Skadelige computerprogrammer

(Revision 6 – 19 okt. 2013)

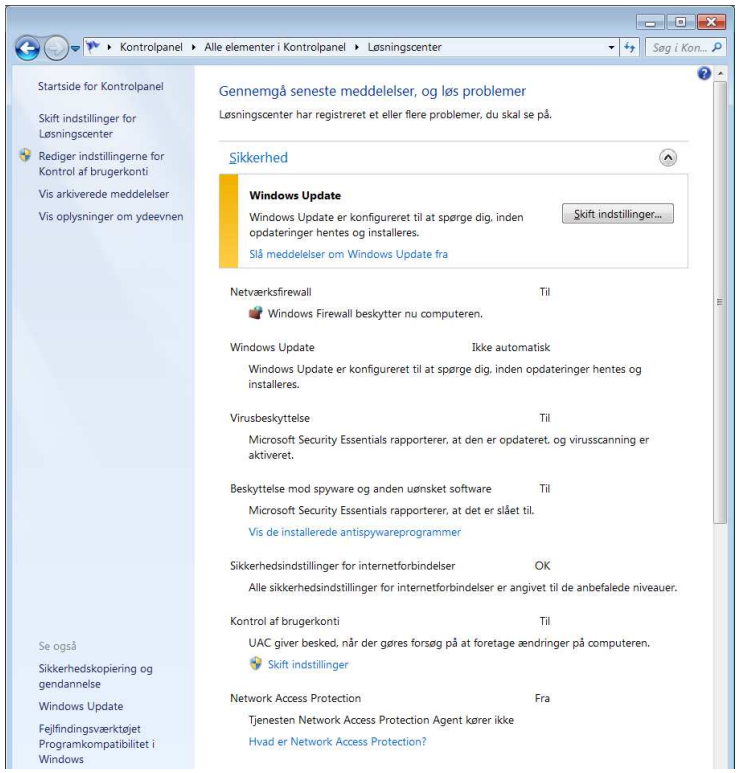
OBS! Ang. antivirusprogrammer: Jeg anbefaler i slutningen af denne artikel brugen af Microsofts antivirusprogram, Microsoft Security Essentials. Bladr frem til side 7, hvis det er det eneste du er interesseret i.

Når du er på nettet, har du hul igennem til hele verden, og hele verden har hul igennem til dig. Så stor nytte vi end kan have af Internet, er der også nogle bagdele. Blandt disse er, at din computer kan blive inficeret med forskellige skadelige programmer og at fremmede personer med ondsindede hensigter kan skaffe sig adgang til din computer, ganske som de selv sad ved tastaturet.

Når du køber en computer med Windows og diverse programmer præinstalleret (installeret ved leveringen), vil de forholdsregler, der beskrives i det efterfølgende, som hovedregel være gennemført. Men du bør selv tjekke, at de forskellige ting er i orden.

Fremmed indtrængning i din computer

Fremmedes indtrængen i din computer beskytter du dig imod ved hjælp af en *Firewall* (Brandmur). En Firewall er et computerprogram, der bygger en slags mur på tværs af din Internet forbindelse. I muren er der bestemte "huller" (porte), hvorigennem du (via computeren) kan kommunikere med omverdenen, læse hjemmesider, sende og hente e-mails, downloade musik, billeder og computerprogrammer.



Figur 1: Oversigt over sikkerhedsindstillinger i Windows 7.

Windows Firewall

Windows er forsynet med en firewall, som du slår til i

Startmenuen ▸
Kontrolpanel ▸
System og sikkerhed ▸
Firewall (Figuren)

Det er muligt at det antivirusprogram, du har fået sammen med computeren, også omfatter en Firewall. I så fald skal du *ikke* aktivere Windows Firewall.

Firewalls benyttes i almindelighed kun ved bredbånds- og kabelforbindelser, hvor computeren er koblet op på Internettet hele tiden.

Har du trådløst netværk (to eller flere computere der deler en Internet forbindelse uden kabelforbindelse til routeren), er det **afgørende vigtigt** at du krypterer net-

værksforbindelsen. Det sker på den måde, der er anført i vejledningen til brug af router eller hub (den kasse, Internetforbindelsen går igennem).

