Freeware for PC security

Indledning:

For en privat person kan det være svært at finde ud af, hvad der er godt for at kunne beskytte sin computer. Denne rapport vil prøve at dække nogle af de programmer, der er beregnet til private. Fælles for dem alle er, at de er gratis, hvis det ikke bruges kommercielt. Derudover vil der blive beskrevet nogle få, men nyttige ændringer af ens computer-opsætning for at øge sikkerheden væsentligt.

Lige for tiden bliver der snakket meget om sikkerhed omkring netværk og computere generelt. Der er fokus på orme og vira, og mange programmer til at sikre sin computer koster penge. Men der er ligeså mange, der er ganske gratis. Her følger en beskrivelse af nogle gode produkter, der klarer sikkerheden for en privat person.

1. AVG antivirus:

Programmet kommer i to versioner, en professionel og en FREE. Den professionelle koster penge og har nogle flere funktioner beregnet til firmaer. FREE-versionen kan downloades fra http://free.grisoft.com/doc/1. Den er stort set selvinstallerende, man skal kun klikke på ”Next” et par gange, så er den installeret. Der er ikke nogle ændringer, der skal laves, medmindre man vil have programmet i en anden mappe end standard-mappen.

Første gang, programmet starter op, undersøger det selv, om databasen er opdateret. Det er den normalt ikke, hvorfor man får muligheden for at vælge, hvor opdateringen skal ske; fra en folder eller internettet.

Når opdateringen er lavet, lægger programmet sig ved siden af uret og kører ellers i baggrunden. Dette er ofte sidste gang, en bruger manuelt skal starte programmet. I standard-opsætningen er den sat til at scanne alle suspekte filer, fx .exe-filer, zip-filer o.a. Det er muligt at sætte programmet op til at scanne alle filer, men det vil nedsætte computerens ydeevne væsentligt og vil ikke have nogen betydning for funktionen med at beskytte mod vira. Selve scanningen foregår i baggrunden og kører hele tiden. Det samme gælder for opdateringen af databasen med alle definitionerne. Programmet leder efter den seneste opdatering, når computeren startes op. Hvis computeren står tændt over en længere periode, sker opdateringen efter et fast interval, som kan fastsættes af brugeren. Som standard er den sat til en gang om dagen.

2. Spybot Search & Destroy/Ad-Aware antispyware:

Det er nemmere nu end før at komme på Internettet. Her ligger dog en ikke uvæsentlig fare, da mange hjemmesider installerer programmer til at registrere en brugers adfærd på nettet, et såkaldt spyware-program (eller spionprogram). Oplysninger, der indsamles om en brugers adfærd, bruges primært til at finde ud af, hvor en brugers interesse ligger, så Internet-reklamerne kan være mere målrettet mod brugeren.

Desværre findes der ikke (så vidt vides) et enkelt program, der kan fjerne alle spyware-programmer i ens computer. Der er dog to, der tilsammen fjerner stort set alt.

Ad-Aware:

