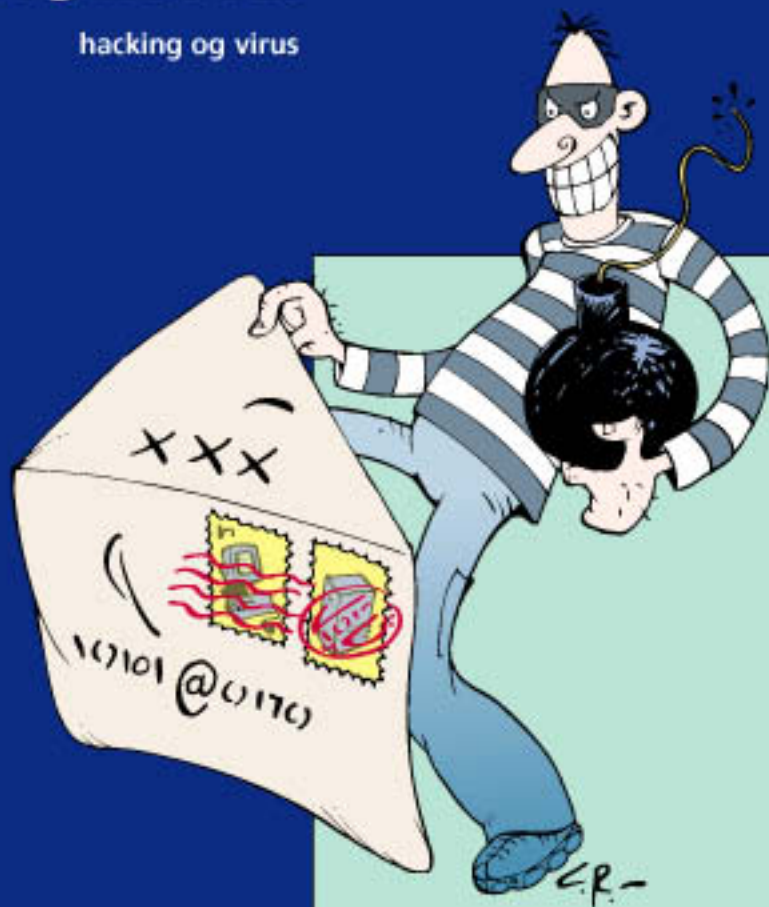


Sikkerhed ved e-post og Internet

hacking og virus



Sikkerhed ved e-post og Internet

hacking og virus

IT-Sikkerhedsrådet
Marts 2001

Sikkerhed ved e-post og Internet

hacking og virus

Publikationen kan rekvireres gratis så længe lager haves ved henvendelse til:

Statens Information

Postboks 1300

2300 København S

Tlf. 3337 9228

Fax 3337 9280

E-post sp@si.dk

Publikationen kan også hentes på

IT- og Forskningsministeriets hjemmeside

<http://www.fsk.dk>

ISBN (Internet): 87-90890-51-5

Udgivet af:

IT-Sikkerhedsrådet

c/o IT- og Forskningsministeriet

Bredgade 43

1260 København K

Tlf. 3392 9700

Fax 3332 3501

E-post fsk@fsk.dk

Illustrationer: Lars Refn

Tryk: K. Larsen & Søn A/S

Oplag: 4.000

ISBN: 87-90890-50-7

FORORD

Erfaringen har vist, at nogle af de største trusler mod IT-sikkerheden skyldes manglende kendskab til de relevante risici. Det sås for eksempel i foråret 2000, da alverdens computere blev ramt af en destruktiv computer-virus, der forklædt som et kærlighedsbrev satte en storm af falske „kærlighedsbreve“ i omløb: Talrige mail-servere gik ned, og både private og professionelle IT-brugere måtte afholde store afhjælpningsomkostninger. Senest er en ny heftig virus under navnet „Anna Kournikova.jpg.vbs“ sat i omløb. Filen indeholder ikke et billede af tennisstjernen, men derimod en såkaldt „orm“, der spredes via Microsoft Outlook postsystemet med overbelastning og risiko for nedbrud til følge.

De gerningsmænd, der frembringer den slags vira med videre, vil nok til stadighed have held til at finde nye „huller“ til deres formål. Derfor er det næppe realistisk at tro, at trusler af denne art vil forsvinde i nær fremtid. I første række må risiciene søges undgået ved, at den enkelte bruger gør sig mindre sårbar.

Med denne lille vejledning håber IT-Sikkerhedsrådet at kunne bidrage til dette forebyggende arbejde. Vejledningen forklarer, hvordan man som privat eller professionel bruger kan begrænse risikoen for hacking og virus når man bruger e-postprogrammer og Internet-browsere.

IT-Sikkerhedsrådet har udarbejdet vejledningen under medvirken af konsulentfirmaet SITICOM Group/Fischer & Lorenz og Bech-Bruun Dragsted, advokatfirma.

København, marts 2001

Mads Bryde Andersen
Professor, dr.jur.
Formand for IT-Sikkerhedsrådet
mads.bryde.andersen@jur.ku.dk

INDHOLD

- 3 **Forord**
- 7 **Indledning**
- 9 **Er din computer „inficeret“?**
- 13 **Er der „huller“ i din computer?**
- 15 **Åbner du ukritisk alle dine e-post-meddelelser?**
- 19 **Surfer du med en åben computer?**
- 23 **Lukker du selv tilfældige programmer ind?**
- 25 **Har din computer programmer, der ikke bliver benyttet?**
- 27 **Har du en hjemmecomputer?**
- 29 **Hvorfor foretage sikkerheds-kopiering?**
- 31 **Sund fornuft og agtpågivenhed**
- 33 **Hvis uheldet er ude**
- 35 **Ordliste**

INDLEDNING

Internettet har ændret vores måde at kommunikere og søge information på. Brug af e-post og søgning på Internettet bliver stadig mere udbredt. I kølvandet på denne udvikling er der opstået risiko for hacker- og virus-angreb og systemnedbrud.

Langt de fleste risici af denne karakter kan fjernes eller reduceres ved en kombination af praktiske foranstaltninger, klare regler (IT-sikkerhedspolitik) og sund fornuft, herunder en smule skepsis.

Denne pjece giver en række gode råd om, hvordan du kan begrænse risikoen for hacking og virus ved brug af e-postprogrammer og Internet-browsere, det vil sige, når du sender og modtager e-post eller søger information på Internettet.

Pjecen omhandler kun det lille område af IT-sikkerhed, der er relevant ved brug af e-post og Internet. Det er til gengæld en vigtig del af IT-sikkerheden.

