Gør din privat pc sikker

Mange mennesker oplever at få virus, at PC'en går ned, at får spy- eller malware og ofte betyder det mistede billeder, dokumenter, mails og kontakter samt at deres maskine står stille i lang tid. Sådan sikre du din PC i 2009

Skrevet den **02. Feb 2009** af **bufferzone** I kategorien **Firewalls / Generelt** | ★★★☆☆

For nogle år siden skrev jeg en tilsvarende artikel her på Eksperten, der hed "Sikkerhed på din private Computer." (http://www.eksperten.dk/artikler/32), denne artikel er løbende blevet opdateret, men dels har miljøet ændret sig og dels er jeg blevet klogere, så jeg har valgt at skrive den helt om i stedet for at pynte på en gammel model.

Din PC, Bærbare og andet udstyr.

Moderne computerudstyr, og det dækker i virkeligheden alt fra dit armbåndsur, over din mobiltelefon til dit medie center, er både let, mobilt, utroligt kraftigt og har masser af funktionalitet og selvom dette er rigtig dejligt og smart, så udgør det også en risiko. Jeg vil selvfølgelig ikke foreslå dig at købe udstyr der er tungt, langsomt og intet kan, men jeg vil opfordre dig til at tænke dig om og slå det udstyr og de funktionaliteter du ikke bruger fra når du ikke bruger dem. Hvis du ikke er på et trådløst net, så slå dit trådløse netkort fra, hvis du ikke har brug for bluetooth, så slå det fra. Jo færre muligheder der er for at kommunikerer med dit udstyr, jo sikre er det.

Se dig om og tænk dig om

For få år siden var en PC något man brugte fra sit hjem eller fra arbejdet. I dag bruges Pc'en når man er på café, i lufthavnen, i toget, i parker, ja faktisk alle steder og det udgør en massiv risiko hvis man ikke gør det rigtigt. Jeg har skrevet en artikel der dækker dette emne mere udtømmende, den vil jeg anbefale du læser hvis du er mobil PC bruger samt selvfølgelig følger rådene. Læs artiklen Trådløse hotspots - Brug dem sikkert (http://www.eksperten.dk/artikler/919)

Hold dig opdateret.

Sikkerhedsopdateringer fjerner huller og sårbarheder i dit system og fjerner dermed nogle muligheder for at svine din maskine til på den ene eller anden måde. Du bør kritisk gennemgå hvordan din maskine opdateres, således at du får det hele med. I dag opdateres meget software automatisk og det kan give en falsk tryghed, for dels findes der software der skal opdateres manuelt og dels kan automatiken slås fra. Gør det til en vane med jævne mellemrum at kontrollerer ALT din software så det er helt opdateret, også de programmer du sjældent bruger.

Ryd op og vælg fra.

Ligesom du bør afbryde det udstyr du ikke anvender, bør du også fjerne de programmer du ikke bruger, Ryd op, ryd ud, fjern det gamle du ikke bruger mere. Jo mindre du har på din maskine jo mindre er der at hacke eller udnytte og jo sikre er du.

Det handler også om at vælge fornuftigt samt om at være bevidst om sine valg. Alle aktive programmer udgør en risiko, men hvis vi skal have fornøjelse ud af vores udstyr, og kunne kommunikerer, så er vi nødt til at være villige til at accepterer en vis risiko. Dette kræver at vi kender risikoen.

Hvis du f.eks. vælger at anvende fildelingsprogrammer som Kazaar, e-mule, torrent og ligende, så er du nødt til at accepterer en forhøjet risiko. Lad være med at køre den slags programmer uden at du sidder ved din maskine og overvåger den, lad være med at hente alt muligt ned på din maskine ukritisk og tænk dig om. De samme råd er gældende for Instant Messing programmer som Messenger, IRC programmer som ICEChat, Telefon programmer som Skype og andre programmer der aktivt kommunikerer ud via internettet. Tænk dig om, slå dem fra når du ikke anvender dem og når du ikke sidder ved din maskine.

Kys aldrig på din første date.