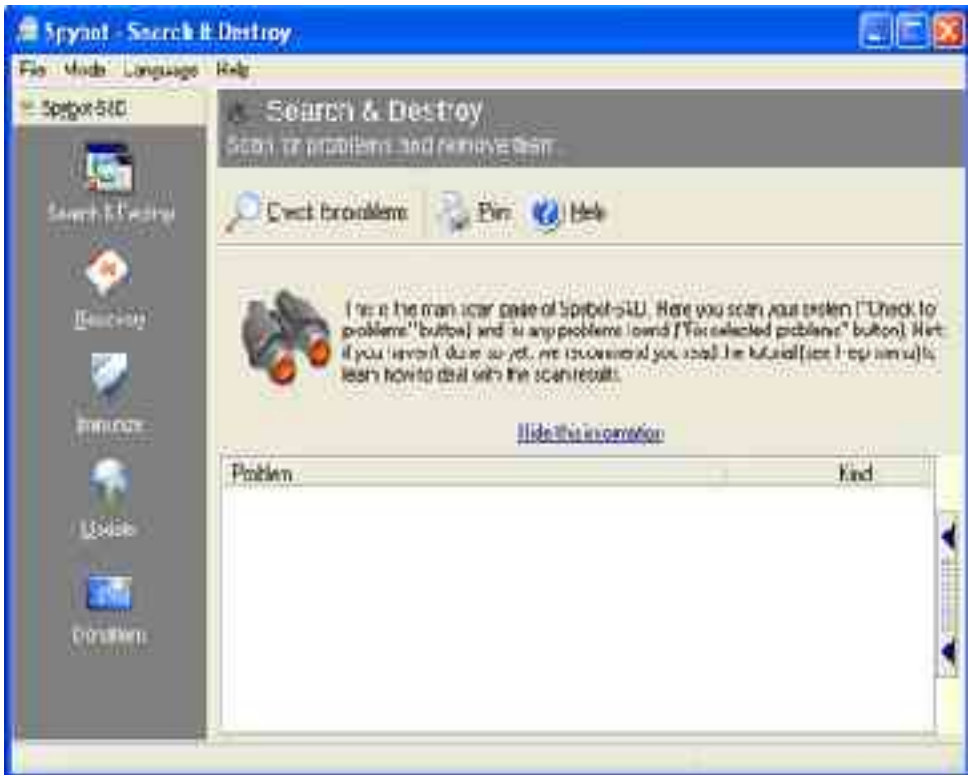
Dette program var i sin tid udviklet for at fjerne alle uønskede cookies, der blev installeret, hver gang man kom forbi en hjemmeside. Senere blev det udviklet til også at fjerne mere avancerede spyware, der indsamlede personlige oplysninger om en bruger. Dog har det den svaghed, at det ikke

går så meget i dybden, hvilket betyder, at det kun er ganske få programmer, der kører i baggrunden, der bliver fjernet med en kørsel. Programmet er ikke selvkørende, man skal selv sørge for at opdatere og køre det med jævne mellemrum. Den hjælper dog ved at fortælle, at ens definitionsfil er forældet. Det er effektivt og forholdsvis hurtigt, men det er bedst at køre det, mens computeren ikke bliver brugt. Spyware-programmerne bliver kategoriseret i to grupper, kritisk og ikke-kritisk. Alle programmerne, der bliver fundet under en kørsel, bliver sat i en af de to grupper, og det er muligt enten at slette alle programmerne eller enkelte bestemte. Det er dog anbefalet, at man fjerner alle programmerne. Der er 4 måder at lave en scanning på. Det er dog kun de to første, der er interessante, da de to andre kræver mere teknisk indsigt. Enten kan man lave en fuldstændig scanning af systemet eller en ”smart” scanning. En smart scanning scanner kun i de mapper, hvor skadelige filer som standard bliver gemt. Det er fx mappen med cookies eller midlertidige filer. En fuldstændig scanning scanner alle filer og mapper. Det er anbefalet, at man kører den fuldstændige scanning for at være på den sikre side, men den tager noget længere tid.

Ad-Aware benytter sig af en teknologi, der kaldes for Code Sequence Identifier, som er udviklet af Lava Soft. Hvad den præcis gør, er ikke forklaret nogen steder. Den benyttes, når der scannes i hukommelsen, altså scanner kun efter programmer, der ligger i hukommelsen.

Når der scannes, benytter Ad-Aware sig af en definitionsfil, som er krypteret med xor-kryptering. Selve filen er en zip-fil, der indeholder alle de definitioner, som bruges til sammenligning, når der scannes.

