De tien geboden voor veilig surfen op het World Wide Web

1. Zorg voor een virusscanner en scan regelmatig

Omdat het even duurt voordat antivirusprogramma's nieuwe virussen herkennen, ontsnappen er wel eens nieuwe virussen aan het oog van een virusscanner. Zorg er dus voor dat altijd de laatste versie van je antivirusprogramma op je computer staat en wees zelf ook altijd waakzaam. Houd er rekening mee dat bij gratis versies van virusscanners, de updates niet altijd accuraat zijn en op tijd worden aangeboden.

Krijg je een document via e-mail of wil je bestanden vanop een usb-stick op je computer plaatsen? Scan deze altijd even voor je ze opent. Dit kan eenvoudigweg via je virusscanner.

Virussen worden niet alleen via mail of bij het uitwisselen van bestanden verspreid, een bezoek aan een onbekende of valse website is soms voldoende om je computer te besmetten. Hiervoor zijn torrents- en pornosites veruit de meest gekende besmettingshaarden.

Voor professionele organisaties is het aan te raden om verschillende types van antivirusproducten te implementeren, waarbij de frequentie van het installeren van nieuwe "signatures" hoger ligt, en bijvoorbeeld om de 5 minuten een nieuwe antivirushandtekeningen binnengehaald wordt.

Opgelet:

Ga bij het bezoeken van een website nooit in op een voorstel of een melding voor de installatie van antivirus of andere softwareproducten. Vaak leidt dit tot de installatie van malafide software.

Welke risico's beperk je hiermee?

Hiermee hou je het risico op spionagesoftware, Trojaanse paarden, enzovoort min of meer onder controle. Je beperkt het risico om ongewild deel uit te maken van een botnet. In het jargon wordt een computer die deel uitmaakt van een botnet een zombie genoemd.

2. Hou je computer en je programma's automatisch up-to-date

Kijk de instellingen van je computer, tablet en smartphone na en zet waar mogelijk de auto-update aan of voer regelmatig het proces uit om de updates uit te voeren.

Een aantal programma's zoals Adobe PDF reader, Java, Flash Player, apps uit een appstrore of verschillende browsers zoals Internet Explorer, Firefox en Chrome, bieden zelf ook automatische updates aan.

Welke risico's beperk je hiermee?

Hiermee beperk je het risico dat hackers of botnets via gekende zwakheden in de software de controle verwerven over wat je als persoon uitvoert op je computer, smartphone of tablet.

3. Maak regelmatig een reservekopie op een externe harde schijf

Maak een reservekopie op één of verschillende externe harde schijven. Bewaar deze op een veilige plek en koppel de reservekopie **steeds los** van je computer of netwerk. Zo beperk je het verlies aan waardevolle data bij een besmetting met 'ransomware'. Met behulp van deze malafide software persen hackers hun slachtoffers af door alle folders op hun pc en aangesloten harde schijven te versleutelen. Om je documenten, foto's en alles wat je hebt opgeslagen vrij te krijgen, vragen ze een betaling in Bitcoins. Meestal gaat het om een valstrik en het is beter om hier niet op in te gaan.

Welke risico's beperk je hiermee?

Bij technische problemen of wanneer je computer besmet is met "ransomware", kun je terugvallen op een kopie zodat je al je data niet finaal kwijt bent.

Dataverlies in het algemeen.

4. Wees wantrouwig

Wees steeds op je hoede wanneer je iets gratis aangeboden krijgt. Dit kan gaan van een pop-up met een uitzonderlijke aanbieding die je uitnodigt om webpagina's te bezoeken tot mailtjes of een telefoonoproep. Ga hier niet zo maar op in. Gebruik je gezond verstand. Als je de verzender kent en de mail lijkt je verdacht, neem dan contact om te checken of de mail wel degelijk van deze persoon afkomstig is.

Een bezoek aan een onbekende of valse website is voldoende om je computer te besmetten. Hiervoor zijn de torrents- en pornosites gekende besmettingshaarden.

Wees wantrouwig wanneer je via mail een bestandje ontvangt, zelfs van iemand die je kent, of wanneer je een usb–stick met de post ontvangt. Indien je er niet gerust op bent, neem dan contact met de verzender. Een usb-stick kan immers besmet zijn met een virus dat niet door de antivirussoftware wordt herkend. Dat wordt 'spear phishing' genoemd. Wees om dezelfde reden ook voorzichtig met het laten rondslingeren van usb-sticks.

