



Fotografie: Momiëk Wegdam.

Wilfred van Roij: "We doen onze deuren op slot, maar beseffen niet dat we de crimineel zelf via onze laptop binnenhalen."

Digitale achterdeur staat vaak wagenwijd open

Door Willy Janssen

Horst • Wat kan een digitale inbreker nou met mijn gegevens? Andere bedrijven zijn veel interessanter dan dat van mij. Waarom moet ik dan dure beveiligingsmaatregelen nemen? "Imagoschade en identiteitsfraude vormen echter voor elk bedrijf een belangrijke bedreiging", weet voormalig digitaal onderzoeker Wilfred van Roij van Com-Connect. "Daarvan is het MKB zich onvoldoende bewust."

Imagoschade kan een bedrijf, ongeacht de grootte, de kop kosten. Google je bedrijf maar eens en kijk wat er allemaal over jou geschreven is. Vaak staan er onuitwisbare fouten in. Bovendien kan een boze klant, slordige journalist of ontslagen werknemer ook onwaarheden op het internet hebben gezet, die alleen via andere zoekma-

chines gevonden worden. Als je de herkomst van onjuiste of ongewenste informatie weet, kun je misschien nog tegenmaatregelen nemen, al kost dat vaak veel tijd en geld. "De grootste risicofactor vormen we vaak zelf", vertelt Wilfred van Roij. "Wie zijn computer bij het oud vuil zet of aan zijn kinderen schenkt, zou eigenlijk eerst de harddisk door de shredder moeten halen. Delen van oude informatie blijven ondanks wissen en formateren toch vaak ergens hangen en zijn dus altijd te achterhalen."

Zwakste schakel

Ook bij identiteitsfraude zijn we zelf vaak de zwakste schakel in de beveiliging. We verstrekken dagelijks persoonlijke gegevens om bijvoorbeeld digitale informatie op te kunnen vragen. Op een website kunnen ongemerkt onderdelen geplakt worden om jou bepaalde identiteitsgegevens te ontfutselen. Zelfs de website van je eigen bedrijf kan door een crimineel voorzien worden van een onzichtbaar voorportaal, waardoor bezoekers en klanten ongemerkt op een andere site terecht komen (*defacing*).

Van Roij adviseert ook om bij alarmerende of opmerkelijke sms-berichten de bekend geachte afzender even te bellen om te controleren of het bericht wel klopt. Het is immers een koud kunstje om iemand met valse sms-berichten te terroriseren en te doen voorkomen alsof het bericht van een goede bekende komt.

Keylogging

Diefstal van identiteitsgegevens en passwords gebeurt ook steeds vaker via *keylogging*: Via hardware (USB-sticks) of software (ongemerkt geïnstalleerde virusprogramma's) kan de crimineel eenvoudig uitlezen welke toetsen jij op je eigen computer aanslaat. Ideaal dus om wachtwoorden en creditcardgegevens te krijgen. Een goede virusscanner houdt deze keyloggers alleen tegen als ze bijvoorbeeld via de mail toegezonden worden. Niet als we ze zelf binnenhalen doordat we op een link klikken om informatie over een klant of bedrijf of een prijs op te vragen. We doen onze deuren op slot, maar beseffen niet dat we de crimineel zelf via onze laptop binnenhalen. Wanneer de politie een (valse) tip krijgt over bijvoorbeeld kinderporno op een bedrijfscomputer, ben je al snel alle computers zes weken kwijt voor het onderzoek. Wilfred van Roij kent bedrijven die op de rand van de afgrond balanceerden doordat digitale criminelen het op hen voorzien hadden. "Met een gerechtelijke procedure om zaken recht te zetten ben je al snel drie jaar verder. Schade doordat pinpas- of creditcardgegevens of je telebankieren door criminelen gebruikt zijn, wor-

den vooralsnog door banken en verzekeraars vergoed. De werkelijke schade is echter tientallen malen groter dan de dertig miljoen euro die in het openbaar worden genoemd. Als we de werkelijke omvang zouden kennen, zou geen mens meer gebruik willen maken van deze 'veilige' betaalmiddelen."

Ondanks al deze waarschuwingen raadt Wilfred van Roij ondernemers toch aan om ook hun voordeel te blijven doen met sociale media als Hyves, LinkedIn of Twitter. "Anders blijf je achter. Let wel op met de manieren waarop je informatie verstrekt en vul niet méér gegevens in dan nodig zijn om gevonden te worden. Het is onmogelijk om je honderd procent te wapenen tegen digitale criminaliteit. Bewustwording van de risico's is daarbij het allerbelangrijkste. We moeten niet panisch worden; maar wel voorzichtig."