‘Ik hoorde alleen maar PING PING PING PING’

Want zo klinkt het als u gehackt wordt en alle bestanden op uw computer versleuteld worden. Helaas is cybercriminaliteit aan de orde van de dag, al lijkt het voor menig ondernemer de ver-van-mijn-bed-show (ze hacken alleen de grote jongens, toch?). Maar ook de minder grote bedrijven zijn regelmatig het slachtoffer van cybercrime en in het mkb vallen er (te)veel slachtoffers. En dat terwijl juist hier goed grip is te houden op de situatie. Hoe? Dat leest u in dit artikel.

Cybercrime. Het klinkt allemaal ontzettend spannend. Hacken, grote bedrijven die ‘platliggen’ door een mysterieus virus, persoonsgegevens van duizenden mensen die openbaar worden. Maar ook in het mkb tiert cybercrime welig. De hoogste tijd dus om stil te staan bij de digitale veiligheid op ons niveau, het niveau van de ondernemer. De dagelijkse realiteit en niet de horrorverhalen uit de media. Hoe staan we ervoor? Wat doen we fout? Wat zijn de valkuilen? En hoe kunnen we ons wapenen?

WAAR GAAT HET MIS EN WAT KUNNEN WE DOEN?

Als we de cijfers erbij pakken dan blijkt dat 20% van de ondernemers het slachtoffer is geweest van cybercrime. Echter, als we bedrijven vragen naar de status van hun digitale veiligheid, is het antwoord meestal ‘Oh ik heb alles goed geregeld’. Alles? Goed? Dit is de eerste veelgemaakte fout, onderschatting. Tip nummer één is daarom, neem uw online beveiliging serieus en haal er een specialist bij. Ja, u moet met de billen bloot wat betreft uw beveiliging maar pas wanneer u inzicht heeft in de situatie kunt u zich ertegen wapenen. Het uitvoeren van de benodigde maatregelen kan uw eigen ICT’er. Het inzicht in online veiligheid echter is het vakgebied van een cybersecurityspecialist.

VALKUIL 2 (EN 3)

Uiteraard zijn er bedrijven die hun digitale veiligheid goed hebben ingericht. De automatisering is uitbesteed en ze gaan ervan uit dat daarmee alles potdicht zit. Totdat een medewerker per ongeluk een mailtje opent met een virus. Dat is de volgende valkuil; menselijk falen. Vervolgens is er paniek want er moet ransomware betaald worden en alle bestanden zijn versleuteld. Valkuil nummer 3 dient zich aan, het ontbreken van een back-up. Want wanneer u wel een back-up heeft hoeft u a. niet op de losgeldeisen van een cybercrimineel in te gaan en b. kunt u gewoon verder werken omdat u een back-up heeft van uw bestanden, mails en contacten. Regelen dus, die back-up!

Het risico op menselijke fouten is overigens aanzienlijk te verkleinen door het volgen van Awareness trainingen, waarin al het personeel (ook u) wordt getraind in het herkennen van de diverse vormen van cybercriminaliteit en in het adequaat handelen bij het vermoeden van een phishing mail of malafide website.

WELKOM0123

Een ander veelvoorkomend euvel in het mkb is slecht wachtwoordmanagement. Niet alleen komt het herhaaldelijk gebruiken van één eenvoudig wachtwoord voor alle accounts schrikbarend vaak voor, de opslagplek van dit wachtwoord blijkt vaak een geel stickertje onder het toetsenbord te zijn. Dit terwijl er professionele wachtwoordbeheeroplossingen zijn om wachtwoorden te bewaren en te onthouden, zoals LastPass. Bovendien hoeft het bedenken van een sterk wachtwoord niet moeilijk te zijn. Neem niet de naam van uw kind maar gebruik de eerste letters van de woorden van een zin als code, varieer met hoofdletters en tekens et voilà, een dijk van een wachtwoord. Uw beheertool doet de rest.

Met deze tips valt al veel winst te behalen. Ze worden u aangeboden door BrainCap, een ICT-organisatie met de focus op digitale veiligheid. Meer tips? Neem contact op met BrainCap via services@braincap.nl. «

BRAINCAP
Randweg 43, 1948 NS Beverwijk
Telefoon 088 – 275 48 88
www.braincap.nl