at give sin version. Det er helt urimeligt,” siger Hanne Lykke, som er faglig sekretær i Prosa.

Ikke engang med en Hotmail-konto kan man altså holde sine mails hemmelige længere.

Ifølge Martin Gräs Lind, som er forsker ved Århus Universitet, har der inden for det seneste år været flere eksempler på fyringer, der ligger på kanten af, hvad der er lovligt. Han efterlyser en klarere lovgivning på området, fordi sager om elektronisk overvågning i øjeblikket både kan behandles i persondataloven, straffeloven, erstatningsansvarsloven og funktionærloven.

”Man kan ikke klart og præcist sige, hvor grænsen for overvågning går, og det er et problem for retssikkerheden. I stedet bruger man en blanding af 10 forskellige retskilder, som man skal forholde sig til. Det ville være meget bedre med en samlet lov,” siger Martin Gräs Lind, som har lavet en ph.d.-afhandling om emnet.

Dansk Arbejdsgiverforening mener (ikke overraskende), at problemerne er overdrevne, og derfor mener organisationen ikke, at der er brug ny lovgivning på området ... så de lurer videre.

Som reglerne er p.t. så må arbejdsgiveren nemlig gerne kigge den ansatte over skulderen – hvis bare han fortæller de ansatte, at han gør det. Dog må man ikke lure i private mails, hvis det tydeligt fremgår, at de er private.

På den anden side er det vel lidt svært at argumentere for, at man har lov til at bruge tid på at skrive private breve og surfe privat i arbejdstiden – bare fordi det foregår på computeren ... Måske bør man hellere kæmpe for at have privatlivet i fred ... derhjemme !!

Industri-spionage

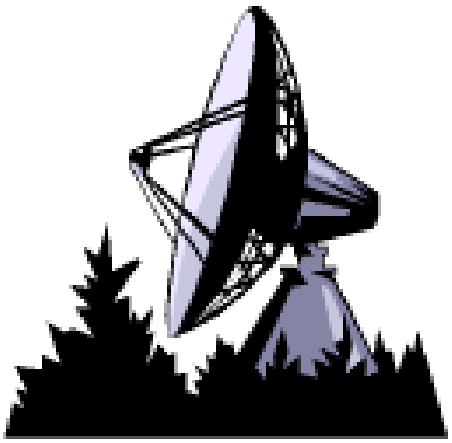
Viden udgør i dag et fundamentalt grundlag for enhver virksomhed – og viden er derfor en attraktiv vare på det illegale marked. Det kan skade en virksomhed alvorligt, hvis konkurrenter eller kriminelle skaffer sig fortrolige oplysninger om et firma.

To tredjedele af de anmeldte sager om industrispionage i Danmark bliver aldrig efterforsket, fordi politiet og anklagemyndigheden vurderer, at efterforskning ikke vil kunne føre til domfældelse. Og de få sager, der bliver efterforsket, fører kun sjældent til dom. Det oplyser foreningen Dansk Industri.

Retsreglerne er blevet strammet op med loven mod IT-kriminalitet (2003), så industrispionage nu kan give op til seks års fængsel. Det er en klar overtrædelse af markedsføringsloven, hvis man skaffer sig information på uærlig vis. Og det er strafbart, hvis man bruger informationen på anden måde, end den oprindelig var tiltænkt af virksomheden.

Faktisk er det sådan, at en medarbejder har tavshedspligt i tre år efter et ansættelsesstop. Ikke desto mindre føler mange ansatte, at de har en form for ejendomsret over projekter eller systemer, som de selv har været med til at lave, og derfor har de ingen samvittighedskvaler, når de stjæler følsomme oplysninger fra deres arbejdsplads.

Målet er, at politiet i fremtiden behandler det mere kvalificeret, end de gør i øjeblikket. I dag er det sådan, at sagerne kun lægges over til Politiets Efterretningstjeneste, hvis man har en mistanke om, at fremmede magter er involveret. Man så gerne, at denne type sager altid blev behandlet af efterretningstjenesten.



Der er klare beviser for, at Echelon-systemet er blevet brugt til at lave industri-spionage til fordel for amerikanske virksomheder ...

Back-up (sikkerheds-kopiering)

”Rigtige mænd tager ikke back-up. Rigtige mænd græder,” lyder en motto i IT-verdenen. Når projektopgaven eller salgsopstillingen ligger på en PC, der pludselig ikke kan startes, så opdager man, hvor nyttig og værdifuld en sikkerhedskopi ville have været, hvis man ikke har nogen ...

Det er for sent at tænke på sikkerhedskopier, når uheldet først er ude. Så brug lidt tid på det, mens dine data og e-mails stadig ligger trygt og godt på PC'en.

