DIN vejledning til computersikkerhed

Det kræver teknisk viden at eje en computer. Selv med en Linux/UNIX distro på systemet.. - Hvis man vender det blinde øje til, kan det gå galt for enhver. VIL man træde i spinaten, kan man altid det, ligegyldigt hvilket system eller antivirus/sikkerheds

Skrevet den **28. Aug 2011** af **OracleJMT (nedlagt brugerprofil)** I kategorien **Sikkerhed / Generelt** |

De kriminelle i cyberspace bliver dygtigere og dygtigere. Der bliver skrevet ny malware hvert sekund, og millioner af
intetanende computerbrugere verden over, bliver inficeret næsten lige så hurtigt. Og hvad så? - Vil du nok spørge.
Lad os først koncentrere os om DIN computer, og hvad du udsætter den og dig selv for, når du er forbundet til internettet.
Hver gang du åbner din browser udsætter du dig selv for en risiko for at blive inficeret med malware.

Hvad er malware?

Malware står for "malicious software" på dansk skadelig software, og er de kriminelles værktøjer. Det er en fælles
betegnelse for virus, orme, bagdøre, trojanske heste, rootkits, hijackers, keyloggere, clipboard-loggere, web-cam
loggere, exploits, spyware, adware, falske sikkerhedsprogrammer, mm.
http://en.wikipedia.org/wiki/Malware

Malware er den slemme dreng den dag i dag, da du kan risikere, at få lænset din bankkonto, fordi der er blevet installeret
en trojansk hest (ondsindet program, der sender oplysninger om dig og din computer videre til en hacker) en keylogger
(program der "opfanger" dine tastetryk i en log og sender loggen tilbage til en hacker, typisk med informationer om
kort/bankoplysninger) eller en bagdør.
Du kan også være uheldig at få et falsk sikkerheds program på din computer. Det er slet ikke spor morsomt, for du bliver
bombarderet med falske scanninger og pop-up vinduer, og bliver bedt om at købe for at få fjernet de resultater
programmet viser.
DU MÅ ENDELIG IKKE KØBE et falsk sikkerhedsprogram, for alt hvad de vil med dig, er at stjæle dine penge og din
identitet, til fordel for noget ubrugeligt bras.
Der findes i øvrigt også falske registry cleanere og andre optimizere. Samme råd bør følges heraf: KØB ALDRIG
ALDRIG NOGENSINDE.

Det værste du kan blive inficeret med overhovedet, er et rootkit. Et rootkit er et stykke malware, altså et MEGET
skadeligt program, med direkte onde hensigter. - Det er bygget op på den måde, at det skjuler sig fra dig, din antivirus-

scanner, og ikke nok med det, også ofte skjuler et andet farligt stykke malware, f.eks. en trojansk hest, eller andet utøj.
Det er næsten UMULIGT at opdage i systemet, fordi det skjuler sig utrolig dybt, og er også næsten umuligt at fjerne, når
det først er aktivt.

Hvis du er blevet inficeret med et rootkit, hvilket du nok ikke opdager, har den person i "den anden ende" altså personen
der har fået forbindelse til computeren vha. rootkittet som DU kom til at downloade og køre, FULD kontrol over dit
system, og kan praktisk talt gøre alt det DU kan på din computer, inkl. se din skærm, optage dine tastetryk på dit
keyboard, optage dit clipboard, (copy-paste) slette/oprette register nøgler, oprette skjulte mapper/drivere, genstarte dit
system, åbne dit cd-rom drev, slette dine filer og mapper, sende data til og fra din computer, tænde og slukke for dit
webcam, se dig vha. dit webcam, aflytte din mikrofon, forhindre dig i at åbne programmer/tilgå dele af systemet og meget
meget mere. Faktisk har en hacker, der kontrollerer et rootkit MERE kontrol over dit system, end du selv har.

Hvad skal jeg så gøre for ikke at blive inficeret med malware?

Start med at anskaffe dig et rigtig godt sikkerhedsprogram, der holder skidtet ude.

Blandt de gode gratisløsninger anbefaler jeg at du enten:

Downloader og installerer Comodo Internet Security(Har det hele. Anti-virus, HIPS (Defense+), Automatisk Sandbox, Firewall, Buffer Overflow Beskyttelse, mm.)

Downloader og installerer Avast Free version, Sandboxie free version og Online Armor Free firewall

Downloader og installerer Avast Free version, Geswall Free version og Online Armor Free firewall

NB. Er behavior blockeren i Avast slået til, slå den fra. Den går ikke sammen med ovenstående kombination af programmer. Slå den fra, hvis den er slået til.