Spybot Search & Destroy:

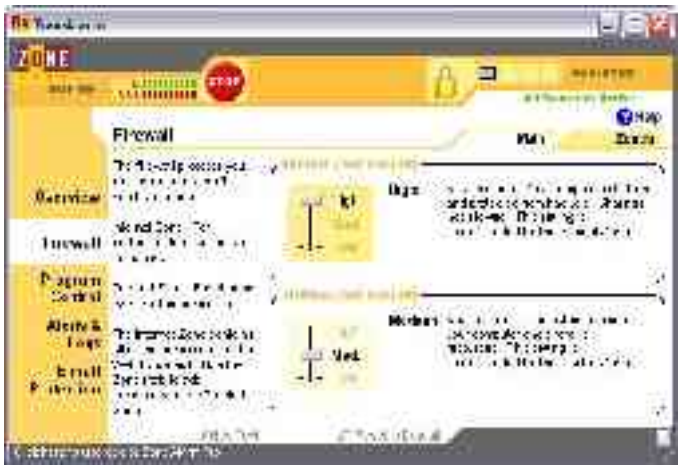


Dette programs primære funktion er at scanne efter decideret spionprogrammer, der indsamler informationerne om en bruger og sender dem videre til bagmanden. Den går helt i dybden og fjerner også alle kørende programmer. Nogle gange kræver den, at man skal genstarte for at den kan slette et program. Den scanner mapper og filer, men fjerner kun dem, der kategoriseres som et spionprogram. Desværre er der en fejl i installationen af programmet, der gør, at man skal genstarte sin computer efter installation, men før opdateringen, hvis man vil undgå, at programmet fryser. Også i dette program er det muligt at vælge, om alle fundne filer eller kun nogle bestemte skal slettes. Det er dog anbefalet at slette alt. Opdatering og kørsel sker manuelt, men der er ingen advarsel, hvis ens database er forældet. Så det er vigtigt, at opdateringen skal ske før hver enkel kørsel.

Det var ikke muligt at finde noget om Spybots søgealgoritme på nettet.

Disse to programmer supplerer hinanden meget godt, og hvis man kører dem begge med et par dages mellemrum, så vil problemet med spyware-programmer være mindre aktuel.

3. ZoneAlarm Firewall:



Dette er en simpel firewall, der er effektiv. Den giver mulighed for at bestemme hvilke programmer, der kan gå til og fra nettet, og hvilke skal blokeres. Men man kan ændre sin blokering, hvis der er sket en fejl undervejs.

Selve installationen er nem, og der er ikke mange ting, man skal tage hensyn til. Standard-opsætningen er ganske udmærket, og man behøver ikke ændre i den.

I starten kan det være lidt irriterende at have det kørende, for det spørger om et programs adgang til Internettet, hvis det ikke er i databasen. Men efterhånden er alle programmer registreret, og man lægger ikke særlig meget mærke til den.

Hvis der kommer et forsøg, hvor nogen prøver at portscanne, pinge eller komme ind i computeren på anden måde, så kommer en boks op nede ved uret, der fortæller, at en maskine med ip-adressen xxx.xxx.xxx.xxx har forsøgt at komme ind i computeren.

På den måde kan man altid forsøge at backtrace maskinen, hvis man ønsker det. At backtrace betyder, at man kan finde kilden, hvorfra forsøget er sket. Dette virker dog ikke altid, og forklaringen er udeladt, da dette ligger udenfor denne rapport emneområde. I Windows XP benyttes en kommando, der hedder ”tracert” efterfulgt af ip-adressen.

Boksen kan sættes til ikke at poppe op, men forsøget på indtrængen vil stadig blive registreret, og man kan efterfølgende gå ind og tjekke loggen.

4. Almindelig sikring af ens computer:

Med en computer med Windows-styresystem følger en standard-opsætning. Men den er ikke optimalt på nogen måder med sikkerheden, og der er nogle ting, man kan gøre for at sikre den en smule mere.

Når der startes op fra BIOS, så er computeren sat til at søge efter opstartsfiler på en diskette, derefter et cdrom-drev og til sidst harddisken. Her skal man sætte opstartssekvensen til at være harddisken først, så cdrom-drev bagefter. Diskettedrevet skal være fravalgt. Dette er for at forhindre, at der kan skaffes adgang til computeren via en cd eller diskette.