Pjecen indeholder en række tekniske ord og begreber og forudsætter derfor et vist kendskab til computere, for eksempel at du har bestået PC-kørekort eller lignende. Hvis du har et mere begrænset kendskab til computere, kan du bruge ordlisten bagest i pjecen.

Sikkerhed er meget mere end fornuftig brug af e-post og browsere. Det er blandt andet også installation af firewalls, adgangskontrol, logning, hemmeligholdelse af data, elektronisk signatur, kryptering med videre. Dette er ikke omtalt i pjecen. På www.forbrugersikkerhed.dk kan du søge mere information om sikkerhed ved brug af e-post og Internet.

Pjecen henvender sig til tre forskellige persongrupper:



Den **private bruger**, der har en computer i sit hjem, og som selv er ansvarlig for at installere og vedligeholde programmer.



Medarbejderen, der anvender en computer på sin arbejdsplads - og som typisk kun vil have ansvaret for selve brugen af programmerne og ikke disses installation - eller medarbejderen, der har en PC stillet til rådighed hjemme.



Den **IT-sikkerhedsansvarlige**, det vil sige den medarbejder, der har ansvaret for driften af IT-systemerne i virksomheden og sikkerheden i forbindelse dermed.

Det er forudsat, at virksomheden har en sikkerhedspolitik, der blandt andet definerer, hvilket niveau virusberedskab med mere virksomheden skal have. Uden en sikkerhedspolitik er det ikke klart, hvilket sikkerhedsniveau der ønskes. Sikkerhedstiltag bliver derfor noget mere tilfældigt uden et samlet mål. Har virksomheden ikke en sikkerhedspolitik, bør den få det. Inspiration kan hentes fra Dansk Standards anbefalinger - DS 484-1. Det tilrådes, at IT-sikkerhedspolitikken forankres i ledelsen og kommunikeres i klare budskaber til medarbejderne.

De råd og anvisninger, der gives i denne pjece, har i relation til medarbejderen og den IT-sikkerhedsansvarlige et generelt præg. For de virksomheder, der har formuleret en IT-sikkerhedspolitik, er det naturligvis denne, der skal følges. Pjecen er i disse tilfælde først og fremmest tænkt som et muligt bidrag til sikkerhedspolitikken.

ER DIN COMPUTER „INFICERET“?

Computervirus, trojanske heste, orme med flere er betegnelser for små programmer, der kan „inficere“ en computer. Programmerne er skabt for at genere eller ødelægge andre programmer eller data på computeren. Kun yderst sjældent kan de ødelægge selve computeren. Men at få ødelagt programmer og data kan i sig selv være alvorligt.

Computervirus kan komme ind på en computer ad flere veje:

- Disketter, CD-ROM og lignende.
- E-post.
- Internettet (World Wide Web).
- Lokalt netværk.

Fra disketter og CD-ROM kan virus komme ind på computeren ved kopiering eller hvis computeren startes med en diskette i drevet, og drevet „bootbart“ - eller autostart er slået til.

Via e-post kan computervirus komme ind på computeren som en vedhæftet fil eller som en macro i selve e-posten.

Surfer du på Internettet, kan virus komme ind på computeren med filer, der downloades.

Computervirus kan endelig komme ind på din computer fra kollegaer, hvis der benyttes fælles filer via et lokalnet.



For den **private bruger** er de tre første adgangsveje relevante. Risikoen for at få en computervirus på den måde kan reduceres betydeligt, hvis du installerer et såkaldt antivirusprogram. Antivirusprogrammet installeres normalt, så det starter automatisk, når du tænder for din computer. Når det først er installeret, sker der et automatisk check af alle nye filer, der kommer på computeren.

Antivirusprogrammer kan enten købes der, hvor du har købt din computer, eller hentes via Internettet. På Internettet findes en række antivirusprogrammer, der er gratis for private brugere, se for eksempel <http://www.tucows.dk>.

Antivirusprogrammer kontrollerer programfiler, dokumenter og e-post for virus. E-post kan sprede virus med stor hastighed. Eksempler på e-postvira er „Melissa“ og „I Love You“. „I Love You“ spredte sig på under et døgn til millioner af computere over hele verden.

Antivirusprogrammer kan typisk sættes op til at:

- advare brugeren og blokere adgang til virusinficerede programmer og dokumenter,
- advare brugeren og tilbyde at fjerne virusen eller blokere adgangen,
- automatisk fjerne virusen.

For den private bruger er den sidste mulighed i de fleste tilfælde den bedste.

Antivirusprogrammet bør opdateres mindst hver 14. dag, da der kommer flere nye vira hver dag. De fleste antivirusprogrammer kan sættes op til automatisk at opdatere sig selv via Internettet. Dette må klart tilrådes.

Ønsker du selv at foretage opdatering, eller er der en ny computervirus i omløb, som du ønsker at blive beskyttet mod, kan du foretage en manuel opdatering via Internettet. Antivirusprogrammets producent har typisk en hjemmeside, hvor de seneste opdateringer kan findes. Adressen på denne hjemmeside står normalt i antivirusprogrammet under „Hjælp“.



For **medarbejderen** gælder generelt de samme forholdsregler som for den private bruger. Antivirusprogrammet vil normalt være lagt på computeren af den IT-sikkerhedsansvarlige.

Opsætningen for medarbejderen vil ofte være, at brugeren advares og tilbydes, at virus fjernes, eller at adgangen blokeres. Herudover er antivirusprogrammet typisk sat op til at sende en besked til den IT-sikkerhedsansvarlige. Disse opsætninger må ikke ændres, idet de hjælper den IT-sikkerhedsansvarlige med at overskue de vira, der kommer ind i virksomheden.

Selvom du som medarbejder normalt har travlt, må den automatiske opdatering af antivirusprogrammet ikke slås fra, idet sikkerheden herved svækkes både for dig, dine kollegaer og virksomheden.



Den **IT-sikkerhedsansvarlige** skal sikre, at antivirusprogrammerne anvendes korrekt. For at minimere risikoen for virus, er det vigtigt, at alle arbejdsstationer og servere benytter et antivirusprogram. Kun på denne måde dækkes alle mulige adgangsveje.

Antivirusprogrammet på arbejdsstationerne bør konfigureres til at:

- advare brugeren,
- tilbyde at fjerne virusen eller blokere adgangen og
- sende en meddelelse til den IT-sikkerhedsansvarlige.

Dette sikrer dels, at brugeren bliver opmærksom på problemet, dels at den IT-sikkerhedsansvarlige får mulighed for at identificere kilden til virusen og få den fjernet.

Antivirusprogrammets virusmønstre bør opdateres mindst hver 14. dag, og når der kommer hurtigt spredende vira. De fleste antivirusprogrammer kan sættes op til automatisk at opdatere sig selv på faste tidspunkter. Dette er især tilrådeligt i virksomheder med konstant Internetadgang.