Brug EN af de tre løsninger, installer aldrig flere sikkerheds- programmer end et på samme maskine samtidigt.
Det vil konflikte BIG-TIME, og kan sløve dit system til næsten standsning. Ydermere vil risikoen for at blive inficeret, blive ENDNU højere. Det gælder for firewall, sandbox, HIPS og andet med overvågende beskyttelse.
Kun én af gangen. Altså f.eks. Ét anti-virus, én sandbox, ét hips, én firewall. Skåret ud i pap: Èn Comodo Internet Security. ELLER én Avast + én Sandboxie + én Online Armor. ELLER én Avast + én Geswall + én
Online Armor.

Blandt de gode købeløsninger anbefaler jeg at du enten:

Køber dig et traditionelt anti-virus f.eks Eset NOD32, og supplerer det med købeversionen af Online Armor Firewall.

NB: Kører du med Windows XP skal du også have en god firewall. Windows Firewall i XP er ikke meget værd.
Kører du med Vista eller Windows 7, skal du SELV konfigurere firewallen, hvilket jeg ikke anbefaler.

Køber dig en sikkerhedspakke f.eks Kaspersky Internet Security. (Har allerede firewall, så du behøver ikke supplere med én.

Køber dig et HIPS med firewall f.eks Defensewall Personal Firewall. (HIPS står for HOST INTRUSION PREVENTION SYSTEM)

Hvad et Host Intrusion Prevention System er:

http://en.wikipedia.org/wiki/Host-based_intrusion-prevention_system#Host-based

Hvad en Sandbox er:

http://en.wikipedia.org/wiki/Sandbox_(computer_security)

NB. Defensewall, Geswall og Sandboxie behøver hverken signaturer eller opdateringer, men beskytter dig alligevel med
98% mod kendte og ukendte trusler. Intet er 100%!

Defensewall hjemmeside:

http://softsphere.com/

Sandboxie hjemmeside:

http://sandboxie.com/

Geswall hjemmeside:

http://gentlesecurity.com/

Kaspersky hjemmeside:

http://www.kaspersky.com/dk/

Comodo hjemmeside:

http://www.comodo.com/

Online Armor hjemmeside:

http://www.online-armor.com/

Eset hjemmeside:

http://www.eset.com/

Paching/opdatering af programmer samt styresystem:

Skal jeg også opdatere mine programmer og styresystem? Svaret er JA!

Du skal opdatere alle dine tredjeparts-programmer til de har den nyeste version. Programmer som f.eks.: Adobe Reader,
Java, itunes, Adobe Flash. ALLE de programmer du har installeret skal have den nyeste version.
Du kan bruge programmet Secunia PSI til at holde alle dine tredjeparts-programmer + styresystem opdateret.
HUSK at fjerne ældre versioner af Java, da de indeholder sikkerhedshuller og udsætter dig for at blive inficeret med
malware, hvis du løber ind i en exploit, mens du surfer.
Du kan bruge programmet JavaRA til at opdatere Java + fjerne gamle versioner, der ligger på systemet. Du skal altid
kun have én version af Java installeret, nemlig den nyeste.
Slå automatiske opdateringer til i Windows Sikkerhedscenter, og sørg generelt for at holde alt opdateret lige fra Windows
opdateringer til programmer.

Browsing:

Der findes langt bedre, sikrere og hurtigere browsere end Internet Explorer.

Her er nogle alternativer:

Google Chrome, Firefox, Opera, Safari.

Installer Web Of Trust. (Web Of Trust er en udvidelse til Internet Explorer, Firefox, og Google Chrome, som advarer imod
farlige sider på nettet)

Google Chrome hjemmeside:

http://www.google.com/chrome

Mozilla Firefox hjemmeside:

http://mozilladanmark.dk/produkter/firefox/

Opera hjemmeside:

http://www.opera.com/

Safari hjemmeside:

http://www.apple.com/safari/

Og pas så på hvad du klikker på. Vær kritisk overfor ALT du møder på internettet. Husk på, at der bliver skrevet ny
malware hvert sekund, så du kan aldrig være helt sikker.
OG LAD VÆRE MED AT BRUGE P2P/FILDELING OG CRACKS/KEYGENS, DA RIGTIG RIGTIG MEGET MALWARE KOMMER AD DEN VEJ!!! DESUDEN ER DET DYBT ULOVLIGT.

Læs hvorfor her:

http://en.wikipedia.org/wiki/Copyright_infringement

Hvad torrent software er:

http://en.wikipedia.org/wiki/BitTorrent_(protocol)

Hvad fildeling er:

http://en.wikipedia.org/wiki/Peer-to-peer

Hvorfor er det farligt at bruge fildeling/p2p/cracks/keygens?

http://www.spywarefri.dk/artikel/farerne-ved-fildeling/

Backup:

Sørg for at have en backup af alle dine vigtige filer. Det værende billeder, dokumenter, musik etc. Det kan redde dig i den
kritiske situation, hvor du er tvunget til at formatere harddisken.
Til online backup anbefaler jeg A-drive. Der er gratis online backup op til 50 GB.