Gem dine data
Som regel vil det være vigtigst at få lavet back-up af sine **datafiler**:

- breve, opgaver, billeder, regneark og andre vigtige dokumenter
- filer med ”Foretrukne” bogmærker
- filer fra Outlook med alle ens e-mails, kalender og adresse-kartotek
- evt. skabeloner
- evt. drivere til div. hardware.

Selve programmerne kan som regel genskabes ud fra de CD'er, de blev leveret på. Dog kan der være særlige indstillinger og skabeloner, der går tabt, hvis man ikke finder frem til dem og tager kopi af dem også. Men ellers handler det primært om at sikre de data, man selv har skabt.

Gem på disk, bånd eller andet
Dokumenterne ligger formentlig på den harddisk, som er indbygget i PC'en, og det næste spørgsmål bliver så, hvor man skal gemme sin sikkerhedskopi.

Normalt vil man vælge at tage sikkerhedskopi på et medie, der kan fjernes fra pc'en. På den måde kan man sikre tingene, selvom PC'en skulle blive stjålet eller inficeret med virus. Der er flere muligheder:

- Disketter (hvis der kun er tale om mindre mængder – men disketter kan som bekendt ikke indeholde ret meget)
- USB-nøgle (fås op til 2 GB plads)
- CD-ROM (op til 700 MB pr. CD) eller DVD som kan indeholde over 6 gange mere)
- Ekstern harddisk (kan fås til under 700 kr med 40 GB plads og nem tilslutning til USB-stikket)
- Tape-streamer (hvis der er tale om meget store mængder data)
- Opbevaring på en web-server på Internettet

Hvis man skal gemme data i flere år, skal man være opmærksom på holdbarheden af det medie, man gemmer dem på. Brændbare CD'er kan for eksempel blive ødelagt, hvis de ligger for varmt eller udsættes for sollys. I øvrigt har forsøg vist, at de går i opløsning efter en årrække – de holder ikke evigt. En mulig løsning er at finde kopierne frem efter 2-3 år, kopiere dem ind på harddisken og brænde en ny CD med dem.

Hvor ofte tages back-up ?
Man kan vælge at bruge styresystemets indbyggede program til at tage kopier af mapper og filer. I Windows XP ligger det under Programmer > Tilbehør > Systemværktøjer > Sikkerhedskopiering.

Men der findes også særlige programmer til sikkerhedskopiering. De gemmer data i en enkelt fil, som er komprimeret, så data fylder mindst muligt.

Jo nyere en sikkerhedskopi er, desto mere er den værd. Derfor er det en god ide at sætte sikkerhedskopieringen til at foregå med jævne mellemrum f.eks. en gang om måneden hjemme i privaten. Men det afhænger naturligvis af, hvad man bruger PC'en til – og hvor meget man bruger den. Under alle omstændigheder så er data, som er skabt *efter* sidste back-up, i farezonen ...

Back-up i virksomheder
Her er det utrolig vigtigt at have en back-up af alle vigtige data, som er så ny som muligt. Der er eksempler på, at firmaer har måttet lukke helt, fordi f.eks. kundedatabase el.lign. var gået tabt p.g.a. hardware-nedbrud, brand, virus eller hackerangreb ...

Virksomheden er derfor nødt til at have en seriøs "back-up politik", som sikrer, at det kun er MEGET få data, der går tabt, hvis uheldet er ude. Det er vigtigt at have en fast **procedure** for:

- hvem der tager back-up
- hvor ofte der tages back-up
- hvad der skal tages back-up af
- hvordan back-up'en gemmes

Her kommer en af fordelene ved netværk ind i billedet, idet man evt. kan nøjes med at tage fuld back-up af ét eller flere **netværksdrev** på serveren, frem for at skulle tage back-up på en masse forskellige computere hver for sig ... Som regel er det en IT-ansvarlig eller IT-afdeling, som har ansvaret for disse opgaver.

Lovgivning, kontrol og politi

Hos Rigspolitiet bekræfter man, at antallet af **anmeldelser** om IT-kriminalitet fra virksomheder er stigende. Og man har indenfor de sidste par år fordoblet mandskabet bl.a. med civile eksperter i kampen for "cyber-kriminalitet".

Den danske afdeling af CERT (www.cert.dk) spiller også en betydelig rolle sammen med flere forskellige IT-sikkerhedsfirmaer. Større sager kan endvidere overdrages til PET (Politiets Efterretningstjeneste) samt FE (Forsvarets Efterretningstjeneste) – sidstnævnte hovedsagelig, når der er tale om udenlandske kriminelle, som direkte truer rigets sikkerhed.