Windows har en administrator-konto, som ikke kan slettes, og navnet kan heller ikke ændres. Dette er en bagdør, der er beregnet til at hjælpe, hvis man skulle have glemt sit kodeord til sin profil. Der er som standard ikke sat kodeord på kontoen, hvorfor man bare kan gå lige ind i computeren og gøre, hvad man har lyst til. Kontoen eksisterer kun i fejlsikret tilstand.

Windows XP (og tidligere versioner) giver mulighed for, at man kan starte sin computer i en tilstand, hvor kun det mest nødvendige til at køre en computer med operativ system er læst ind i hukommelsen. Denne tilstand kaldes for en fejlsikret tilstand. I denne tilstand er det ikke muligt at køre 3. parts programmer, installere 3. parts programmer og alle drivere er deaktiveret. Der er kun grafikkortet, der har indlæst en meget simpel driver, der gør brugeren i stand til at benytte computeren med en meget lav opløsning.

For at komme ind i den fejlsikret tilstand og ændre kodeordet til administrator-kontoen kan man gøre en ud af to følgende metoder:

1. Under opstart af sin computer holdes F8-tasten nede, hvorefter en menu fremkommer, hvor man kan vælge fejlsikret tilstand.
2. Hvis computerens login-instillinger er sat til, at man skal skrive sit brugernavn og password ligesom i Windows 2000 og Windows 98, så skal ”Administrator” stå som brugernavn. Ved at trykke på ”OK”, fremkommer fejlsikret tilstand automatisk.

Når fejlsikret tilstand er startet, åbnes funktionen ”Brugere”, der giver mulighed for at oprette en bruger eller ændre i eksisterende brugeres profiler. Herinde åbnes kontoen for Administrator, hvorefter kodeordet kan ændres. Dette er med til at sikre, at bagdøren ikke er tilgængelig uden et kodeord.

I Windows XP er det muligt at skabe kontakt til en computer via fjernkontrol. Under egenskaber for Denne computer findes fanebladet, hvor Fjernkontrolstatus kan sættes. Hvis fluebenet ud for ”Fjernsupport” fjernes, så er der ikke mulighed for at oprette en fjernforbindelse til en anden computer. Hvis fluebenet ud for ”Fjernskrivebord” fjernes, så kan der ikke skabes fjernkontrol til lokalcomputeren. Det er muligt at etablere en fjernkontrol fra en hvilken som helst computer, der er forbundet med Internettet til en hvilken som helst anden computer, der også er forbundet med Internettet. Dette kræver, at begge computere giver muligheden for at oprette og etablere fjernkontrol. Mange personer har flere computere i et lokalt netværk. Dette gør, at denne funktion er god at have.

Hvis der forsøges skabt fjernkontrol fra en anden computer ved at benytte et brugernavn på computeren, der forsøges skabt forbindelse til, der allerede er aktiv på computeren, så vil forsøget mislykkes. Aktiv på en computer betyder, at brugernavnet allerede er i brug.

Under netværksinstillinger er det muligt at fravælge, at filer og printere må deles i et netværk. Dette er med til at sikre, at vira ikke så nemt kan spredes i et netværk. Men det betyder så også, at der ikke kan deles filer eller printer mellem alle computere i netværket.

Windows XP har en indbygget firewall. Den er ikke god, og duer faktisk ikke til så meget. Dog er den effektiv nok til at forhindre ping-request og andre forespørgsler udefra, men der sker intet, hvis der udsendes forespørgsler fra computeren selv. Det gør ikke noget at have den aktiveret, men det er smartest at have en anden firewall kørende samtidig for at sikre optimal beskyttelse.