Det må anbefales, at medarbejderne ikke uden den IT-sikkerhedsansvarliges samtykke har tilladelse til at foretage ændringer i opsætningen.

Brug antivirusprogrammer og opdater jævnligt

Alle kan blive ramt af computervirus, uanset hvor korrekt man opfører sig, men med et opdateret antivirusprogram kan risikoen for at få virus reduceres til et minimum.

ER DER „HULLER“ I DIN COMPUTER?

Computerprogrammer bør vedligeholdes på samme måde som et hus eller en lejlighed. Fra tid til anden bliver der opdaget fejl eller uhensigtsmæssigheder i Internet-browsere, e-postprogrammer med mere, som en hacker - eller under tiden hjulpet af en virus - kan udnytte til at få adgang til computeren. Den slags uhensigtsmæssigheder kaldes ofte for sikkerhedshuller eller bare „huller“.

Når producenten af programmet bliver opmærksom på sådanne „huller“, laver producenten en såkaldt fejlrettelse.



Som **privat bruger** bør du mindst én gang om måneden kontrollere, om der er nye fejlrettelser til de programmer, der benyttes. Hvis du har en konstant Internet-forbindelse, eksempelvis en ADSL forbindelse, bør du overveje at kigge efter nye fejlrettelser oftere. Dette skyldes, at en konstant Internet-forbindelse øger risikoen for, at en hacker identificerer din computer.

For at hente og installere eventuelle fejlrettelser skal du gå ind på programproducentens hjemmeside. Nogle producenter har specifikke sider, der kun omhandler fejlrettelser og programopdateringer.

For Microsoft-produkter skal du bruge følgende adresser i din Internet-browser:

<http://www.windowsupdate.microsoft.com> og

<http://www.officeupdate.microsoft.com>

For Netscape er adressen:

<http://www.netscape.com>

For Corel er adressen:

<http://www.corel.com>

For Lotus er adressen:

<http://www.lotus.com>

Andre producenter har tilsvarende hjemmesider. Opdateringen foretages ved at følge de anvisninger, den enkelte producent giver.



Medarbejderen kan som hovedregel gå ud fra, at den IT-sikkerhedsansvarlige løbende vurderer, hvilke fejlrettelser der skal lægges ind i virksomhedens programmer.



Den **IT-sikkerhedsansvarlige** bør ugentligt checke, om der er kommet fejlrettelser/opdateringer til de programmer, der anvendes i virksomheden, herunder specielt e-post-programmer og Internet-browsere. For hver enkelt ny fejlrettelse bør den IT-sikkerhedsansvarlige aktivt tage stilling til, om det „hul“, fejlrettelsen lukker, er relevant for virksomheden eller ej. Hvis det er relevant, bør fejlrettelsen lægges ind hos alle brugere så hurtigt som muligt.

Foretag jævnligt fejlrettelser i de programmer, der er installeret

Der opdages hele tiden nye „huller“, som producenten efterfølgende forsøger at lukke med fejlrettelser. Hvis producenter anbefaler opdatering af et program med en fejlrettelse, bør fejlretning ske hurtigst muligt.

ÅBNER DU UKRITISK ALLE DINE E-POST-MEDDELELSER?

Der er grund til at være langt mere kritisk over for den e-post, du modtager, end over for almindelig brevpost. En forkert håndtering af e-post kan nemlig få alvorlige konsekvenser. Selv om langt hovedparten af den e-post, du modtager, ikke indeholder andet end de budskaber, afsenderen ønsker at give dig, er det en kendsgerning, at virus ofte spredes via e-post, og at e-post er en nem måde for en hacker at få adgang til din computer på.

Forudsætningen for at der kan komme virus på din computer er, at du åbner en e-post fra en hacker og aktiverer det program eller dokument, hackeren har medsendt. I sjældnere tilfælde kan det være nok blot at åbne selve e-posten, hvor en såkaldt macro kan udnytte en svaghed i e-postprogrammet. Dette var tilfældet med „I love you“-virusen. I nogle opsætninger var det dog nødvendigt at åbne den vedhæftede vbs-fil for at aktivere virusen.

Denne virus har netop vist, hvor farligt det kan være at åbne e-post selv fra kendte afsendere uden først at have henvendt sig til afsenderen for at høre, hvad den pågældende meddelelse indeholder. „I Love You“-virusen var en såkaldt „orm“, der spredtes fra et system til et andet gennem Microsoft Outlook postsystemet. Denne virus var særlig farlig, fordi afsenderen var kendt af modtageren. De fleste modtagere fattede derfor ikke mistanke og åbnede den tilsendte e-post.



Den **private bruger** kan begrænse risikoen for at få en „I Love You“-lignende virus ved altid at sammenholde meddelelsens overskrift med afsenderen. Hvis overskriften virker mistænkelig, eksempelvis fordi den er på et andet sprog end afsenderen normalt bruger, har en usædvanlig formulering eller et mistænkeligt indhold, bør du kontakte afsenderen (telefonisk eller i en **ny** e-post) for at høre, hvad meddelelsen indeholder.

Vedhæftede filer, (for tiden i langt de fleste tilfælde) med endelserne „.com“, „.exe“ eller „.vbs“ bør du være kritisk over for. Er der en fornuftig grund til, at afsenderen sender dig et program, som vil blive kørt på din computer, så snart du aktiverer det? Det er der sjældent, og som hovedregel bør du derfor ikke aktivere den vedhæftede fil.

Sørg for at dit e-postprogram ikke automatisk åbner din e-post, så snart den er modtaget. Hvis du bruger en „preview“-funktion, hvor en del af e-postens indhold bliver vist sammen med overskriften, åbner e-postprogrammet automatisk alle dine e-postmeddelelser. Denne „preview“-funktion bør du slå fra, så du ikke risikerer, at e-postprogrammet automatisk aktiverer et program med virus.

Op til jul sendes der mange elektroniske julekort via e-post. Langt de fleste af disse er harmløse, men der findes desværre også elektroniske julekort, der kan spolere juleglæden. Slæk derfor ikke på opmærksomheden over for elektroniske julekort, spørg for eksempel afsenderen i en **ny** e-post: „Jeg har fået et julekort, er det ok?“ og lad være med at åbne julehilsener fra afsendere, du ikke kender. Det samme gælder for de meget populære skærmskånere (screen savers).

Slet mistænkelig e-post (uden at gemme det under „slettet post“), hvilket i de fleste tilfælde kan ske ved at trykke på „Shift“- og „Delete“-funktionstasterne samtidig.

