



‘Elk bedrijf is vatbaar voor computervirus’

De bollenteler is zich nog te weinig bewust van de gevaren en mogelijke gevolgen van een virusbesmetting op de bedrijfscomputer. Foutieve linkjes en bijlages zijn steeds lastiger te herkennen, het is vrijwel onmogelijk om te voorkomen dat het een keer misgaat, stellen softwarespecialisten. “De mens is vaak de zwakste schakel in dit proces”, waarschuwen zij.

Tekst: Annemarie Gerbrandy | Fotografie: René Faas

Computervirussen

- Malware is elke software die wordt gebruikt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen.
- Ransomware is een type malware die een computer blokkeert of bestanden versleutelt. Pas als je losgeld (ransom) betaalt, kan je de computer of bestanden weer gebruiken.
- Phishing is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank) website, die een kopie is van de echte website, om ze daar te laten inloggen met inlognaam en wachtwoord of creditcard-nummer.

Dit jaar zijn tien miljoen virussen (malware, ransomware) op de markt gezet, met een globale schade van ongeveer elf miljard euro, zegt Peter van Grieken, directeur van VG Automatisering in Breezand. “Tegenwoordig komt veel malware binnen doordat op een verkeerd linkje op een website wordt geklikt of doordat er een vervuilde bijlage bij een e-mail wordt geopend. Wanneer dat je overkomt, is het zeer belangrijk dat je kan teruggevallen op een goede en actuele back-up.” Sommige bloembollentelers hebben hun automatisering uitbesteed aan een IT-bedrijf dat voor de beveiliging van de computers zorgt, aldus softwarespecialist Edwin Hauwert van Automated4U uit Wervershoof. Maar hoe de data zijn beveiligd en of die zijn beveiligd, daar hebben ze vaak geen kijk op, zegt hij. “Ook zien we bedrijven waar de IT wordt beheerd door een ‘handige’ medewerker of door een kennis met verstand van computers, maar waar weinig aan beveiliging wordt gedaan. De teler komt hier pas achter als het te laat is. Zo is het afgelopen jaar een bloembollenbedrijf getroffen door een cryptovirus en bleek ook dat de back-ups niet optimaal waren.”

PHISHING MAILS

Mark Lammers van Hexapole in Beverwijk waarschuwt voor phishing mails. “De ontvanger krijgt een e-mail van een onbekend persoon die zich bijvoorbeeld voordoeft als iemand van Microsoft. Deze persoon vraagt om gegevens om in te loggen in je pc. Voor je het weet, heb je een hacker toegang tot je computer gegeven.” Volgens Lammers vormen malware en phishing mails een grotere bedreiging dan bijvoorbeeld een hacker. “Veel mensen zijn bang voor hackers, maar dat gebeurt zelden. Een bloembollenteler is in de regel geen interessant doelwit voor hackers, maar ieder bedrijf is vatbaar voor malware of phishing mails.”

De softwarespecialisten raden bollentelers aan om bedrijfscomputers te voorzien van de laatste beveiligingsupdates, een goede en geüpdatete virusscanner en alle data minimaal dubbel te back-uppen. Voer Windows-updates altijd gelijk uit, adviseert Van Grieken. “Die bevatten vaak beveiligingsupdates, waardoor je gegevens beter beschermd blijven.” Verder is het belangrijk om een betaalde virusscanner te gebruiken. “De meeste bekende virusscanners hebben tegenwoordig een beveiliging tegen crypto, maar ook dat is geen garantie”, aldus Hauwert. “Een goede back-up is de redder als je ondanks alles toch bent getroffen. Zo doen wij onze back-ups zowel lokaal als in de cloud.”



Waarop moet de bollenteler letten zodat er geen malware zijn bedrijfscomputer binnenkomt en hoe houdt hij hackers buiten? Let op vreemde mailtjes, benadrukt Van Grieken nogmaals, en kijk naar de naam van de afzender in combinatie met het mailadres. “Soms wordt een e-mail verzonden uit naam van een eerder uit je eigen adresboek gekopieerde relatie. Als je het niet vertrouwt: niet openen en direct verwijderen. “Tegenwoordig bestaat ook het gevaar dat je wordt doorgestuurd naar nepwebsites van bijvoorbeeld een bank, waarschuwt hij. “Het lijkt er dan op dat je op de website van je bank zit. In werkelijkheid typ je jouw gegevens in op een website van een crimineel, die daarna met gebruik van je inloggegevens je rekening kan leeghalen.”

Volgens Hauwert is het openen van onbekende bestanden meestal de oorzaak van een hack. “Zo komen cryptovirussen vaak per mail binnen. Dat kan een mailtje zijn dat lijkt op een mail van de bank of de internetprovider, maar ook van een vriend of kennis die besmet is zonder dat te weten. Na het openen van het bestand in de bijlage krijg je een melding van: ‘klik op inschakelen om het bestand te kunnen lezen’. Door op ‘inschakelen’ te klikken, deblokkeer je een script en draait er een kwaadaardig programma op de achtergrond, zonder dat je dat in de gaten hebt.”

WAARDE VAN DATA

De ondernemer is zelf verantwoordelijk voor zijn data en online veiligheid, stellen de specialisten nadrukkelijk. Niet iedereen staat er altijd bij stil wat de waarde van die data is. “Bedenk voor jezelf wat het betekent als je van de ene op de andere dag niet meer bij je documenten, planning en administratie kan komen”, zegt Van Grieken. “Wat voor impact heeft dat op de bedrijfsvoering? Richt daar je beleid op. Blijf uiteraard attent, klik niet zomaar op alle buttons en gooi mails van onbekende afzenders weg als je het niet vertrouwt. Kom je op een nepsite van bijvoorbeeld je bank, klik deze weg en neem contact op met je bank om hiervan melding te doen.”

Desondanks kan het iedereen overkomen dat een computer wordt besmet met een virus. Er zijn voorbeelden bekend van bedrijven die een keer met een ransomware zijn geïnfecteerd, waarbij dat is hersteld, maar het virus een aantal weken later toch weer opduikt. Van Grieken: “Laat je pc na een infectie heel goed nakijken door een ICT-bedrijf. Wanneer er geen duidelijke aanwijzingen van een virus zijn, is herinstallatie waarschijnlijk de beste optie.” ♦