En ny trussel mod din computer

Computertrusler er almindeligvis upersonlige, i den forstand at din computer ikke er specielt mål for disse trusler. Alle er udsat for disse trusler.

Hacking er en anden form for trussel. Hacking er et målrettet forsøg på at overtager kontrollen med en bestemt computer, eller et bestemt netværkssystem, for eksempel et firmas netværk eller en offentlig myndigheds netværk.

Hidtil har private personers computere været forholdsvis forskånet for hacking, af den grund at der ikke er så meget at hente.

I — Ny trussel

Det har nu ændret sig efter opkomsten af, hvad der er døbt Ransomware.

"Ransom" betyder løsepenge, og ideen er at tage din computer som gidsel for at få dig til at betale for at få computeren "løsladt".

Truslen effektueres på følgende måde:

A) En hacker (der er medlem af en gruppe af sådanne, fortrinsvis i Østeuropa), skaffer sig adgang til din computer.

B) Hackeren installerer et program på din computer, der låser din adgang til vigtige filer på din computer.

C) Du får at vide, at du for et forholdsvis beskedent beløb kan få tilsendt en nøgle, der låser op for disse filer.

D) Hvis du ikke betaler, vil din computer som hovedregel være ubrugelig eller af hackeren blive gjort ubrugelig som "straf".

E) Den opkrævede løsesum er forholdsvis lille, ud fra den tankegang hos hackeren, at det er billigere for ofret at betale end at anskaffe sig en ny computer.

II — Hvad kan du stille imod denne trussel?

Jeg har læst lidt på nettet om problemet. De forholdsregler, jeg har læst om, er forholdsvis komplicerede og ikke brugbare for den almindelige privatperson, der ikke er overmåde interesseret i hvordan hans/hendes computer fungerer.

Dette afsnit er derfor mine tanker om, hvilke forholdsregler du kan tage. Det står helt for min egen regning og jeg garanterer ikke for noget som helst.

1) Hvis du bliver ramt af denne trussel, bør du melde det til politiet. Det er muligt at du hos politiet kan få andre og/eller bedre råd, end dem jeg giver her.

2) Derefter bør du kontakte en ven eller slægtning, som du tror har mere forstand på sagerne end du selv har.

3) Denne kontaktperson vil starte med at spørge ind til dine sikkerhedsprocedurer. Sandsynligheden taler for, at du ikke har nogen.

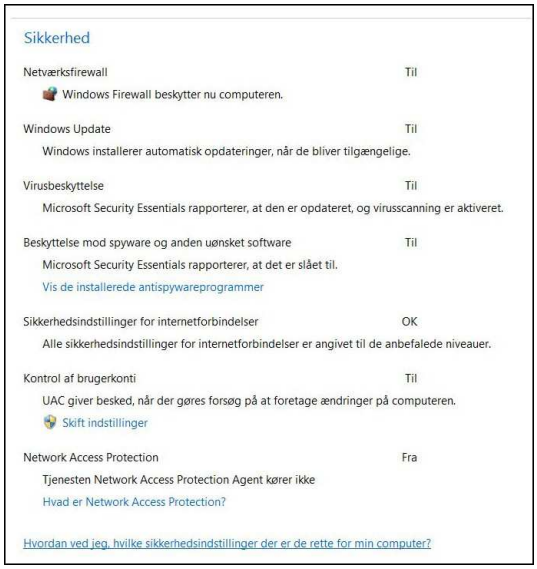
4) Hensigten med denne artikel er at forberede dig på den samtale.

III — Sikkerhedsprocedurer

1. Er din internetforbindelse via routeren forsvarlig krypteret? Manglende eller svag kryptering er det samme som at aflevere nøglerne til dit hus, din bil og din båd til en nyligt løsladt tyveknægt med et alenlangt generalieblad.

   Krypteringen finder du på følgende måde: Kontrolpanel → Netværk og Internet → Administration af trådløse netværk. Der skal stå noget med WPA, WPA-PSK el. lign.

   Er der ikke nogen kryptering, skal du rette henvendelse til din ISP [1]) for at vejledning i dette.



2. Gennemgå din sikkerhedsopsætning: Kontrolpanel → Løsningscenter → Sikkerhed.

   Opsætningen bør se ud som figuren til højre.

3. Har du oprettet en systemafbildning for nylig?

   Kontrolpanel → Sikkerhedskopiering og gendannelse. Brug dette program til følgende:

3a) Oprette en systemafbildning.

3b) Oprette en system reparationsdisk.

3c) Konfigurere din sikkerhedskopiering.

Noget om computerens D-drev

Programmer og filer, der berøres af virus, trojanske heste og hacking angreb ligger altid på harddiskens C-drev. De fleste nyere computere har foruden dette drev også et D-drev, der ligger adskilt fra C-drevet på samme harddisk. På et sådant D-drev ligger som regel nogle filer, der muliggør en gendannelse til computerens originale opsætning (fabrikstilstanden). Denne gendannelse effektueres ved et særligt tastetryk under computerens opstart.