Windows Update

Windows operativsystemet er et temmelig kompliceret system af software, hvori der kan forekomme såkaldte sikkerhelhedshuller. Microsoft modtager løbende oplysninger om sådanne og udarbejder programkode, hvis hensigt er at lukke sådanne huller. Disse distribueres til Windows-brugerne via *Windows Update* abonnementssystemet. Det koster ikke noget.

Sådan tegner du abonnement på Windows Update:

Start ▸
Kontrolpanel ▸
System ▸
Fanebladet Automatiske opdateringer

Her bør du vælge Automatisk, hvis det ikke allerede er valgt. (Figuren på foregående side).

Virus og trojanske heste

Virus er ondartede små computerprogrammer, der evt. kan gemme sig i andre programmer, i e-mails, i musikfiler, billedfiler og (sjældnere) på hjemmesider. Deres virkning er højest forskellig, men aldrig noget godt.

Du kan ikke undgå virusangreb, men du kan beskytte dig imod dem. Først og fremmest ved at bruge din sunde fornuft:

1. Lad være med at åbne og læse e-mails fra personer, du overhovedet ikke kender og som du ikke har fortalt, hvilken e-mail adresse du har.
2. Lad være med at åbne vedhæftede filer, f.eks. billeder, hvis de kommer fra et firma eller en person, du ikke kender noget til.
3. Gode venner eller familiemedlemmer kan sende dig vedhæftede filer med "morsomme" små computerprogrammer, som de selv har fundet "et sted på nettet". Lad dig ikke narre - hvis du ikke er helt på det rene med filens herkomst, skal du ikke åbne den.
4. Download kun musik, billeder og film fra hjemmesider, der har lovlig adgang til at distribuere det pågældende materiale.

Antivirusprogrammer er programpakker, der som et minimum indeholder en virusscanner og et virusskjold.

Virusscanneren gennemgår med faste tidsintervaller, som du selv bestemmer, alle filer på din computer, der kunne tænkes at indeholde en virus. Programmet melder så, efter at kørslen er færdig, om der findes nogen vira. Findes nogen, fortæller programmet hvad det er for nogen, og stiller dig overfor valget mellem at prøve at rense den inficerede fil eller, hvis ikke det lykkes, at slette filen.

Virusskjoldet er aktivt hele tiden og holder øje med "nye filer". Det klassiske eksempel er en fil, der indlæses fra en diskette eller en CD. I vore dage er de hyppigste angreb forbundet med de e-mails man modtager. Det skal understreges, at du godt kan modtage en e-mail fra et familiemedlem eller en ven eller veninde, som er inficeret med virus, uden at afsenderen er klar over det. Den hyppigste årsag er, at afsenderens

computer er inficeret. Men der kan også ske det, at ondsindede personer "stjæler" afsenderadressen og misbruger den.

Uanset årsagen er det i alles interesse, at du kontakter afsenderen og gør opmærksom på problemet.

Trojanske heste er tilsyneladende uskyldig programkode, der udfører en eller anden tilsyneladende uskyldig funktion, men i virkeligheden bag facaden inficerer din computer med en virus. Virusskjoldet beskytter også mod sådanne.

Cookies

Cookies er små stykker tekst som nogle hjemmesider lægger ind på din computer. Det hyppigste formål med cookies er identifikation: Når den hjemmeside, der har lagt cookie'n, igen får besøg fra din computer, kan den bruge cookie'n til at identificere dig. Det gør det muligt at genskabe de data, du evt. tidligere har oplyst, for eksempel bankkontonumre, forsendelsesadresser og lignende. For eksempel ved netboghandelen amazon.co.uk at jeg altid leder efter bogtitler inden for en bestemt genre, så derfor skræddersyr Amazon en hjemmeside til mig med det nyeste inden for mit interesseområde.

Cookies er altså i almindelighed nyttige og fuldstændigt uskadelige. Det er rene tekstfiler, og du kan selv kigge i dem for at se indholdet. Det er dog som regel noget kryptisk, blot en lang række tal og bogstaver.