Rensning/On-demand:

Er du havnet i store problemer, og vil blive fri for malware, vil jeg anbefale, at du i første omgang scanner med dit
antivirus-program og fjerne hvad den finder. Dernæst kontakter Spywarefri Forum / almindelig rensning og beder om
hjælp. - Hvis du er god til engelsk er der andre fora, hvor du kan få hjælp til rensning, bla. Bleeping-computer.
Det er det en god idé at installere Malwarebyes' Anti-Malware i gratis-udgaven til at scanne med som en "second
opinion" til din etablerede sikkerhedspakke/antivirus. Det kan finde og fjerne rigtig meget malware fra computeren.
Du kan også bruge Super Antispyware. Det er en anden gratis scanner, der også er meget effektiv.
Du kan også installere Hitman Pro, det er et købeprogram og fungerer som prøveperiode indtil du aktiverer det og kan
derfor kun fjerne i en begrænset periode, men du kan altid scanne og se om den finder noget.

Links til frivillig online rensning:

http://www.spywarefri.dk/forum/

http://www.eksperten.dk/

http://www.bleepingcomputer.com/

http://www.malwarecheck.dk/forum/

http://forums.malwarebytes.org/

Rescue disc/SARDU:

Hvis du er inficeret har også muligheden for at scanne dit system med en Rescue CD. Mange anti-virus firmaer har en
Rescue disc ISO du kan downloade, f.eks. Kaspersky Rescue Disc.

Du kan også downloade SARDU, som er et program der samler flere anti-virus boot-ISO'er, som du kan lave om til én
multi boot rescue disc. - Der er også mulighed for at lave en Rescue USB. - Du kan også tilføje andre rescue-værktøjer
til SARDU, endda et rescue-styresystem, f.eks.Ultimate Boot CD 4 WIN, (UBCD4WIN) og andre værktøjer.

SARDU adressen er:

http://www.sarducd.it/

Ultimate Boot CD 4 WIN adressen er:

http://www.ubcd4win.com/

For yderligere information / vejledning vedrørende SARDU henviser jeg til Fromsej's side:

http://www.fromsej.dk/Vejledninger/html/sardu.html

Og

http://www.fromsej.dk/Vejledninger/html/sardu2.html

Oprydning og clean-up:

Er din computer langsom af andre årsager end malware, kan du installere et lille gratis, men godt stykke software ved
navn Ccleaner. Det fjerner midlertidige internet filer, og andre gamle rester der sløver din computer.
Der findes et rigtig godt program til defragmentering af din harddisk ved navn Auslogics Disk Defrag. Det går mere i
dybden end den indbyggede defragmentering i Windows, som ikke er af høj kvalitet.
God fornøjelse med fremtidig brug af din PC!
Og husk, DU er den bedste sikkerhed din computer kan få. Dine sikkerheds-programmer er kun til for at hjælpe dig.

Kontakt mig:

Hvis du har spørgsmål til min vejledning, er du velkommen til at kontakte mig. Min mail adresse er:

oraclejmt(A)gmail.com

Grunden til, at jeg skriver det sådan, er så jeg undgår at en evt. spam-bot skal opfange min mail adresse. Bare til din
information.

Kommentar af john_stigers (nedlagt brugerprofil) d. 28. Aug 2011 | 1

God guide :)

Kommentar af hardwareguy15 d. 31. Aug 2011 | 2

En nem hovedregel: Køb aldrig sikkerhedssoftware,dvs. antivirus,antispyware,m.v men brug gratis programmer, de fungere udmærket.

Kommentar af OracleJMT (nedlagt brugerprofil) d. 01. Sep 2011 | 3

Hardwareguy15>>

Jah, men det kommer jo også meget an på hvilke gratis programmer der er tale om. Comodo Internet Security kan beskytte lige så godt som betalingsprogrammerne, men har man kun et antivirus og klarer sig med Windows firewall, er man ikke godt sikret.

Kommentar af Burgdorf d. 07. Sep 2011 | 4

Anway, lækker guide :) Den giver lidt til tænkeren

Kommentar af tobrukDk d. 09. Sep 2011 | 5

Utrolig dejlige Guide!..

Kommentar af Besil d. 20. May 2016 | 6

Hejsa

Til backup, er det stadig A-drive der anbefales?
Og hvad er der lagt vægt på (prisen, sikkerhed, overskuelighed over sine filer ...) ?