Den private bruger kan yderligere sikre sig ved at installere en såkaldt „privat firewall“, der slår alarm, hvis der automatisk aktiveres programmer på computeren. En privat firewall beskytter nemlig mod, at nye programmer uopdaget benytter Internet som adgangsvej. Herved vanskeliggøres det for en virus, at benytte computeren til at videresende sig selv, uden brugeren opdager det.

En privat firewall kan for eksempel være „ZoneAlarm“, der er gratis for den private bruger, men der findes også andre produkter på markedet, herunder hardwareløsninger. Spørg der, hvor du har købt din computer.



Medarbejderen skal være opmærksom på det samme som den private bruger. Hvis du modtager mistænkelig e-post, bør den IT-sikkerhedsansvarlige kontaktes. Som medarbejder skal du derudover huske, at e-post med advarsler om virusangreb generelt kun bør sendes videre til den IT-sikkerhedsansvarlige. Mange advarsler er „hoaxes“, det vil sige falske advarsler om virusangreb, der intet reelt har på sig. Disse falske advarsler kan udgøre mindst lige så stort et problem som rigtige virus. De belaster post-systemerne unødigt og forstyrrer alle virksomhedens medarbejdere, hvis de ukritisk videresendes til alle.



Den **IT-sikkerhedsansvarlige** bør konstant være opdateret om hvilke computervira, der spredes via e-post og advare medarbejderne mod at åbne sådanne. Foruden de tidligere nævnte filtyper „.com“, „.exe“ eller „.vbs“, skal den IT-sikkerhedsansvarlige være opmærksom på, at mange virksomheders edb-programmer kan afvikle macroer, der har andre endelser end de ovenfor nævnte. Den komplette liste er på mere end 120. Det er derfor nødvendigt, at den IT-sikkerhedsansvarlige holder sig løbende opdateret. Det bør være en del af IT-sikkerhedspolitikken, at medarbejderne har fået instruktion om kun at videresende advarsler mod computervirus til den IT-sikkerhedsansvarlige og at kontakte den IT-sikkerhedsansvarlige ved modtagelse af mistænkelig e-post.

Den IT-sikkerhedsansvarlige bør vurdere, om ulemperne ved at fjerne preview-funktionen for medarbejderne står mål med den risiko, der altid findes. Hvis ulemperne vurderes at være for store, bør det alternativt overvejes at installere „private firewalls“ på den enkelte PC.

Vær skeptisk og brug sund fornuft, før du åbner e-post og navnlig medsendte filer

Mange e-post virusangreb kan undgås med et godt antivirus-program. Væn dig til at sammenholde meddelelsens overskrift med afsenderen. Virker modtaget e-post mistænkelig, så lad være med at åbne den. Medarbejdere bør i disse tilfælde kontakte den IT-sikkerhedsansvarlige. De vira, der ikke automatisk opfanges af antivirusprogrammerne, vil oftest kunne undgås ved at være en smule kritisk over for den e-post, der modtages.

SURFER DU MED EN ÅBEN COMPUTER?

En Internet-browser er beregnet til at søge på forskellige hjemmesider på Internettet. For at gøre disse søgninger mere attraktive og mindske brugernes antal af indtastninger, er der indbygget en række hjælpeværktøjer til de forskellige Internet-browsere. Programmeringsværktøjer såsom JavaScript, Java, VBScript og Active X giver alle mulighed for, at en indehaver af en hjemmeside kan lave programmer, som, når du besøger sådanne hjemmesider, bliver kørt på din computer.

Hvad et sådant program kan, afhænger af hvad det er for et program. I de fleste tilfælde bliver sådanne programmer brugt til at lette brugernes søgning. Der er imidlertid også eksempler på, at programmerne har sendt kodeord eller andre hemmelige oplysninger til en hacker.

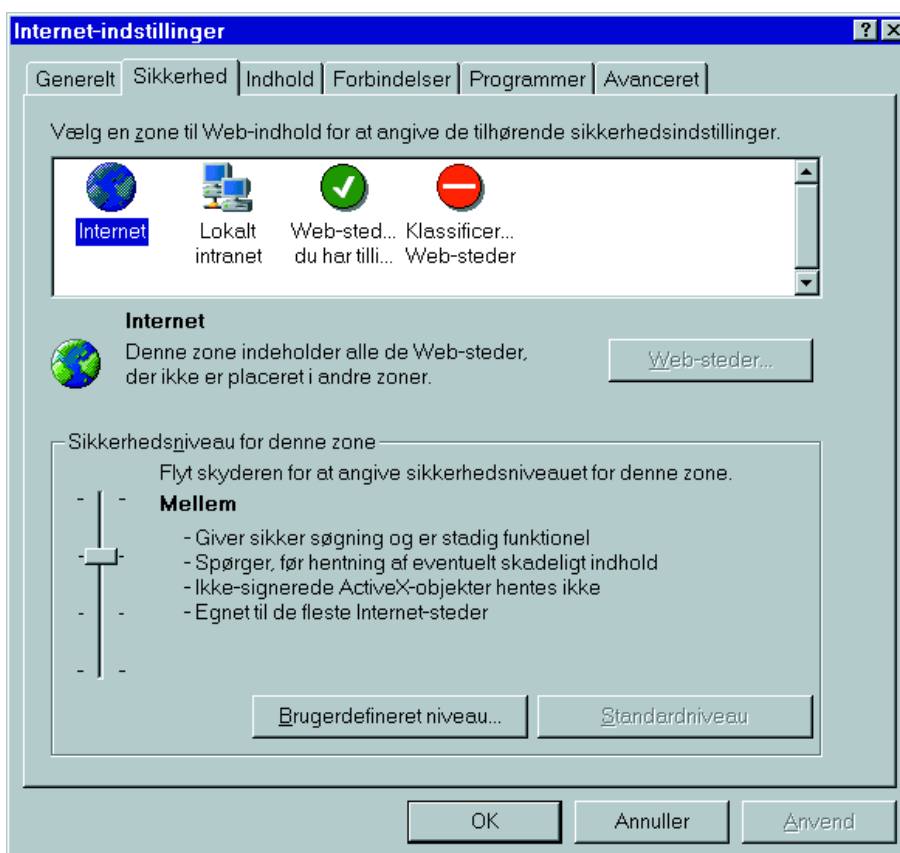
Java og Active X programmer kan underskrives af producenten med en elektronisk signatur, som sikrer, hvem programmet kommer fra. En sådan signatur sikrer ikke, at programmet er virusfrit, men du kan være sikker på, hvorfra programmet kommer.

Både Internet Explorer og Netscape kan sættes op, så de kun giver mulighed for at aktivere programmerne, hvis de er underskrevne.