Sociale netværk som FaceBook, LinkedIN, Myspace og andre er blevet meget populærer og de fleste har i dag profiler disse steder. Selvom jeg helst ville foreslå at du ikke kom den slags steder, så ville det lyde lidt hult, så jeg er der selv. Brug disse sites, lige som med alt andet, med fornuft og omtanke.
Lad være med at trykke på links som du modtager via facebook og andre sites, hvis du ikke er HELT sikker på at det der linkes til er i orden. Kontakt evt personen der har sendt det til dig via mail og spørg hvad det er og om det er rigtigt at han/hun har sendt det til dig.
Lad være med ukritisk at installerer alle mulige udvidelser til din facebook profil, de samler oplysninger om dig og kan udnyttes til ting du ikke ønsker.
Lad være med at afsløre for mange detaljer om dig selv. Hvis du f.eks. tydeligt via det du skriver og de grupper du er medlem af signalerer at du interesserer dig for heste, så er det let for mig at sende dig et link eller en fil som ser ud til at indeholde præcist det du interesserer dig for og dermed får dig til at klikke på det. Dette kaldes Spear Phishing og det virker.

Der er altid alternativer.

Det er klart at både hackere, virus, spyware og malware producenter går efter de programmer hvor de rammer flest og det betyder oftest Microsoft programmer. Der er heldigvis udmærkede alternativer til de fleste af de kendte MS programmer. Brug f.eks. FireFox i stedet for Internet Explorer og Thunderbird i stedet for Outlook. Der findes også andre IM klienter end Messenger og f.eks. er denne artikel skrevet i Open Office i stedet for Word. De fleste af disse alternativer er en smule mere sikre end Microsoft's programmer, og f.eks. Fire'Fox kan sikres yderligere med forskellige tredieparts plug-ins. som NoScript og du kan let krypterer og signerer dine mails med GNUpg i Thunderbird.

Gør lidt ekstra ud af tingene.

Du bør selvfølgelig have både et fornuftigt Antivirus program, en firewall og anti Spyware/malware programmer installeret op fuldt opdateret. Hvilke programmer du bør vælge vil jeg ikke sige noget om, da det dels er lidt et spørgsmål om smag og så fordi det der er det bedste valg i dag, måske i morgen har et massivt hul der dømmer det ude.
Du kan også gøre en masse for at sikre din maskine yderligere, og hvis du interesserer dig for det og gerne vil læse uddybende, så kig forbi http://www.nsa.org og http://www.microsoft.com/security hvor du kan finde gode og omfangsrige vejledninger.
Et ret godt trick som du bestemt bør overveje at bruge er at redigerer i din HOSTS file. I gamle dage da internettet ikke var ret stort, skete alt routningpå nettet vie disse HOSTS filer. De findes på Windows maskiner i biblioteket windows/system32/drivers/etc og på linux i etc biblioteket. Hvis du i din HOSTS fil skriver linien:

127.0.0.1 www.arto.dk

så vil man ikke kunne åbne www.arto.dk på din maskine sådan uden videre. Du behøver ikke skrive hele filen selv, en udmærket HOSTS fil som du kan tage udgangspunkt i eller bruge direkte kan downloades flere steder f.eks.

http://www.mvps.org/winhelp2002/hosts.txt og http://someonewhocares.org/hosts/

du indkopiere blot de relevante linier (eller dem alle) i notepad, navngiver fil HOSTS (uden endelse) og

placerer den det rigtige sted (overskriver den der er der i forvejen). Efterfølgende kan du jo tilføje de sites du ønsker at blokkerer, f.eks. ARTO og ligende.
Denne løsning er langt fra en 100%´s løsning, men den vil standse en del skidt og fjerne en masse muligheder.
En anden lille ting du bør kigge på er McaFee Site Advisor der er gratis og som hjælper dig med at undgå skidt når du søger med f.eks. google.

Opfør dig nu ordentligt.