Et EU-direktiv kræver, at en webservice bede om tilladelse til at lægge en cookie på din computer. Det sker som regel i form af en sætning, der fortæller dig at forudsætningen for at bruge hjemmesiden er, at du samtykker i brugen af cookies fra denne tjeneste. Her er et eksempel:

Brug af cookies på Rejseplanen.dk

Vi bruger cookies for at give dig en bedre brugeroplevelse, bl.a. så vi kan huske dine seneste indtastninger. Når du fortsætter med at bruge rejseplanen.dk, accepterer du samtidig brugen af cookies. Læs mere om brugen af cookies her .

Det er langt fra alle hjemmesider, der følger reglerne. Derfor bør du fra tid til anden — afhængig af hvor mange forskellige websteder du besøger, rydde op i bunken af Cookies.

I Chrome-browseren (Googles browser) sker dette i

Indstillinger ▸
Beskyttelse af personlige oplysninger ▸
Indstillinger for indhold.

Her kan du også indstille til at websteder ikke må anbringes cookies på din computer. Dermed risikerer du dog, at webstedet ikke har den nødvendige funktionalitet.

Spyware

Spyware (Spionsoftware) er også en slags cookies, men ikke helt så uskadelige som de netop nævnte. Formålet med spyware "cookies" er heller ikke specielt gavnligt for dig. Det er som regel små programmer, der har til formål at registrere din e-mailadresse og din færden på Internet. Disse oplysninger kan skruppelløse personer bruge til en aggressiv e-mail markedsføring overfor dig. Jeg formoder også, at der findes spyware med mere ondsindede formål, som f.eks. opsnapning af adgangskoder.

Virkningen af spyware på din computer kan ofte være, at den bliver mere og mere langsom til at gøre de ting, du er vant til at gøre, dine programmer kommer til at virke ret sløve i optrækket.

Spyware bekæmpes med en spyware-scanner, der ligesom et antivirusprogram med korte mellemrum gennemgår de områder på computerens harddisk, hvor sådanne programmer skal findes, for at de kan have den tilsigtede virkning. Igen bliver du spurgt, om du ønsker at slette dem, hvis der findes nogen. Microsoft Security Essentials beskytter også mod Spyware.

Spam

Spam er kort fortalt uønskede e-mails. Markedsføring via e-mails er meget billig og derfor meget populær metode til at promovere sine varer og tjenester over for rigtig mange mennesker. Derfor er der folk der lever af at "høste" e-mail adresser ved hjælp af mere eller mindre legitime metoder og sælge disse e-mail samlinger videre.

Den nemmeste måde at høste e-mail adresser på er ved at scanne hjemmesider. Hvis din e-mail adresse derfor står på en hjemmeside, skal du bede den, der har lavet hjemmesiden, om at "skjule" adressen for høst-programmet. Det er let på nettet at finde forskellige metoder til at gøre det.
(*http://www.webdesign101.dk/www/javascript/nophishing.php*)

I Danmark er det forbudt at masse-distribuere e-mails, hvis formål er at markedsføre eller sælge varer og tjeneste, medmindre firmaet, der står bag udsendelsen, kan dokumentere, at de folk de sender til, selv har bedt om det. Men det hjælper jo ligefedt når de firmaer, der høster e-mail adresser og de firmaer, der udsender de uønskede e-mails uden videre kan gøre fra USA, Bhutan, Ukraine eller et hvilketsomhelst andet land, der har en mere liberal markedsføringslovgivning end Danmark.

Derimod er det fuldt lovligt, også i Danmark, at massedistribuere e-mails til adressater, der selv har bedt om at få sådanne e-mails. Det er oven i købet en forbrugervenlig metode, idet du fra forskellige butikker og butikskæder, varehuse og så videre, kan få e-mails om ugens tilbud og lignende.

Du kan blokere for de fleste spam-mails ved hjælp af et spam-blokeringsprogram. Nu er det desværre ikke helt ligetil at kende forskel på en e-mail, du selv har bedt om og en du ikke har bedt om. Derfor skal du selv oplære din spam-blokker.