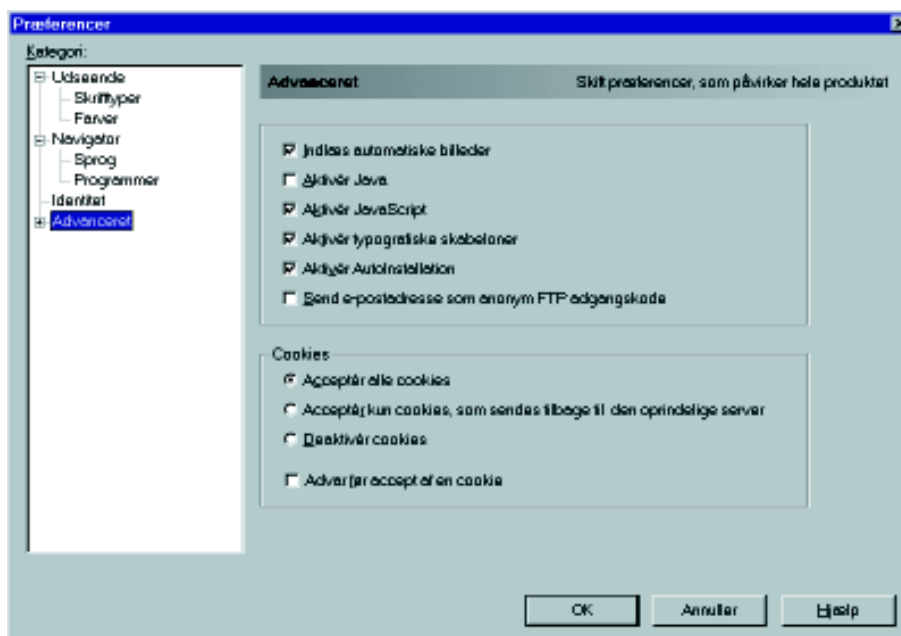


Den **private bruger** bør slå mulighederne for at køre disse programmer fra, med mindre de er underskrevne.

I Internet Explorer sker dette i „*Sikkerhed*“, som findes under „*Indstillinger*“ under „*Værktøjer*“ i menulinien. Sikkerhedsindstillingen skal sættes til „*mellem*“.



I Netscape sker dette i „*Avanceret*“, som findes under „*Præferencer*“ under „*Redigere*“ i menulinien. Der må ikke være mærke ved „*Aktivere JAVA*“.



Medarbejderen bør kunne gå ud fra, at den IT-sikkerhedsansvarlige har konfigureret Internet-browseren, så den svarer til det sikkerhedsniveau, der er gældende for virksomheden. Medarbejderen bør derfor aldrig ændre på sikkerhedsopsætningen i Internet-browseren uden først have fået den IT-sikkerhedsansvarliges tilladelse.

Vær opmærksom, når du surfer på Internettet. Mange hjemmesider bruger specielle browserudvidelser, såkaldte *plug-ins*, der giver mulighed for at vise forskellige former for film. Det kan for eksempel være Macromedia Shockwave eller Macromedias Flash player.

Hvis browseren har brug for en plug-in til at vise indholdet af en hjemmeside, og denne plug-in ikke er installeret på din computer, vil browseren spørge, om den nødvendige plug-in skal hentes og installeres

automatisk. Inden du svarer ja til dette, skal du indhente den IT-sikkerhedsansvarliges tilladelse.



Den **IT-sikkerhedsansvarlige** skal sikre, at den enkelte browser er konfigureret til det sikkerhedsniveau, som virksomheden har defineret som hensigtsmæssigt. Det vil normalt være det næsthøjeste niveau. Det højeste sikkerhedsniveau kræver, at der eksplicit åbnes for hver enkelt hjemmeside, som medarbejderen skal have adgang til. Dette er ikke overkommeligt i ret mange virksomheder, hvis Internettet skal være til nogen nytte.

Den IT-sikkerhedsansvarlige bør installere de mest almindelige plug-ins, således at medarbejderne kun undtagelsesvis får behov for at installere plug-ins. Herved øges forståelsen for, at medarbejderne skal indhente samtykke til installation af mere sjældent forekommende plug-ins. Denne procedure giver også den IT-sikkerhedsansvarlige overblik over mulige „huller“ i systemet.

Brug den opsætning (konfiguration), der passer til det ønskede sikkerhedsniveau

For alle gælder, at sikkerhedsniveauet ikke skal sættes højere, end at man kan få nytte af Internettet. Den nyttige del af Internettet er fuldt tilgængelig med næsthøjeste sikkerhedsniveau.

LUKKER DU SELV TILFÆLDIGE PROGRAMMER IND?

At installere programmer ukritisk på computeren, uanset hvor de kommer fra, svarer til at lukke en hvilken som helst person ind i sit hjem. Det går godt i de fleste tilfælde, men.... Der er selvfølgelig ingen, der ukritisk lukker hvem som helst ind i hjemmet. På samme måde bør du også være kritisk over for, hvilke programmer der installeres på din computer.

Du bør som udgangspunkt kun hente og installere programmer fra anerkendte forhandlere eller leverandørers hjemmesider.



Den **private bruger** bør ikke ukritisk tage imod programmer og dokumenter på disketter eller CD-ROM. Det er meget almindeligt, at der følger „gratis“ CD-ROM'er eller disketter med for eksempel computerblade. Du kan også opleve at modtage en CD-ROM som reklame. I de fleste tilfælde er sådanne programmer i orden, men der kan være undtagelser.

Et godt råd er at checke for virus og læse den medfølgende beskrivelse af programmerne, inden du begynder at installere sådanne programmer. Er der ingen beskrivelse af programmerne, bør du nøje overveje, om du vil løbe risikoen for, at der er virus i programmerne.



Medarbejderen bør ikke selv installere programmer på computeren, men bør overlade dette til den IT-sikkerhedsansvarlige. I arbejdsmæssige sammenhænge findes der en lang række relevante programmer på Internettet, ligesom forskellige forretningsforbindelser ofte tilbyder interessante hjælpeprogrammer på CD-ROM. Medarbejderen bør i disse tilfælde overveje, om programmet er en reel hjælp i arbejdet, og i så fald aftale med den IT-sikkerhedsansvarlige, hvorledes programmet bedst installeres.



Den IT-sikkerhedsansvarlige bør altid afprøve alle programmer, der skal installeres, i et „sikkert“ miljø, inden programmet installeres i netværket. Medarbejderne har ofte brug for specielle programmer fra Internettet eller leverandører i kortere eller længere perioder til specielle arbejdsopgaver. Den IT-sikkerhedsansvarlige bør give klare anvisninger på, af hvem og hvorledes sådanne programmer installeres på betryggende måde.

Installer kun programmer fra kilder, du stoler på.

HAR DIN COMPUTER PROGRAMMER, DER IKKE BLIVER BENYTTET?

