Thema Fraude – Ethiek – Integriteit
Tekst Ing. Jan Hendrikx MSc RE CISA CISSP CRISC CISM
Björn Walrave RO CIA
Beeld Adobe Stock

Tien tips om veilig te internetten

Wapen u tegen digitale bedreigingen! Word geen slachtoffer van hackers, ransomware en cyberspionage, maar internet veilig. Hoe? Door deze tien tips op te volgen.

Het zal je maar gebeuren. Op een ochtend start je, zoals op iedere doordeweekse ochtend, nietsvermoedend je laptop op. Je hebt een drukke dag voor de boeg: voor een belangrijke audit moet een rapportage worden opgeleverd. Eerst maar even koffie halen, terwijl de laptop verder laadt. Je vertrekt voor de korte wandeling naar het koffiezetapparaat. Op het moment dat je even later met een gevulde mok weer achter je laptop kruipt, blijkt dat die helemaal niet is opgestart. In plaats daarvan wordt een vreemd rood scherm weergegeven. Een scherm met een slotje en een klok die aftelt. De boodschap is even helder als zorgwekkend: al je bestanden zijn versleuteld en pas weer raadpleegbaar nadat je hebt betaald. Het angstzweet breekt je uit. Je bent het slachtoffer van ransomware!

Ver-van-mijn-bedshow

Klinkt dit als een ver-van-mijn-bedshow? Toch zijn we in toenemende mate doelwit van cybercriminaliteit. Beroepscriminelen leggen met (Internet of Things) DDoS-aanvallen websites plat of gijzelen met behulp van ransomware, zoals Cryptolocker en WannaCry, kritische data van organisaties voor losgeld. Statelijke actoren krijgen door middel van cyberspionage waardevolle informatie in handen en weten tegenwoordig zelfs door middel van hacking democratische processen te beïnvloeden.
Organisaties lijken zich in toenemende mate bewust van de risico's en voeren maatregelen door. Lang niet alle risico's kunnen echter technisch worden afgevangen. De digitale weerbaarheid van organisaties valt of staat in grote mate met het gedrag van haar medewerkers. Een mooi object van onderzoek voor audit dus. We moeten er daarnaast als auditors natuurlijk ook voor waken dat we zelf slachtoffer worden en daarmee onze organisatie in gevaar brengen. Daarom tien tips om veilig te kunnen internetten.

1 Installeer een virusscanner

Een virusscanner scant de bestanden op uw computer op tekenen van infectie, waarschuwt u wanneer malware wordt aangetroffen en geeft u in sommige gevallen de optie de malware direct te verwijderen of in quarantaine te plaatsen. Verreweg de meeste organisaties dwingen het gebruik van een virusscanner in de zakelijke omgeving af. Het is echter verstandig ook buiten deze omgeving gebruik te maken van een virusscanner. Hierbij is het tevens belangrijk dat u de virusdefinities up-to-date houdt.

2 Activeer uw firewall

Een firewall controleert inkomende en uitgaande pakketten met informatie en blokkeert verdachte pakketten. Organisaties maken doorgaans gebruik van firewalls en ook uw internetserviceprovider dwingt in de meeste gevallen gebruik van een in uw modem geïntegreerde firewall af. Zowel thuis als op uw werk bent u over het algemeen dus goed beschermd. Onderweg bent u echter kwetsbaarder. Firewalls maken vaak deel uit van anti-virus software, maar moeten in sommige gevallen wel separaat worden geactiveerd.

