DHZ IT:

Wat elke MKB'er behoort te weten

Cybersecurity is een onderwerp waar iedere ondernemer zich waarschijnlijk zorgen over maakt – of zou moeten maken. De lijst van zakelijke websites die gehackt zijn, groeit nog steeds, en daarmee de illegale toegang tot bedrijfsgegevens en andere kritische informatie. Men is zich blijkbaar nog niet optimaal bewust van de veiligheidsrisico's die in deze moderne, digitale wereld bestaan.

Ondanks talloze onderzoeken en statistieken over hackers die zich richten op kleinere ondernemingen, hebben veel ondernemers nog steeds een houding van 'dat gebeurt mij toch niet'. Dat is een gevaarlijke en eigenlijk onverantwoorde opvatting die uiteindelijk kan leiden tot een forse digitale inbraak, met alle mogelijke gevolgen van dien. Met name de eigenaren van kleinere bedrijven onderschatten de mate waarin zij blootgesteld zijn aan beveiligingsrisico's. En er is geen gebrek aan bedreigingen: van malware tot phishing en ransomware, en de 'aanvallers' variëren van hackers die solo opereren tot de zogeheten 'disgruntled employees', ontevreden (ex-)medewerkers. Als een onderneming eenmaal met succes gehackt is, is het vaak heel moeilijk, zo niet onmogelijk vanwege de hoge kosten, om het vertrouwen van de klanten terug te winnen en de schade te herstellen.

Dit probleem wordt nog eens vergroot omdat kleinere bedrijven, in tegenstelling tot de 'grote jongens', geen speling in hun budget hebben voor een eigen IT-professional. Maar het gebrek aan een IT-afdeling (ook al bestaat die maar uit één persoon) is geen excuus om je zakelijke gegevens onbeschermd te laten. Je kunt zelf een heleboel maatregelen nemen, zeg maar Doe-Het-Zelf-IT.

Waarom gegevensbeheer nuttig is

Waarschijnlijk verbruikt en analyseert je bedrijf elke dag een continue stroom aan gegevens van meerdere bronnen. Maar wat gebeurt er met al die data als jij er eenmaal klaar mee bent? Veel eigenaren van kleinere ondernemingen denken vaak niet meer die 'verwerkte data', met name wanneer ze een grote opslagcapaciteit hebben in de cloud. Maar juist die gearchiveerde informatie die maar 'rondhangt', kan snel een risico gaan vormen in plaats van een waarde. Soms maken ondernemingen zich schuldig aan het hamsteren van gegevens, er van uit gaande dat ze die informatie ooit nog wel eens zouden kunnen gebruiken. Bovendien is opslaan in de cloud tamelijk goedkoop. Maar wat je niet (meer) hebt, kan ook niet van je gestolen worden. Bewaar dus alleen gegevens waar je een zakelijk doel mee kunt realiseren.

Daarom is het zo belangrijk om een beleid te hebben op het gebied van gegevensbeheer, of je nu wel of geen eigen IT-afdeling hebt. Niet-versleutelde bestanden, slechte wachtwoorden en zelfs onbeveiligde fysieke documenten vormen een bedreiging voor de veiligheid van je onderneming. Daarom moet je een solide bescherming hebben voor alle gegevens die je verzamelt. En wat je niet meer gebruikt, moet je weggooien. De criteria om iets weg te gooien zijn hetzelfde als bij je thuis: heb je het onlangs nog gebruikt? Heb je plannen om het binnenkort of in de nabije toekomst nog te gebruiken? Is het gebonden aan een contractuele of wettelijke bewaarplicht? Niet van toepassing? Weg ermee!
Als je eenmaal deze schifting hebt gemaakt,

> "Niet-versleutelde bestanden, slechte wachtwoorden en zelfs onbeveiligde fysieke documenten vormen een bedreiging voor de veiligheid van je onderneming."

kun je ook acties ondernemen om ervoor te zorgen dat wat je bewaart, ook veilig is – en oproepbaar. Om een veilig IT-systeem te creëren en te behouden, moeten de eigenaren van kleinere ondernemingen hun medewerkers, leveranciers en klanten informeren over het aanvaardbare gebruik van de 'assets' van de onderneming, en wat ze moeten doen als iets niet geheel correct lijkt.

In-house of outsourcen?

Bij de overweging hoe je het beheer van de IT-gegevens van je onderneming moet

regelen, heb je twee opties: je kunt dat beheer in-house houden door de IT-taken te delegeren aan de slimste medewerkers (of het zelf doen), of het outsourcen aan een freelance consultant of beveiligingsbedrijf. Afhankelijk van je budget zou het een combinatie van beide kunnen worden, maar vervolgens dient de vraag zich aan welk deel van de gegevens je gaat toevertrouwen aan een buitenstaander.