Programmer, der ikke bliver brugt, kan sammenlignes med ekstra ubenyttede yderdøre i et hus. Mange yderdøre udgør altid en ekstra risiko, da de vil kunne bruges som adgangsveje for indbrudstyve.

På samme måde forholder det sig med ubenyttede programmer på en computer. Da alle programmer kan indeholde fejl af sikkerhedsmæssig betydning, er det klart, at du udsætter dig for en større risiko, jo flere programmer der er installeret.



Som **privat bruger** bør du fjerne de programmer, du aldrig bruger. Derved kan du formindske risikoen for hacking. De fleste programmer kan fjernes ved at foretage en afinstallering. I Microsoft Windows sker dette gennem kontrolpanelets ikon for tilføjelse/fjernelse af programmer.

Kan det ikke lade sig gøre den vej, kan du slette den programmappe, der blev oprettet, da programmet blev installeret.

Du skal dog ikke fjerne de programmer, du har behov for at bruge af og til blot for at formindske risikoen.



Som **medarbejder** bør du sikre dig, at den IT-sikkerhedsansvarlige fjerner programmer, der ikke længere benyttes, fra din computer. Specielt er dette vigtigt, hvis du til en specifik opgave har benyttet et specielt program gennem et stykke tid og nu ikke længere har brug for det.

Generelt bør du som medarbejder ikke selv fjerne programmer fra computeren. Kontakt i stedet den IT-sikkerhedsansvarlige.



Den IT-sikkerhedsansvarlige bør fjerne ubenyttede programmer fra servere og arbejdsstationer. Dels udgør de en sikkerhedsrisiko, da der normalt ikke foretages opdateringer af dem, dels tager de unødigt lagerplads.

Der findes en række driftsværktøjer, der kan foretage en løbende måling af, hvor meget de enkelte programmer anvendes. Disse værktøjer er også anvendelige til at konstatere, hvorvidt et program overhovedet anvendes. Et program, der ikke er blevet anvendt i et år, bør fjernes, da du i så fald typisk kan gå ud fra, at der ikke er egentligt behov for programmet.

Fjern overflødige programmer

Fjern eventuelt programmer, der ikke længere anvendes. De fylder og udgør en mulig sikkerhedsrisiko.

HAR DU EN HJEMMECOMPUTER?

Med en hjemmecomputer menes her en computer, der er koblet op mod arbejdspladsens netværk via telenettet. I de fleste tilfælde er hjemmearbejdspladsen stillet til rådighed for en medarbejder af en virksomhed, men benyttes ofte af hele familien.



Den **private bruger**, der benytter en medarbejders hjemmecomputer, bør være opmærksom på, at medarbejderens virksomhed typisk har regler for brugen af hjemmecomputeren. Sådanne regler skal efterleves.



En **medarbejder** med en hjemmecomputer skal være opmærksom på, hvilke krav der stilles med hensyn til brug og vedligeholdelse. Ofte vil den IT-sikkerhedsansvarlige ikke have mulighed for selv at installere nye fejlrettelser med mere. Den IT-sikkerhedsansvarlige vil typisk sende fejlrettelserne, som medarbejderen så selv skal installere.

Virksomhedens sikkerhedspolitik omfatter i de fleste tilfælde også din hjemmecomputer. Sæt dig grundigt ind i, hvilke regler der gælder for din hjemmecomputer og overhold dem. Hvis andre i din husholdning efter reglerne kan bruge hjemmecomputeren, skal de også informeres om reglerne og naturligvis overholde dem.

Har ægtefællen og børnene også computere, skal du spørge den IT-sikkerhedsansvarlige, hvorledes I bedst kan koble computerne sammen for eksempel for at I kan deles om printere.



Den **IT-sikkerhedsansvarlige** skal være ekstra opmærksom på hjemmecomputere, der er koblet op mod virksomhedens netværk. De udgør ikke i sig selv en større fare end andre arbejdsstationer, men de glemmes ofte, når der foretages opdateringer af arbejdsstationerne. Glemmes de for tit, kan de pludselig

udgøre en potentiel risiko. Orienter medarbejderne om, hvilke regler der gælder for hjemmecomputere.

Det er normalt ikke overkommeligt for den IT-sikkerhedsansvarlige selv at foretage den fysiske vedligeholdelse af hjemmecomputere, men det er relativt nemt at stille alle opdateringer til rådighed for de medarbejdere, der har hjemmecomputere. Det er vigtigt med en udførlig brugsanvisning, der trin for trin angiver, hvorledes opdateringen foretages.

Den IT-sikkerhedsansvarlige bør også anvise, hvorledes flere computere i hjemmet kan kobles sammen med hjemmecomputeren på en måde, der tilfredsstillende sikkerhed. Det vil sjældent være hensigtsmæssigt bare generelt at forbyde hjemmecomputere at være koblet sammen med andre computere.

Slæk ikke på sikkerheden blot fordi det er en hjemmecomputer.

HVORFOR FORETAGE SIKKERHEDS- KOPIERING?

En ødelagt harddisk, en fejlbetjening af et program eller et hacker-/virusangreb kan medføre beskadigelse eller tab af de lagrede data og programmer på computeren. Tabte data kan genskabes, og programmer kan geninstalleres, men det går hurtigst og lettest, hvis det sker fra en sikkerhedskopi. Der bør derfor tages sikkerhedskopi af samtlige lagrede data og programmer på computeren med regelmæssige mellemrum.



Den **private bruger** kan benytte disketter til sikkerhedskopiering, men efterhånden som de fleste har skrivbare CD-ROM, er dette medium et godt og billigt alternativ.

Den private bruger bør tage en sikkerhedskopi, hver gang der er installeret et nyt program, eller hvis et program er blevet ændret meget i opsætningen, for eksempel når der er lagt en fejlrettelse ind. Desuden bør den private bruger tage en sikkerhedskopi af data med jævne mellemrum.

Hvor ofte afhænger af, hvor meget du benytter computeren, hvor meget e-post du får og sender og så videre. Benytter du kun computeren til at surfe på Internettet, behøver du reelt ikke tage sikkerhedskopi af data, men vurder selv, hvor stort tabet vil være, hvis du mister alle data en uge eller en måned tilbage. Beslut herefter, om du med fordel bør tage sikkerhedskopi af data hver uge eller hver måned. Optimalt set bør sikkerhedskopier opbevares som anført nedenfor i afsnittet om den IT-sikkerhedsansvarlige. Dette vil dog i de færreste tilfælde være muligt.