3 Gebruik sterke en unieke wachtwoorden

Het belang van sterke wachtwoorden wordt door veel mensen nog onderschat. Zo kan een wachtwoord dat louter bestaat uit een Engels of Nederlands woord door hackers vaak binnen enkele seconden worden gekraakt. Kijkt u maar eens op https://howsecureismypassword.net/ (vul hier vanzelfsprekend nooit uw echte wachtwoorden in, u weet nooit wat er met uw invoer gebeurt). Daarnaast weten

cybercriminelen soms de volledige gebruikersbestanden van organisaties te kapen. Zo bleek vorig jaar dat hackers al in 2013 de namen, wachtwoorden en telefoonnummers van alle 3 miljard (!) gebruikers van Yahoo! hadden gestolen. Hackers proberen gestolen wachtwoorden uit op andere diensten, zoals online winkels of betalingssystemen. Dit in de wetenschap dat nog altijd veel mensen hetzelfde wachtwoord gebruiken voor verschillende diensten. Het is dus van groot belang dat u sterke en unieke wachtwoorden gebruikt. Een zogenoemde passwordmanager kan u hierbij helpen, maar het gebruik ervan creëert natuurlijk tegelijkertijd een 'single point of failure'. De keuze is aan u. Wat u ook doet, log in ieder geval nooit in bij een dienst gebruikmakend van een publieke computer, zoals u die aantreft in internetcafés en bibliotheken. Met deze computers kan gerommeld zijn en ze zijn daarom niet te vertrouwen.

4 Activeer two-factor authentication (2FA)

Steeds meer diensten bieden 2FA aan. Hierbij dienen gebruikers twee stappen te doorlopen om in te loggen. De eerste stap is gerelateerd aan iets wat u weet, doorgaans uw gebruikersnaam en wachtwoord. De tweede stap is gerelateerd aan iets wat u hebt of wat u bent. Dit kan bijvoorbeeld een code zijn die u ontvangt op uw smartphone of uw vingerafdruk. 2FA zorgt voor veel meer veiligheid. Activeer 2FA dus daar waar mogelijk.

5 Beheer uw wifinetwerken

Uw computer en smartphone houden voor u een lijst bij van wifinetwerken waar u in het verleden op bent ingelogd. Dat is handig, want zo wordt uw systeem de volgende keer dat u op een bepaalde plek bent direct weer verbonden met het betreffende netwerk. Hackers weten echter soms op vernuftige wijze gebruik te maken van deze functionaliteit. Zo kunnen zij u verleiden verbinding te maken met hun kwaadaardig netwerk, door dat netwerk een voor u reeds bekende netwerknaam te geven. Hierna kan de hacker iedere beweging die u maakt op internet op de voet volgen. Het is dus zaak om uw wifinetwerken te beheren. Een algemene tip daarbij is dat uw openbare wifinetwerken zo min mogelijk probeert te gebruiken en na gebruik direct weer verwijdert. Maak bovenal nooit verbinding met wifinetwerken die u niet vertrouwt.

6 Maak zoveel mogelijk gebruik van end-to-endencryptie

Bij end-to-endencryptie worden pakketten met informatie versleuteld op het systeem van de verzender en pas ontsleuteld op het systeem van de ontvanger (die hiervoor uiteraard over de geheime sleutel moet beschikken). U herkent het aan het slotje in de adresbalk van uw browser. Een alternatieve wijze om een dergelijke versleutelde verbinding op te zetten is door gebruik te maken van een virtual private network (VPN) dienst. Wanneer u gebruikmaakt van een dergelijke dienst verloopt al uw internetverkeer versleuteld tot aan de server van de VPN-provider, zelfs wanneer u (per ongeluk) met een kwaadaardig wifinetwerk verbonden bent.

7 Blokkeer advertenties

Organisaties verhuren soms een deel van hun website aan advertentienetwerken. Deze advertentienetwerken plaatsen vervolgens op de gehuurde ruimte (maatwerk)advertenties. Hackers proberen via deze advertentienetwerken

advertenties met kwaadaardige codes op allerlei websites geplaatst te krijgen. Dit doen zij bijvoorbeeld door legitiem advertentieruimte in te kopen of door advertentienetwerken te hacken. Wanneer een website een besmette advertentie aan u toont, kan hierdoor op de achtergrond malware op uw systeem worden geïnstalleerd. In 2016 waren gedurende ongeveer een dag de bezoekers van bijna driehonderd Nederlandse websites, waaronder Nu.nl, Buienradar en Marktplaats, het doelwit. Besmette advertenties die via deze sites werden aangeboden, lieten bezoekers ongemerkt verbinding maken met een exploitkit, die vervolgens malware probeerde te installeren gebruikmakend van een aantal bekende kwetsbaarheden in onder meer Internet Explorer en Flash Player. U kunt door gebruik te maken van 'ad blockers' voorkomen dat uw systeem op deze wijze besmet raakt. In Nederland wordt hier steeds meer gebruik van gemaakt. Vanzelfsprekend raakt dit tegelijkertijd de websites die hun inkomsten halen uit het verhuren van advertentieruimte.