Du kan (og bør) klage over spam, spam fra danske firmaer på dansk@spamklage.dk, spam fra udenlandske firmaer på int@spamklage.dk. Du klager på følgende måde: Gem den e-mail du vil klage over (Gem som fil, CTRL-S), og send derefter en e-mail til en af ovennævnte adresser med en kort besked som emne (for eksempel ”Klage over spam fra [afsenderens navn]”) og sendt den gemte e-mail som vedhæftet fil. *Brug ikke* Videresend-*funktionen*.

(E-mails, der gemmes på denne måde får endelsen .eml).

En af fordelene ved Webmail tjenester som for eksempel Gmail er, at disse tjenester har nogle meget effektive spam-filtre. Jeg kan til illustration af dette nævne at jeg på en ”almindelig” e-mail adresse får 15-20 spam mails om dagen, mens jeg på en ganske tilsvarende webmailtjeneste får måske 1 eller 2 om måneden.

Popup-vinduer

Nogle hjemmesider har den facilitet, at de åbner et eller flere små ekstra browservinduer med meddelelser, oftest annoncer. Som regel lægger disse ekstra browservin-

duer sig oven på den side, man er i færd med at læse, og de er derfor ganske lette at fjerne ved at lukke det ekstra browservindue på sædvanlig facon. I nogle tilfælde er de imidlertid minimerede eller lagt i baggrunden, så man kun kan se dem ved at kigge i proceslinien forneden på skærmen.

Moderne browsere er som standard indstillet til at blokere disse ekstra vinduer, men der findes metoder til at omgå denne blokering. Under alle omstændigheder er det vigtig hele tiden at have et halvt øje på proceslinjen.

Link

http://www.spywarefri.dk er et dansk websted med en masse information om de emner, der er omtalt i dette notat.

På dette websted kan du blandt andet lave en online test af din computer for at finde ud af, om den er inficeret med spyware. Du kan også finde links til forskellige programmer, der letter bekæmpelsen af spyware, virus osv.

Windows Defender

Microsoft har lavet et godt program til beskyttelse mod spyware, *Windows Defender*. Det kan downloades fra

http://www.microsoft.com/danmark/athome/security/spyware/software/default.mspx

(Ovenstående indtastes på én linie).

Efter installation af Windows Defender vil Windows Update automatisk opdatere datafilen med oplysninger om nye spyware cookies eller -programmer.

Hvis du bruger det program, der er omtalt til sidst i denne artikel, har du ikke behov for at installere eller aktivere Windows Defender, da det er en integreret del af Microsoft Security Essentials.

Datafiler og opdatering

Såvel antispyware som antivirusprogrammer fungerer på basis af en database på computeren over alle kendte spyware og virus. Da der hele tiden kommer nye af den slags, er det nødvendigt at disse databaser bliver opdateret. Dette sker automatisk når man har tegnet abonnement på programmet, uanset om det er et gratis program som Microsoft Security Essentials eller AVG antivirus, eller om det er et kommercielt program, du har betalt for.

Udskiftning af antivirusprogram

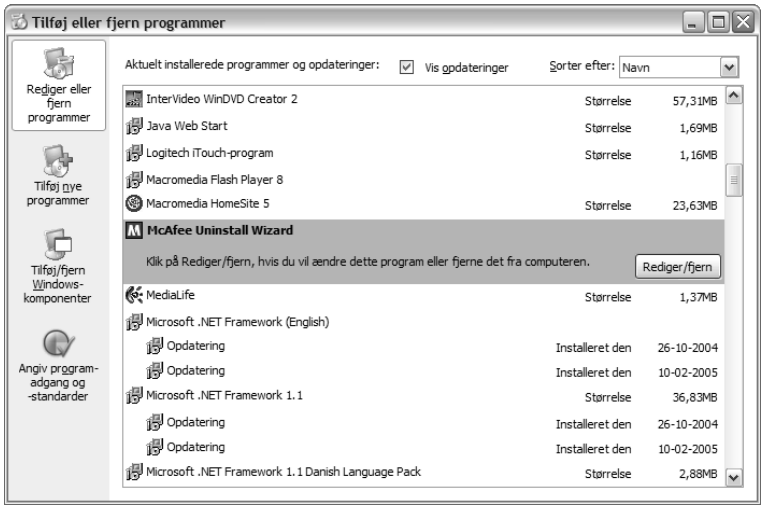
Når du købere en ny computer, leveres den altid med et antivirusprogram. Dette er som regel et kommercielt produkt – det vil sige, det koster penge – som fungerer i en periode efter købet af computeren. Når denne periode er udløbet, får du typisk et tilbud om at opdatere eller forny programmet. **Du skal tage stilling til dette**. Hvis du ikke fornyer dit abonnement, bliver din antivirus-database ikke længere opdateret, og så er Fanden løs i Laksegade.

