Cybercrime schaadt ook grafische bedrijven

Alex Kunst

Op internet wemelt het van de taaie stappenplannen om uw ICT-netwerk te beveiligen. Tegelijkertijd benadrukken specialisten dat elk netwerk gekraakt kan worden. Het is om moe van te worden. Intussen moet u ook nog geld verdienen met uw bedrijf. Tijd voor een andere aanpak.

Tussen alle headlines over gehackte netwerken bij multinationals en overheden vorig jaar, was daar ineens het bericht over de cyberaanval op PaperShop. De bestanden van het verpakkingsbedrijf in Charleroi waren versleuteld door internetcriminelen. Tegen betaling van losgeld in Bitcoins kreeg het bedrijf zijn gegevens terug, meldde het bericht op het scherm. De bedrijfsleiding gaf niet toe aan chantage, maar de aanval leverde een flinke kostenpost op.

Momenteel lijkt het relatief rustig. Van de honderden aanvallen op uw netwerk merkt u weinig, mits uw firewall en antivirussoftware actief zijn en uw software up-to-date is. Maar het wachten is op weer een wereldwijde aanval die computernetwerken op slot zet. Sinds het WannaCry-virus een jaar geleden toesloeg, weten we dat computercriminaliteit zich niet beperkt tot grote instanties, ook KMO'ers zijn slachtoffer. Geen bedrijf loopt ermee te koop, maar tijdens bijeenkomsten in de grafische industrie gingen in het afgelopen jaar vingers omhoog bij de vraag of er iemand was gehackt.

Onwerkbare situaties

Het grootste probleem is niet de vindingrijkheid van de boeven – iedereen kan computervirussen online kopen – maar de collectieve onverschilligheid van overheden en softwareontwikkelaars enerzijds, en de tegenstrijdige belangen van de ICT-beveiligers anderzijds. De overheid begrijpt weinig van ICT, dus daar hoeven we niet bij stil te staan. Interessanter is de houding van de softwarebouwers en systeembeveiligers. Het falen van de een is het businessmodel van de ander. Tijdens een bijeenkomst van de Nederlandse kennisvereniging CMBO met het thema "Hoe word ik hackerproof", kwam een beveiligingsexpert met adviezen als: gebruik nooit een usb-stick, zorg dat niemand uw beeldscherm ziet, plak uw webcam af en voorkom elk contact tussen smartphone.

Kortom, wie zijn netwerk wil beveiligen komt al snel in een onwerkbare situatie terecht. Netwerkbeveiligers hebben vast het beste met hun klanten voor, maar ze hebben weinig belang bij eenvoudige, permanente oplossingen. Voor sommigen van hen geldt dan ook, hoe groter het probleem, des te hoger de factuur. Ze hebben de wind mee dankzij de onwetendheid van de opdrachtgever en – het moet maar eens gezegd – de monomane keuze voor Microsoft-software.

Afkicken

Bedrijfsleven en overheid zijn collectief verslaafd aan één besturingssysteem: Microsoft Windows. Andere zakelijke software-toepassingen werken bijna uitsluitend op Microsoft-platformen. We zijn dus grotendeels afhankelijk van één software-leverancier.

Hoewel het sinds Windows 10 beter gaat, heeft Microsoft geen goede reputatie op het gebied van beveiliging. Gebruikers lopen achter met versies en updates. Microsoft kan daar van alles aan doen, maar het heeft helaas geen prioriteit. De software-gigant legt de verantwoordelijkheid bij de gebruiker, en die gebruiker ziet geen alternatief.

De achilleshiel

Zo'n alternatieve oplossing is er wel degelijk, althans voor een deel van het probleem. U komt niet snel af van CRM-, MIS- en andere Windows-software, maar u kunt een achilleshiel uit uw netwerk wegnemen. De belangrijkste toegang om in te breken loopt namelijk via e-mail en de browser. Een medewerker klikt per ongeluk op een link, en voordat u het weet is het netwerk geïnfecteerd. Door e-mail en browser alleen te gebruiken op aparte pc's die verbinding hebben met een afgesloten deel van het bedrijfsnetwerk (en met internet) vermindert u risico's.

Op die pc's installeert u dan een gratis Linux-besturingssysteem (bijvoorbeeld Ubuntu of Linux Mint). Ook op oude, afgeschreven pc's werkt dat vaak nog prima. Linux is niet immuun voor computervirussen, maar de kans dat u er een krijgt is te verwaarlozen. Voor hackers is het een lastiger systeem om te kraken. Ze doen niet eens de moeite, vanwege het kleine marktaandeel van Linux. De Linux-gebruiker krijgt na het klikken op een foute link de kans om zijn vergissing in te zien, zonder dat hij schade oploopt. Bijkomend voordeel: dankzij Linux krijgt u de beschikking over een grote hoeveelheid, veelal gratis, software-toepassingen. Daarmee kunt u volop experimenteren en uw voordeel doen.

Uiteraard blijft het oppassen met het delen van bankgegevens, wachtwoorden en andere gevoelige informatie, of het klikken op onbetrouwbare links. Computergebruikers moeten nu eenmaal alert blijven. ■