Ga ook altijd verstandig om met wat je op sociale media en op internet publiceert. De 'hacking community' maakt bij doelgerichte aanvallen vaak gebruik van gegevens die ze over personen vinden op het internet. Dit heet social engineering. Google is een van de databanken die door hackers het meest gebruikt wordt en het is volledig gratis.

Het voorkomen van doelgerichte aanvallen is niet alleen een technisch gegeven van firewalls, antivirussoftware en andere tools. Hoewel deze ook noodzakelijk zijn, speelt de manier waarop je omgaat met informatie en hoe je je gedraagt op het internet en de informatie die je onbewust ter beschikking stelt van hackers ook een grote rol. Aan de hand van de data die hackers aantreffen over personen en/of organisaties op het internet gebruikt de hacking community de informatie om de standaard veiligheidssystemen (antivirus, firewalls, inbraakdetectie,...) te misleiden. Deze techniek is in het jargon gekend onder noemer van "social engineering" om als uiteindelijk doel mensen te misleiden en/of organisaties te infiltreren.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact van dataverlies, virussen, malware en spionage.

5. Installeer alleen software van een betrouwbare bron

Download een programma nooit van de eerste de beste website die door zoekmachines (zoals Google) wordt weergegeven, maar download enkel van de officiële website van de maker van het programma.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact van dataverlies, virussen, malware en spionage.

6. Gebruik sterke wachtwoorden, hergebruik ze niet, deel ze nooit en vernieuw ze regelmatig

De gouden regel is: hoe langer en complexer het wachtwoord, hoe veiliger.

Gebruik een wachtzin in plaats van een woord: een lange zin is eenvoudig om te onthouden én veiliger.

Je kan ook een beroep doen op programma's, de zogenaamde 'wachtwoordkluizen', om het wachtwoord voor jou aan te maken en te onthouden.

Hernieuw op regelmatige basis je wachtwoorden. Probeer bij registratie op websites steeds andere wachtwoorden en mailadressen te gebruiken.

Naast je wachtwoord geef je bijvoorbeeld ook een code in die alleen jij via je gsm toegestuurd krijgt. Deze mogelijkheid kan je vaak zelf activeren binnen het programma of bij de website waarmee je werkt.

De antwoorden op geheime vragen die je kan invullen om je wachtwoord extra te beveiligen of te resetten, zijn eenvoudig te raden. Moet je dit toch invullen, dan antwoord je best niet op de vraag, maar geef je een fictief antwoord. Onthoud dit zelf goed of maak gebruik van een wachtwoordkluis.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact in het geval er misbruik van je account en maak je het hackers moelijker om op het net gehackte wachtwoorden en accounts te hergebruiken.

7. Surf via https indien je wil voorkomen dat de communicatie wordt afgeluisterd

Wanneer https:// in je browser staat als begin van de site die je wenst te bezoeken dan werk je met een beveiligde verbinding. Indien hierbij een foutmelding verschijnt dat het certificaat niet correct is, dan is deze verbinding niet meer veilig.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact van dataverlies en het afluisteren van de verbinding.

8. Beveilig je Wi-Fi-netwerk thuis

Beveilig je netwerk thuis met een wachtwoord.

Zo kan niemand, of het nu cybercriminelen of je buren zijn, gebruik maken van je draadloos internet.

Welke risico's beperk je hiermee?

Hiermee beperkt je de impact van dataverlies en het afluisteren van de verbinding.

9. Zorg dat het geheugen van je toestel volledig gewist is wanneer je het niet meer wenst te gebruiken

Het geheugen van je smartphone of tablet maak je leeg via de optie "wissen" op je toestel. Je computer of laptop wis en formatteer je best volledig. Een snelle "format" is geen goed idee, dan blijven er altijd gegevens achter. Laat je eventueel assisteren door een IT-expert om een grondige format uit te voeren.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact van dataverlies en voorkom je dat gebruikersnamen en wachtwoorden in de verkeerde handen vallen.

10. Wees waakzaam wanneer je openbare Wi-Fi gebruikt

Online betalen of wachtwoorden ingeven van belangrijke accounts, zoals je e-mail, doe je best nooit wanneer je op een onbeveiligd draadloos netwerk werkt.

Welke risico's beperk je hiermee?

Hiermee beperk je de impact van dataverlies en het afluisteren van de verbinding.

Bronnen

(https://www.safeonweb.be/nl/tips)

(https://cert.europa.eu/cert/alertedition/en/malware.html)

(https://pentestmag.com/the-cyberwar)