Medarbejderen kan gå ud fra, at alle data, der lagres på en fælles server, bliver sikkerhedskopieret dagligt. Hvis du som medarbejder gemmer dine filer på PC'ens harddisk (drev C eller drev D), må du som udgangspunkt regne med, at disse data ikke bliver sikkerhedskopieret. Er det normalt i

virksomheden at gemme egne filer på egen PC, bør du som medarbejder spørge den IT-ansvarlige, hvorledes sikkerhedskopi af disse data kan tages.



Den **IT-sikkerhedsansvarlige** skal sikre, at der tages daglige sikkerhedskopier af alle data, der er ændret, siden sidste sikkerhedskopi blev taget. Sikkerhedskopieringsrutinerne varierer fra virksomhed til virksomhed. Det væsentligste er, at sikkerhedskopieringen er sat i system.

Det bør altid sikres, at alle data og programmer er kopieret korrekt over på backup-mediet, inden backup'en arkiveres.

Yderligere bør proceduren til at genskabe data og programmer fra sikkerhedskopien være afprøvet. Proceduren bør afprøves med jævne mellemrum, for eksempel årligt eller halvårligt.

Sikkerhedskopien bør opbevares i brandskab adskilt fra det øvrige system, eksempelvis i en anden bygning.

Husk endvidere, at en backup kun har en vis levetid afhængig af det anvendte backup-medie.

Et backup-medies levetid er endvidere meget afhængig af opbevaringsforholdene. Fugt, varme, skarpt lys og magnetisme kan alle skade forskellige typer af backup-medier. Det er derfor vigtigt at følge producentens anbefalinger for opbevaring nøje, da det ellers risikeres, at en ellers perfekt sikkerhedskopi ikke kan bruges, hvis uheldet er ude.

Tag sikkerhedskopier

Tag sikkerhedskopier, der passer til dit behov. Sæt sikkerhedskopiering i system. Det gør det lettere at få det gjort.

SUND FORNUFT OG AGTPÅGIVENHED

Når du modtager e-post eller surfer på nettet, er klare regler og praktiske foranstaltninger gode at have, men du kommer længst, hvis du også bruger din sunde fornuft.



Både den **private bruger** og **medarbejderen** kan øge sikkerheden ved at være opmærksomme på følgende:

Check adressen en ekstra gang

Når du besøger hjemmesider, bør du sikre dig, at adressen/navnet på hjemmesiden er den, du går ud fra, og ikke bare en, der ligner. Der har været eksempler på, at hackere har kopieret bankers hjemmesider og for eksempel antaget en adresse, der er forvekslelig med en banks adresse med det formål at lokke brugere til at afgive kreditkortoplysninger.

Hvis du selv taster adressen ind, så vær altid opmærksom på, at du ikke taster forkert. Undersøg med andre ord en ekstra gang, inden du „accepterer“. Hvis du kommer til en hjemmeside via en anden hjemmeside, bør du kontrollere, om den er stavet, som du forventer.

Fortrolige oplysninger

Hvis du skal afgive fortrolige oplysninger for eksempel i forbindelse med køb via Internettet, bør du altid benytte en såkaldt sikret linie, hvor de sendte data er beskyttet. En sikret kommunikationslinie vil i Microsoft's browser være vist med en lille gul hængelås i statuslinien. I Netscape's browser skal ikonet på knappen „Sikkerhed“ i menulinien skifte fra en åben hængelås til en lukket hængelås.

Password

Det er en god idé at ændre dit password med jævne mellemrum. Ved at ændre password hyppigt forhindrer du, at uvedkommende for eksempel får adgang til din Internet-konto og dine e-postmeddelelser.

Ved at benytte et password, som består af såvel bogstaver som tal, mindsker du risikoen for at andre kan bryde dit password eller din adgangskode. Jo flere kombinationsmuligheder, desto bedre. Tal og bogstaver tilsammen giver dig flest muligheder og dermed størst sikkerhed. Et password bør bestå af mindst otte tegn.

Password'et skal også kunne huskes af dig selv, uden at du skriver det ned, for et password er en adgangskode, som hindrer andre i at få adgang til dine data. Ingen, ud over dig selv, bør derfor kende dit password - heller ikke IT-afdelingen. Derfor skal du holde det for dig selv. Det er altså vigtigt, at der ikke skiftes password så ofte, eller at det er så komplekst, at du ikke uden videre kan huske det.

Log af

Det er vigtigt, at du husker at logge af Internettet efter brug. Herved undgår du, at uvedkommende får adgang. Ved at logge af efter brug lukker du din forbindelse, hvorefter overførsel af skadelige programmer ikke kan finde sted. En åben linie øger risikoen for, at „hackere“ trænger igennem.

Slet spam- eller junk-mail

Ved at returnere såkaldt spam- eller junk-mail kan du risikere, at dit mailsystem bliver offer for en uendelig strøm af mails, som kan blokere dit system. Disse spam- eller junk-mails kan måske være skabt til at virke mere skadeligt, end navnet antyder. Slet dem **helt** - typisk ved at trykke på „Shift“- og „Delete“-funktionstasterne samtidig - i stedet for at læse eller besvare dem.

HVIS UHELDET ER UDE

Skulle du trods alle forholdsregler alligevel blive ramt af en computer-virus, gælder det som ved andre uheld om at begrænse skaderne, så virus ikke spreder sig, og at få ryddet op efter uheldet.



Den **private bruger** kan begrænse skaderne ved at afbryde forbindelsen til Internet eller e-postdelen, eventuelt ved at hive telefonforbindelsen ud. Dernæst skal selve virusen standses. Du kan forsøge at afbryde det program, hvor virusen optræder, uden at gemme (Ved for eksempel at trykke på „Alt“- og „F4“-funktionstasterne samtidig). Kan det ikke lade sig gøre, kan du slukke for computeren uden at lukke forskriftsmæssigt ned.

Har du fået virusen via diskette eller e-post, skal du fortælle afsenderen dette - (via telefon).

Dernæst skal der ryddes op. Det program, der er inficeret, må ikke startes igen, før der er ryddet op. Er det et program i en office-pakke, må ingen programmer i office-pakken startes, før der er ryddet op. Oprydning kan ske på følgende måder:

Er virus kommet ind via Internet, skal du have en opdatering til antivirusprogrammet på CD-ROM eller diskette, da der kan være en risiko for, at Internet-browseren er inficeret. En CD-ROM/diskette kan laves ved at downloade opdateringen til antivirusprogrammet på en anden computer.

Er virusen **ikke** kommet via Internet, kan du downloade en opdatering til antivirusprogrammet og installere denne. Derefter skal computeren scannes med antivirusprogrammet, der vil forsøge at rydde op.