Også på EU-plan forsøger man hele tiden at øge samarbejdet og harmonisere (og skærpe) lovgivningen omkring IT-kriminalitet – også set i lyset af den internationale terrorisme.

Dansk lov om IT-kriminalitet blev i 2005 skærpet og udvidet – og ideerne omkring div. elektronisk overvågning/aflytning er kraftigt voksende.

I Danmark benyttes i forbindelse med **virus** samt **hacking** især §263 (om brevhemmelighed og private gemmer) og §291 (hærværk) i Straffeloven. Straframmen går fra bøde til max. 6 år samt evt. konfiskering af IT-udstyr og erstatning til skadelidte personer eller firmaer. (se evt. www.stophacking.dk)

I forhold til udsendelse af **spam** benyttes især Markedsføringsloven §6a – og som tidligere nævnt kan man videresende spam fra danske spammere til Forbrugerombudsmanden (dansk@spamklage.dk), som så vil tage sig af sagen. Adskillige danske spammere har fået store bøder op til ½ million kroner.

Udbredelse af **piratkopiering** dømmes naturligvis iflg. loven om ophavsret. I Danmark findes en forening kaldet Anti-Piratgruppen (www.antipirat.dk), som driver en form for klapjagt på folk, som piratkopierer musik, film, software m.v.

Indsamling og håndtering af **personoplysninger** ligger naturligvis under Persondataloven, og tilsyn/kontrol varetaget af Datatilsynet (www.datatilsynet.dk).

Alle gældende danske love kan ses på nettet på www.retsinfo.dk

Fremtiden ??

Ifølge beregninger fra det amerikanske forbundspoliti, FBI, kostede IT-kriminalitet som f.eks. virusangreb, spyware og tyveri af computere de amerikanske virksomheder hele 413 milliarder kroner sidste år.

Den mest dramatiske udvikling er ikke fremkomsten af nye og mere avancerede internet-virus, men snarere at bagmændene ikke længere er private PC-entusiaster, men organiserede kriminelle bander.

Preben Andersen fra DK-CERT mener, at det især er professionelle kriminelle, der foretager elektroniske indbrud på computere:

”De forbrydelser, der før skete i den fysiske verden, sker nu i den elektroniske verden. Og derfor ser vi et opsving i kriminaliteten”.

Han peger på de såkaldte botnet, hvor hackere skaffer sig kontrol over tusindvis af computere, der f.eks. kan misbruges til udsendelse af spam eller til at bombardere firmaers hjemmesider med data og dermed blokere dem, hvis ikke firmaet betaler ”beskyttelsespenge” til hackerne.

Vi vil se, at spam og virus smelter mere sammen og låner metoder fra hinanden.

Man kan også frygte en form for Cyber-terrorisme, hvor en enkelt person vil kunne udrette frygtelig stor skade – ikke med våben eller gift … men blot med en computer med adgang til Internettet.

Vi har alle et ansvar at leve op til, hvis ikke det hele skal køre af sporet !!

:-) Søren Noah (IT-lærer) Febr. 2006

Links & kilder

Gode links til mere viden

- Min egen IT-hjemmeside med en masse links til **programmer** og yderligere **informationer** m.m. http://forum.brock.dk/noah
- Masser af letforståelig information om IT-sikkerhed: www.it-borger.dk

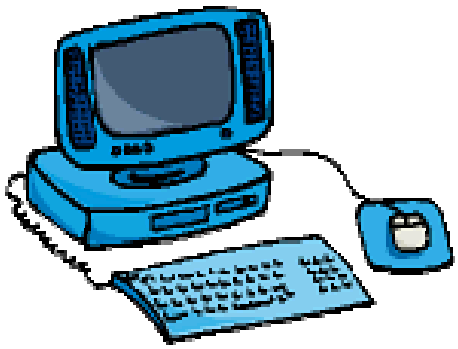
- IT- og Telestyrelsen: www.itst.dk

- Rådet for IT-sikkerhed (som faktisk er nedlagt ultimo 2005, men der ligger en masse gode informationer på websitet) www.rfits.dk

- God gennemgang af firewalls og ordforklaring: www.rfits.dk/fileadmin/public/Billeder/firewall/

Kilder

http://sikkerhed.tdconline.dk (TDC)
www.itst.dk (IT- og Telestyrelsen)
www.rfits.dk (Rådet for IT-sikkerhed)
www.it-borger.dk (offentlig IT-information til borgerne)
www.politi.dk
www.tiscali.dk
www.comon.dk
www.computerworld.dk
www.hotstart.dk/netmag
www.ftf.dk
www.csis.dk
www.cert.dk



Magasiner m.v.

Alt om Data
PC-Planet
Komputer for alle
Computerworld
Politiken
Hæftet "IT-sikkerhed" (forlagt Libris, 2003)