Standard-mapper er gode at have, og man skal ikke bekymre sig om at oprette andre mapper eller huske, hvor man har dem liggende. Men det er en dårlig ide at benytte sig af standard-mapper til data, der ikke må slettes, af flere grunde. Det er sværere at lave backup, medmindre man ønsker at lave backup af filer og mapper, der ikke er nødvendige. En hacker vil som udgangspunkt starte med at søge i standard-mapperne efter nødvendige data.

Rigtige mænd tager ikke backup. Det duer bare ikke, når man først har mistet sine data. Og en backup behøver ikke gøres via et program. Man behøver kun at have et eller flere medier, hvor ens data kan overføres til, fx brændbart cd-medie eller en usb-nøgle. En vigtig ting er dog at have flere kopier af ens data, hvis den ene backup skulle forsvinde eller blive beskadiget, så man ikke kan genskabe dataene igen. Det optimale er at have data på både sin harddisk, usb-nøgle og cd-medie. På den måde vil man undgå, at ens backup er ubrugelig, hvis et medie går i stykker eller bliver væk.

En anden backup, der tit bliver overset, er ens mail og email-adresser. Her er en sikker, men noget besværlig fremgangsmåde. Man skal gemme sin mail som en fil, når den modtages, og man har stadfæstet, at den ikke må slettes, fx en mail med adgangskoder til et website. Denne fil vil der så blive lavet backup af med jævne mellemrum. En adressebog indeholdende email-adresser kan normalt gemmes som en kommasepareret fil. Det er noget besværligt at genskabe email-adresserne igen, da man skal copy/paste dem alle, men det er bedre end at have mistet dem.

Ens færden på Internettet er fuld af farer. Derfor er det en god ide at køre med to forskellige browsere, hvor den ene er sat op til højeste sikkerhedsniveau til den almindelige surfing, og den anden er på et lavere sikkerhedsniveau, men den skal så til gengæld kun bruges på de websites, man har fuldstændig tillid til.

Konklusion:

Det er svært at beskytte sin computer, hvis man ikke lige ved, hvilke programmer er de bedste, og hvilken opsætning er den mest optimale. Der findes rigtig mange programmer på nettet, der reklamerer med, at de kan sikre ens computer bedre end den anden. Men computerens bedste sikkerhed er faktisk en fejl 40 (brugeren selv). Hvis brugeren benytter sin sunde fornuft og logiske sans, så er chancen for at få vira og indbrud i sin computer ganske minimal. Her følger nogle gode råd til, hvordan man som person kan sørge for, at sikkerheden på sin computer ryger et niveau højere:

1. Hvis du ikke kender afsenderen af en mail, så slet den uden at se indholdet. Hvis du mistænker mailen for at komme fra en af dine venner, så dobbelttjek med vedkommende enten telefonisk eller personligt, men aldrig via email.
2. Download aldrig noget fra nettet, medmindre du skal bruge det. Hvis du er i tvivl, om du skal bruge det eller ej, så er det nok, fordi du ikke skal bruge det. Og ellers spørg en person, der har forstand på det.
3. Forlad aldrig en computer uden at være logget ud eller lås den, så der skal bruges adgangskode for at komme ind.

Nogle kan undre sig over, hvorfor man skal igennem alt besværet med at gemme og lave backup af sine filer på den måde, der er beskrevet tidligere. Der findes jo masser af programmer på nettet, der kan gøre det samme for en og noget hurtigere. Men som udgangspunkt skal man aldrig stole på programmer, der er gratis, når det gælder filer, der ikke må slettes eller mistes. Det er aldrig til at vide, hvad programmet i virkeligheden gør ved ens computer; om der bliver installeret en bagdør eller andet program, der giver adgang til computeren udefra.

http://www.cprogramming.com/tutorial/xor.html
http://www.packetstormsecurity.org/0604-advisories/Ad-Aware.txt
http://www.lavasoft.com/?=ABCDEFGH
http://www.spybot.com/dk/index.html
http://www.zonealarm.com/
http://www.microsoft.com/