Dette er en af de metoder, hvorpå man kan gendanne en computer efter et totalt nedbrud. Bagsiden er selvfølgelig, at alle programmer, der er installeret siden anskaffelsen af computeren og alle data der siden er oprettet, forsvinder. Det er en genfødsel af computeren, så at sige.

Du kan til nød bruge D-drevet til systemafbildning og sikkerhedskopiering, men jeg vil anbefale, at du til disse formål anskaffer en ekstern USB-forbundet harddisk. En sådan med en kapacitet på 500 Gigabyte (rigeligt plads til den almindelige private bruger) kan erhverves for 3-400 kr.

Systemafbildning: Klik på "Opret en systemafbildning" i Kontrolpanel → Sikkerhedskopiering og gendannelse. Marker C-drevet og vælg den eksterne USB-disk til at rumme systemafbildningen. OBS at det kan tage en rum tid, 1-2-3 timer, alt efter hvor meget der er på din computers C-drev.

[1] ISP = Internet Service Provider: Det firma, du køber din internetforbindelse hos, f.eks. Yousee, TDC, Profiber, Stofa m.fl.

Systemreparationsdisk: Prop en blank CD eller DVD skive i din computers DVD-drev og klik på "Opret en systemreparationsdisk" i Kontrolpanel → Sikkerhedskopiering. Den bruges til at starte computeren fra, hvis du oplever sort skærm eller andre opstartsproblemer. For at starte computeren fra denne skive er det nødvendigt at bruge et bestemt tastetryk under opstarten. Det er vist forskelligt fra maskine til maskine og er i øvrigt ikke en triviel øvelse. Få fat på computerens manual eller en nørd blandt dit bekendtskab.

Sikkerhedskopiering: I Kontrolpanel → Sikkerhedskopiering og gendannelse finder du et link, der gør det muligt for dig at oprette en tidsplan for sikkerhedskopieringen samt vælge, hvor sikkerhedskopien skal bero. Jeg foreslår en gang om ugen og kopiering til en ekstern harddisk.

Vælg et tidspunkt, hvor du ikke bruger computeren, for eksempel søndag morgen kl. 3, og undlad at slukke for computeren lørdag aften. (Sluk bare for skærmen for at spare lidt strøm).

En gang om måneden klikker du på "Administrer plads" for at sikre dig, at der er tilstrækkelig med plads på harddisken. Slet evt. de ældste sikkerhedskopier.

IV — Og hvad så, hvis ulykken kommer til min computer?

Ovenstående beredskabsplan vil betyde at du i fremtiden er klædt på til at håndtere eventuelle nedbrud på din computer, hvad enten der nu er tale om et udefra kommende problem eller det skyldes at du har gjort et eller andet fjollet ved din computer.

Det er langtfra sikkert, at du selv kan udrede sagerne, men som allerede nævnt vil tilkaldehjælp være langt bedre rustet til at ordne det, hvis du selv har gjort det forberedende arbejde.

V — Hvad du selv kan gøre

Oplever du problemer med din computer, kan du selv foretage dig forskellige simple ting, inden du tager tungere skyts i brug. Der ikke grund til at bruge en tunnelboremaskine hvis en Black & Decker håndboremaskine fra Silvan kan klare det.

Gør din computer knuder, gør da følgende i rækkefølge ind til problemet er løst:

1) Scan din computer med dit virusprogram og evt. med de programmer, jeg beskriver længere nede.
2) Genstart ved hjælp af den lille pil til højre i "Luk computeren"-knappen.
3) Luk computeren ved at holde Tænd-knappen nede ind til lyset går ud. Start igen efter 20 sekunders pause. Vælg "Start Windows normalt".
4) Tag batteriet ud (af din bærbare) og gentag punkt 2.
5) Foretag en systemgendannelse: Kontrolpanel → Genoprettelse.

Følgende programmer kan anvendes til en dyberegående hovedrengøring af computeren. De bør anvendes i den angivne rækkefølge:

1) Malware Bytes (https://www.malwarebytes.org/). Download og installer gratisversionen. Programmet er en tand skarpere end de almindelige antivirus programmer.
2) Ccleaner (http://www.piriform.com/ccleaner) er et program, der tilbyder flere forskellige funktioner for at rense computeren for filer, der ikke har nogen aktuel funktion. Det er ikke et antivirus-program. Husk at vælge dansk sprog version.
3) Adwcleaner (https://toolslib.net/downloads) er et program, der er meget effektivt til at fjerne uønskede reklamer og programer, der sniger sig ind "på ryggen" af andre programmer. Et markant og velkendt eksempel er Ask.com, der sniger sig ind i forb. med installationen af en Java opdatering, medmindre man er påpasselig.

   Obs at programmet ikke skal installeres, men eksekveres direkte fra den downloadede fil.

23/1/2015