Som jeg har skrevet flere steder, så afhænger din sikkerhed meget af hvordan du selv opfører dig når du bruger den. Tænk dig om når du installerer, når du starter programmer, når du ikke bruger programmer eller udstyr aktivt og når du gør aktive ting på nettet. Lad være med ukritisk at trykke på links, lad være med at åbne vedhæftede filer som du ikke er sikker på, tænk dig om når du læser e-mails (og nej du har ikke vundet de 23.000.000.000.000 $ selvom den email du har modtaget fra Afrika er stilet til dig) og ting der ser lidt for gode ud til at være sande er det oftest (altid).

Når det skal være virkeligt sikkert!!!

Nu er Ekspertens brugere for det meste en smule mere lærte på computerområdet end gennemsnittet, så der skal selvfølgelig også være lidt særligt til dem. Her er en opskrift på hvordan min ultra-sikre maskine er sat op.

Vi starter fra bunden med maskinens operativ system. Jeg har valgt Damm Small Linux, men du kunne også vælge f.eks. XP. Efter installationen (i linux gøres det under installationen) fjerner du alle de programmer du kan fra din maskine, du skal nemlig ikke bruge bund operativ systemet til ret meget. Når du har strippet OS helt ned og opdatered det der er tilbage, installerer du 3 programmer (i Linux kun 1) nemlig Antivirus, Firewall (der er indbygget i Linux og den i XP er ikke god nok) samt VMWare (server eller workstation)

Når du har din VMWare oppe og køre laver du et antal (gerne identiske) virtuelle maskiner, jeg selv har flere forskellige, men det der er vigtigt at at du laver 4 maskiner til specifikt brug og med forskellige brugerkonti med forskellige passwords på hver maskine. Du bør lave:

En maskine til Net bank og sikker kommunikation med det offentlige (e-postkasse og dit offentlige certifikat)

En maskine til email og almindelig brugsrelateret informations surfing (ikke prono og pirat software)

En maskine til net handel

En maskine til skidt, porno, fildeling, messenger, online spil, mm.

Du tager et snapshot af alle disse maskiner, de skal selvfølgelig alle sikres maksimalt og alle kun have den software på der er nødvendigt. Så ofte det er muligt vender du tilbage til dit første snapshot, idet du skal huske at placerer din mail, dine dokumenter og andre filer på et eksternt medie da de ellers forsvinder.

Sikkerheden ved denne løsning kommer fra flere forhold. Dels tvinger den dig til at tænke over hvilken maskine du sidder på og hvad du har gang i. Dels fjerner du alt skidt og alle infektioner når du går tilbage til et snapshot og endeligt er der meget af det moderne skidt der ikke vil inficerer en virtuel maskine (virtuelle maskiner bruges nemlig af antivirus eksperterne til analyse).

Spørg alt hvad du lyster.

Der er heldigvis masser af muligheder for at spørge når man er i tvivl og for at få informationer. Brug sites som Eksperten og spywarefri og mailing lister som Bugtraq og du er også velkommen til at spørge mig via

mail på kim@bufferzone.dk hvis du har lyst. Lad være med at stille spørgsmål i artiklens kommentarer, der kan jeg jo ikke svare på dem.

Kommentar af jih d. 27. Jan 2009 | 1

Kommentar af tuidoi d. 28. Jan 2009 | 2

Godt arbejde! og mange gode idéer også.
Man kan gøre meget for at sikre sin maskine, men ens største forsvar er almindelig sund fornuft, så godt at se du tager den side med også :)

Kommentar af tomojo d. 25. Jan 2009 | 3

Jeg kan kun tilslutte mig rosen, inklusiv bemærkningen om at sætte tanker i gang..

Kommentar af jetdirect (nedlagt brugerprofil) d. 30. Jan 2009 | 4

Kommentar af forevernewbie d. 25. Jan 2009 | 5

Flot artikel, med nogle gode ideer. Er dog ikke overbevist om at Firefox og Thunder bird gør nogen stor forskel mere.

Kommentar af jokerper d. 24. Jan 2009 | 6

Hej Bufferzone
Jeg gerne rose din nyeste artikel, som jeg syntes er skrevet i et godt og let forståeligt sprog. Virkelig brugbar sætter nogle tanker igang, ihvertfald hos mig.

Kommentar af casper95 d. 25. Jan 2009 | 7

Sådan, god artikel ^^