



Beveiligen doe je zelf

Of het nu gaat om bronbescherming of het stoppen van luistervinken, een goed beveiligd systeem is voor journalisten een must. Anoniem surfen op internet, je USB-stick versleutelen of een firewall installeren. Met de volgende tien tips van Certified Secure wordt dat een koud kunstje. Ze helpen je bij het beveiligen van je computer, communicatie en gegevens. Bovendien beschermen ze je privacy.

1. Beveilig je communicatie met PGP en OTR

Waarom: Voor zowel journalisten als bronnen is het van belang om op een veilige en private wijze te communiceren.

Oplossing: Door je communicatie te versleutelen kan niemand die afluisteren. Voor Instant Messaging is er de chatclient Pidgin in combinatie met de OTR (Off the Record) plugin. Deze combinatie werkt met de meeste chatdiensten. Voor e-mail is er het programma Thunderbird in combinatie met de Enigmail uitbreiding en GnuPG software. Voor wie ook zijn VoIP-gesprekken wil versleutelen, is er het programma Zfone.

<http://www.pidgin.im/>

<http://www.cypherpunks.ca/otr/>

<http://enigmail.mozdev.org/>

<http://www.gnupg.org/>

<http://www.zfone>

2. Versleutel je complete harde schijf

Waarom: Iedere laptop kan door een dief gestolen worden, maar ook in beslagname door politie of douane is een mogelijkheid. Als iemand fysieke toegang tot je computer heeft, heeft hij of zij ook toegang tot alle gegevens die erop staan. Windows wachtwoorden bieden namelijk geen bescherming tegen een aanvaller die fysieke toegang heeft, in tegenstelling tot een volledig versleutelde harde schijf, waar je gegevens wel beschermd zijn.

Oplossing: Met de Full Disk Encryption optie van TrueCrypt kun je de hele harde schijf versleutelen. Voor toegang tot je gegevens zul je eerst een passphrase moeten invoeren. <http://www.truecrypt.org>



3. Update alle software

Waarom: Eén van de voornaamste redenen dat systemen met malware besmet raken komt door het gebruik van verouderde software. Beveiligingslekken in programma's zoals Windows, Internet Explorer, Adobe Flash, Adobe Reader, Apple QuickTime en Oracle Java, zorgen ervoor dat aanvallers direct toegang tot het systeem kunnen krijgen.

Oplossing: Gelukkig is dit met een beetje zelfdiscipline en handige software eenvoudig op te lossen. Gebruik Windows Update voor het updaten van Windows en Microsoft Office. Gebruik de Secunia Online of Personal Software Inspector voor alle overige software.

<http://www.secunia.com> (scan now of download PSI)

<http://windowsupdate.microsoft.com>

4. Gebruik TOR voor anoniem surfen

Waarom: Alleen het bezoeken van een website geeft een webmaster allerlei interessante informatie. Deze informatie is te combineren en te herleiden naar een individuele gebruiker. Daarnaast heerst er in sommige landen censuur waardoor bepaalde sites niet zijn te bezoeken of wil je niet dat anderen weten welke websites je bezoekt.

Oplossing: Met TOR kun je grotendeels anoniem surfen en gecensureerde websites toch bezoeken.

<http://www.torproject.org>

5. Beveilig je browser en surfgedrag

Waarom: De browser is het favoriete doelwit van een aanvaller, hiermee kan hij toegang krijgen tot bijvoorbeeld je webmail, creditcardgegevens of internetbankieren. Daarnaast kun je via de browser veel persoonlijke gegevens lekken.

Oplossing: Gebruik Firefox met minimaal de onderstaande plugins. Ook kun je met Scroogle en IxQuick anoniem zoeken en geeft 10 Minute Mail je een tijdelijk e-mailadres. Handig om je ergens snel te registreren.

<http://www.getfirefox.com>

<https://addons.mozilla.org/en-US/firefox/addon/722/> (NoScript)



<https://addons.mozilla.org/en-US/firefox/addon/60333/> (GoogleSharing)

<http://www.ixquick.com>

<http://scroogle.org/>

<http://www.10minutemail.com>

6. Versleutel je USB-stick

Waarom: USB-sticks bevatten vaak gevoelige gegevens, maar zijn door hun kleine omvang eenvoudig te verliezen. Vertrouwelijke informatie komt zo letterlijk op straat te liggen.

Oplossing: Met de Traveller Disk optie van TrueCrypt kun je de hele harde schijf versleutelen en moet je eerst een passphrase invoeren voordat je toegang tot de gegevens krijgt. <http://www.truecrypt.org>

7. Gebruik Eraser en DBAN

Waarom: Het naar de prullenbak slepen van bestanden of formatteren is niet voldoende om gegevens permanent te verwijderen. Via op het internet verkrijgbare programma's zijn ze eenvoudig te achterhalen.

Oplossing: Gebruik Darik's Boot and Nuke (DBAN) of Eraser om gevoelige gegevens permanent te verwijderen.

<http://www.dban.org>

<http://eraser.heidi.ie>

8. Schakel Autorun uit

Waarom: Autorun is de Windows functie die automatisch USB-sticks, cd-roms en externe harde schijven start. Veel malware gebruikt juist deze functie om systemen te infecteren en infiltreren.

Oplossing: Schakel de functie uit en benader je datadragers handmatig. In Windows 7 en Vista kun je dit doen via het Configuratiescherm en dan het Automatisch afspelen menu. Schakel het selectievakje Automatisch afspelen voor alle media en apparaten gebruiken uit en klik op Opslaan. Voor Windows XP heeft Microsoft een pagina met uitleg.

<http://support.microsoft.com/kb/967715/nl>



9. Installeer een virusscanner

Waarom: Als journalist download je regelmatig bestanden van het internet of ontvangt die per e-mail. Een virusscanner kan controleren of er geen malware in verstopt zit. Virusscanners zijn niet in staat om alle malware te detecteren, daarom is het belangrijk om altijd voorzichtig te zijn met ongevraagde links en bijlagen.

Oplossing: Er zijn verschillende aanbieders van virusscanners, zowel commercieel als gratis. Toch zit er niet veel verschil tussen de meeste aanbieders. Wel zit er een verschil tussen virusscanners en Internet Security Suites. De laatste beschikken vaak ook over een firewall, aanvullende filters, uitgebreidere opties om malware te detecteren en ondersteuning.

http://www.microsoft.com/security_essentials/ (gratis)

<http://www.avast.com/free-antivirus-download> (gratis)

<http://www.symantec.com> (commercieel)

<http://www.gdata.nl/> (commercieel)

10. Installeer een firewall

Waarom: Een firewall moet voorkomen dat aanvallers of malware toegang tot het systeem krijgen of op een systeem informatie naar buiten kunnen sturen.

Oplossing: Windows beschikt standaard over een firewall. In het geval van Windows XP is die vrij karig, aangezien die geen uitgaand verkeer blokkeert. De firewalls in Windows Vista en Windows 7 zijn uitgebreider en geven gebruikers meer opties. In plaats van de standaard Windows firewall kun je ook een gratis/commerciële firewall gebruiken, zoals Online-Armor.

<http://www.online-armor.com/> (gratis en commerciële versie)

Conclusie

Met deze tien tips wordt het beveiligen van je systeem en gegevens een stuk eenvoudiger, terwijl het voor kwaadwillenden lastiger wordt om je data te bemachtigen. Vergeet ze niet toe te passen, want voorkomen is nog altijd beter dan genezen, ook als het om digitale beveiliging gaat.