Det billigste tilbud er en fortsat løbende opdatering af virus-databasen. Det koster typisk nogle få hundrede kroner om året. En anden mulighed er at købe en ny version af programmet - på forunderlig vis har disse programhuse altid en ny og bedre pakke på det tidspunkt, hvor du skal forny dit abonnement.

Det allerbilligste tilbud er at udskifte det præinstallerede antivirusprogram med et gratis ét af slagsen. Der findes flere forskellige gratis antivirusprogrammer. Det mest kendte er (eller var(?)) *AVG antivirus*. Det kan downloades fra

http://free.grisoft.com/

Den nyeste version af AVG er i skrivende stund version *AVG AntiVirus FREE 2013*. Har du AVG antivirus i forvejen er det sandsynligvis en tidligere AVG version og i så fald skal du downloade og installere ovennævnte version inden en bestemt dato.



Figur 2: Du fjerner programmer fra din computer ved hjælp af kontrolpanelet.

Før du skifter til AVG Free antivirus skal du afinstallere det, du har i forvejen.

Fremgangsmåden er følgende:

Lav først af alt et gendannelsespunkt:

Kontrolpanel ▸
System ▸
Systembeskyttelse ▸
Klik på knappen "Opret"

Find nu ud af, hvilket antivirusprogram, du nu har. Der vil som regel være en lille ikon i systembakken til højre i proceslinien, der fortæller hvilket program der er tale om. Ellers må du gå igennem dine programmer (Startmenuen, Alle programmer) og finde navne som Norton, McAfee, E-Trust, Panda eller hvad det nu kan hedde.

Du fjerner et sådant program ved hjælp af

Start
Kontrolpanel
Tilføj/fjern programmer

Dobbeltklik på Tilføj eller fjern programmer og vent, indtil computeren har opbygget listen over installerede programmer.

Find nu på listen – jf. figuren herover – dit antivirusprogram, marker det og klik på Rediger/fjern-knappen. Så bliver du ført igennem en afinstallationsproces, hvor du skal bekræfte, at du ønsker at fjerne dette program.

Det er muligt, du bliver bedt om at genstarte computeren i løbet af denne proces.

Når du har fjernet det gamle program, skal du installere det nye. Du starter med at downloade pakken fra ovennævnte websted. Når det er sket, dobbeltklikker du på ikonet for AVG antivirus, hvorefter programmet installeres.

Microsoft Essentials

Siden dette notat blev skrevet første gang i 2006 er der sket det, at Microsoft, der står bag Windows styresystemet, har frigivet et gratis antivirusprogram, der er alt rigeligt til private husholdninger. Programmet kan downloades fra nedenstående link:

http://windows.microsoft.com/da-DK/windows/security-essentials-download [1]

Dette er et dansksproget alternativ til AVG og andre gratisprogrammer. Det er noget lettere at håndtere for private husholdninger og kræver ikke noget særlig vedligehold for at fungere. Firewall'en er Windows' egen og opdateringerne foregår sammen med Windows Update. Installer og glem!

———

19. oktober 2013

En opdateret udgave af dette dokument kan downloades fra

http://733/seniorpc/artikler/virspy.pdf

[1] Programmet findes i to versioner. Du skal vælge enten 32-bit eller 64-bit versionen, afhængigt af om din Windows er 32 bit eller 64 bit. Det finder du ud af ved at højreklikke på Computer (Min Computer) og vælge egenskaber. Lidt nede på den side, der vises, står der noget om system type. Står der ikke noget er dit system et 32 bit system.