Het antwoord op die vraag is afhankelijk van de primaire functies en doelen van je onderneming, en welke IT-processen een directe impact hebben op je operaties. Zaken als klantenbeheer (customer relationship management, CRM) kunnen de meeste bedrijven beter zelf, intern beheren. Op die manier kunnen ze de volledige controle behouden over alle interacties met bestaande of toekomstige klanten. Meer omvangrijke taken als infrastructuur-management of cloud hosting kunnen ook (misschien wel beter) door externen worden verricht. Dit vermindert niet alleen de tijd die besteed wordt aan IT management, het vermindert ook de risico's dat er iets fout gaat. De media staan tegenwoordig bol van de data-inbraken en hacks, daarom is het voor eigenaars van kleinere ondernemingen enorm belangrijk om zorgvuldig om te gaan met de interne en klantgegevens. En als IT-beveiliging niet echt jouw ding is, zou je deze cruciale taak moeten outsourcen aan een ervaren deskundige. Kleine ondernemers hebben vaak de tijd, know-how en interne bronnen niet om dagelijks de netwerk-activiteiten te monitoren, en bedreigingen te herkennen.

Een beveiligings-consultant kan je helpen beslissen welke tools je nodig hebt en een veiligheidscheck uitvoeren waarbij hij of zij een grondig onderzoek doet naar alle ingangspunten en zo kwetsbare gebieden kan aanwijzen die aangepakt moeten worden. Die persoon kan ook een basis cyber security plan en business recovery plan opstellen zodat je niet alleen voldoet aan de wet- en regelgeving (voor zover die voor jouw bedrijf van toepassing is), maar ook zorgen dat bij een eventuele geslaagde aanval de schade snel wordt hersteld en de zaken weer kunnen worden opgepakt. Externe partijen die je hierbij inschakelt, moeten zich niet alleen verplichten je gegevens te beschermen, maar zich daar ook verantwoordelijk voor stellen, want als er toch iets fout gaat, is jouw zaak uiteindelijk

de klos. Met het outsourcen van IT-functies of het gebruik maken van clouddiensten verschuift jouw verantwoordelijkheid niet voor het beschermen van bedrijfskritische of klantgegevens.

Beste IT praktijken

Of je het nu zelf ter hand neemt, of uitbesteedt aan een derde partij, je IT-gegevens moeten afgeschermd worden voor onbevoegden. Nog wat tips:

Instrueer je medewerkers. Eigenaars van kleinere ondernemingen moeten er voor zorgen dat hun medewerkers beseffen dat bedrijfs- en klantgegevens waardevol zijn voor kwaadwillenden en dat er dus veilig moet worden omgegaan met die gegevens. Benadruk dat iedereen zijn gezond verstand moet gebruiken en dat iedereen zijn eigen verantwoordelijkheid heeft te nemen.

Beveilig alles met een wachtwoord of encryptie. Of het nu je smartphone is, je laptop of je desktop computer, beveilig die altijd met een wachtwoord (of beter: met een vingerafdruk-scan, of nog veel beter: met zogeheten tweetraps-authenticatie). Jaarlijks worden talloze digitale inbraken gepleegd via smartphones die wijd open blijven staan omdat mensen het wel makkelijk vinden als hun kinderen daar snel toegang op hebben zodat ze hun favoriete spelletje kunnen doen of video's kunnen bekijken.

Wachtwoorden moeten regelmatig worden vervangen voor huidige medewerkers, en direct voor medewerkers die afscheid nemen (of krijgen). Eén van de grootste blinde vlekken qua beveiliging wordt gevormd door voormalige medewerkers. Als een persoon om één of andere reden de zaak verlaat, moeten alle wachtwoorden direct worden vervangen, en zorg er ook voor dat die persoon, voordat hij het pand werkelijk verlaat, niet allerlei informatie meeneemt (op stick, of naar zijn privé-adres mailt).

> "Wachtwoorden moeten regelmatig worden vervangen voor huidige medewerkers, en direct voor medewerkers die afscheid nemen (of krijgen)."

Download altijd updates en patches. De grootste misvatting is dat je onderneming met één enkel product kan worden beschermd. Malware, ransomware en phishing-systemen zijn dingen waar we helaas mee moeten leven, en die zullen de komende jaren nog veel slimmer te werk gaan. Als je je systemen geüpdated houdt en je medewerkers op het hart blijft drukken zorgvuldig om te gaan met bedrijfsgegevens, en hen ook leert hoe ze risico's en aanvallen kunnen herkennen en vermijden, ben je beter voorbereid om de zwakke plekken die aanvallers misbruiken, om te zetten in slimme afweersystemen.

Wees realistisch over je bronnen. Gebruik de beschikbare technische tools in jouw voordeel en tegen redelijke kosten. Als het je teveel tijd kost om je kleinere onderneming op te laten nemen in honderden directories, outsource die verantwoordelijkheid dan. Als je het fijn vindt om je eigen e-commerce website te ontwerpen, ga je gang. Maar wees niet te bescheiden om om hulp te vragen wanneer je dat nodig hebt. ■