Medarbejderen skal først og fremmest følge de anvisninger, som virksomhedens IT-sikkerhedspolitik foreskriver for sådanne tilfælde. Ofte vil det være hensigtsmæssigt, at medarbejderen forsøger at stoppe det program, hvor virusen optræder, uden at gemme. Kan det ikke lade sig gøre, kan man slukke for computeren uden at lukke forskriftsmæssigt ned. Dernæst skal den IT-sikkerhedsansvarlige orienteres, hvorefter vedkommende vil tage over for det videre arbejde.



Den **IT-sikkerhedsansvarlige** skal i sin IT-sikkerhedspolitik have en beredskabsplan, der anviser de tiltag, der skal iværksættes, herunder også hvem der skal kontaktes og hos hvem, der kan tilkaldes hjælp i forbindelse med virus- og hackerangreb.

ORDLISTE

ADSL (Asymmetric Digital Subscriber Line)

Teknik til at overføre digital information ved høj hastighed, gennem allerede eksisterende kobber-telefonledninger. Der kan overføres data med hastigheder fra 256 Kbps to 8 Mbps.

Backup-medie

Lagring af vigtige data og programmer på et eksternt lagermedie, der kan opbevares sikkert og anvendes i tilfælde af, at de originale dataer gået tabt.

Computervirus

En programkode, der er skjult og udfører handlinger, som brugeren ikke har tiltænkt. Handlingen har typisk en skadende eller ødelæggende virkning på data eller programmer. En virus laver kopier af sig selv og kan sprede sig selv til harddiske og netværk eller til andre datamaskiner via netværk og flytbare datalagringsmedier (for eksempel disketter og magnetbånd).

Cookies

Cookies er en udvidelse lavet af Netscape til HTTP/1.0-protokollen, der gør det muligt for en WEB server at gemme informationer om brugeren - hos brugeren. Dette giver mange muligheder for designere af web-sider, da HTTP-protokollen ellers er tilstandsløs.

Cracker

Ofte anvendt betegnelse for en person, der bryder („cracker“) en kopi-beskyttelse, for eksempel på et spil eller et edb-program. Se også Hacker.

Elektronisk signatur

Data i elektronisk form, der knyttes til et program eller et dokument, og som anvendes til at kontrollere, at programmet eller dokumentet *stammer fra den person*, der er angivet som underskriver, og at programmet eller dokumentet *ikke er blevet ændret* efterfølgende.

Fil

En samling af data eller instruktioner organiseret til givne formål. For eksempel en fil til lagerstyring kan bestå af den samlede mængde faktura.

Firewall

„Brandmur” - et begreb for beskyttelse af en virksomheds interne edb-net mod indbrud udefra.

Hacker

Ofte anvendt betegnelse for en person, der på retsstridig vis forsøger at skaffe sig adgang til et IT-system, som han ingen lovlig adgang har til. Metoderne hertil kan enten være tekniske (ved benyttelse af indbyggede svagheder i systemet) eller sociale (ved under foregivende af at være systemansvarlig eller lignende at få den retmæssige bruger til at give et password fra sig). Se også Cracker.

Harddisk

En fast disk indeni computeren, hvorpå der kan lagres informationer.

Hjemme-pc

En pc opstillet i en medarbejders hjem med forbindelse til arbejdsgiverens edb-systemer, således at medarbejderen kan udføre visse arbejdsopgaver hjemmefra.

Hoaxes

E-post med falske advarsler om virusangreb, der samtidig opfordrer modtageren af e-posten om at videresende advarslen. Formålet hermed er at overbelaste postsystemer og net.

Internet

Et verdensomspændende netværk som kobler mindre netværk sammen til ét stort net. Internet blev udviklet i 60'erne af det amerikanske forsvar. Hensigten var at lave et netværk som også kunne fungere selv om dele af selve ledningsnettet er beskadiget.

Internetbrowsere

Det program, du benytter til at vise hjemmesider på Internettet med. De mest udbredte er Internet Explorer og Netscape Navigator.

Konfigurering

Det samme som opsætning, hvilket vil sige at skrive de værdier ind i et program, der får programmet til at opføre sig som du ønsker.

Kryptering

Kodning af læsbar klartekst, således at teksten ikke er læsbar for udenforstående, uden at de er i besiddelse af kryptograferingsforskriften og kryptograferingsnøglen.

Macro

Et program skrevet i et makrosprog (for eksempel Visual Basic), der normalt kun kan anvendes i bestemte anvendelsesprogrammer (for eksempel MS Word og MS Excel).

Orm

Et selvstændigt program, der er i stand til at lave kopier af sig selv hele tiden, uden at være afhængig af et andet program. Kan spredes i datanetværk og disketter med videre til andre datamaskiner, hvor ormen så starter sig selv og derved stjæler datakraft fra datamaskinen, som hermed „overbelastes“.

Password

Kodeord som en bruger skal afgive for at få adgang til information.

Plug-in

Et tillægsprogram til et hovedprogram, der fungerer som en opdatering. For eksempel indsætter man et Shockwave-plugin i Netscape, så den kan vise Shockwave-film på Internettet.

Preview-funktion

En funktion i e-post der giver mulighed for automatisk at vise en del af e-postens indhold.

Programfil:

Fil (se denne), som indeholder et program. Alt som sker i en computer kræver et program. Programmer opdeles i to grupper: operativsystemer og brugerprogrammer.

Scanne med antivirusprogram

Sammenligning af pc'ens filer med antivirusprogrammets database over kendte virus karakteristisk med henblik på at opdage og fjerne virus.

Screen savers

Pauseprogrammer der har til formål at beskytte en pc's skærm mod at blive ødelagt af en ensidig „elektronisk“ påvirkning.

Sikkerhedshuller

En fejl i et program eller et edb-system der kan udnyttes til at skaffe sig uautoriseret adgang til data eller programmer.

Sikkerhedsniveau

Et sikkerhedsniveau angiver hvor meget eller hvor lidt den enkelte bruger kan foretage sig på computeren. Ved laveste sikkerhedsniveau har brugeren alle rettigheder til alle programmer, brugerdata og systemdata. Ved højeste sikkerhedsniveau har brugeren kun adgang (måske endda kun læseadgang) til lige præcis de brugerdata, der er relevante for brugeren.

Skærmskånere = Screen savers**Spam- eller junk-mail**

Spam- eller junk mail er uopfordret reklame e-post meddelelser. Man modtager spam- eller junk-mail fra folk, der har opfanget ens e-post-adresse. Normalt er afsenderen i en spam- eller junk-mail ikke en gyldig e-post-adresse, derfor kan du ikke skrive tilbage og klage.

Surfer

Bevæge sig rundt på Internettet.

Trojansk hest

En trojansk hest er et skjulested for mere eller mindre ubehagelige ting. Der er ofte tale om et program, der i sig selv er uskadeligt, men som samtidigt skjult udfører ubehagelige handlinger i form af en computer-virus eller et drilleprogram.