8 Verwijder kwetsbare plug-ins

Plug-ins als Flash Player, Shockwave Player, Silverlight en Java bevatten vaak veel onbekende (ofwel 'zero day') kwetsbaarheden waar hackers hun voordeel mee kunnen doen. Zo kunnen ze in sommige gevallen uw computer overnemen en toevoegen aan een zogenoemd botnet. Uw computer voert dan in opdracht van de hacker opdrachten uit, zoals het verspreiden van spam of malware, zonder dat u dat zelf merkt. Indien u dergelijke kwetsbare plug-ins niet absoluut nodig heeft, is het beter ze te verwijderen.

9 Update regelmatig uw software

Hackers maken ook gebruik van kwetsbaarheden in software. De WannaCry ransomware die vorig jaar zomer uitbrak en meerdere bedrijven hard trof, is daar een sprekend voorbeeld van. WannaCry maakte gebruik van een kwetsbaarheid in het besturingssysteem Windows en heeft in de korte tijd dat het actief was flink weten toe te slaan. Zo werd kritische apparatuur van de National Health Service in Engeland totaal onbruikbaar, vertoonden de schermen langs de perrons van Deutsche Bahn enkel nog het befaamde ransomwarescherm en moesten Nissan en Renault hun productie noodgedwongen tijdelijk stilleggen. Microsoft had drie maanden voorafgaand aan het uitbreken van WannaCry al een security patch beschikbaar gesteld waarmee de betreffende kwetsbaarheid kon worden verholpen. Die was helaas niet door iedereen geïnstalleerd, getuige het feit dat WannaCry binnen een dag ruim 230.000 computers in 150 landen wist te besmetten. Het bewijst maar weer eens dat al die waarschuwingen van uw besturingssysteem om te updaten niet voor niets zijn!

10 Maak back-ups

We kunnen het niet vaak genoeg zeggen: maak back-ups! Mochten hackers er namelijk toch in slagen uw systeem te compromitteren, dan bent u in ieder geval niet al uw data kwijt. Wij adviseren hierbij de 3-2-1 back-upregel te volgen. Maak drie back-ups van uw data, bewaar die back-ups op twee verschillende soorten gegevensdragers en bewaar één back-up op een externe locatie (of in de cloud).

Zo kan een wachtwoord dat louter bestaat uit een Engels of Nederlands woord door hackers vaak binnen enkele seconden worden gekraakt

Helaas kunnen we ook degene die alle tien de tips voor veilig internetten volgen, niet garanderen dat ze nooit slachtoffer zullen worden van cybercriminaliteit. De tips helpen weliswaar, maar bieden nooit absolute zekerheid. Tegelijkertijd geldt dat de toepassing van een combinatie van de besproken maatregelen sterker is dan iedere individuele maatregel op zichzelf. We kunnen slechts ons best doen om ons zo goed mogelijk te wapenen tegen de bedreigingen op het internet. En dat laatste is wel nodig, want een ver-van-uw-bedshow is het inmiddels al lang niet meer! <<

Jan Hendrikx is ondernemer op het gebied van technische informatiebeveiliging. Hij voert technische beveiligingsonderzoeken uit en adviseert organisaties over de wijze waarop zij hun beveiliging tegen onder meer cybercriminaliteit kunnen optimaliseren.
jan@hendrikx-itc.nl

Björn Walrave is zelfstandig gevestigd organisatieadviseur, docent, trainer en coach en daarnaast redactielid van *Audit Magazine*.
bjorn.walrave@auditability.nl