EyeXS, specialist in optimaal inrichten en beveiligen ICT-werkwijze:

"Een MKB'er is online erg kwetsbaar"

Ongure types die een e-mail, voorzien van een code, versturen met de bedoeling om de computer van de websitebezoeker te infecteren. Internetcriminelen die online ongevraagd data bekijken, ze versleutelen om ze vervolgens pas na betaling weer vrij te geven. Het zijn deze en vele andere ongemakken die een ondernemer kan ondervinden als hij zich op de digitale snelweg begeeft. Mede-eigenaar Jeffrey Menick van EyeXS: "Veel ondernemers denken dat het een ver-van-mijn-bedshow is, maar recente cijfers laten zien dat internetcriminelen hun focus verleggen van multinationals naar MKB-bedrijven. Ze passen steeds hun strategie aan, maar wij hebben ze gelukkig altijd in het vizier."

TEKST HERMAN VAN AALST

Jeffrey Menick: "Internetcriminelen bekijken websites en als ze zwakheden ontdekken plaatsen ze daar een code op. De pc van de bezoeker van die website raakt geïnfecteerd met ransomware of een andere vorm van malware. Ransomware is een digitale chantagemethode die bij ondernemers binnenkomt via een geïnfecteerde e-mail of een website. Gegevens worden verzameld, om ze vervolgens meteen te versleutelen en te gijzelen. Het is voor iedere ondernemer de grootste nachtmerrie. Gegijzelde bestanden als tekstdocumenten en foto's worden pas na betaling, vaak in Bitcoins, weer vrijgegeven. Ransomware komt meer en meer voor bij MKB-bedrijven in Nederland. We kennen vooral de verhalen uit de Verenigde Staten, maar ook bij ons kloppen steeds meer bedrijven aan die ermee te maken hebben." Van alle bedrijven in de wereld is Nederland momenteel nummer twee als het gaat om meest geïnfecteerde bedrijven op het gebied van ransomware. Daarnaast heeft de wetgever vanaf 1 januari dit jaar iedereen verplicht om datalekken, die gevoelige persoonsgegevens bevatten, te melden. Jeffrey Menick: "Een gedupeerde mag de portemonnee trekken om zijn gegijzelde gegevens weer veilig te stellen en wordt in sommige gevallen bestraft met een fikse boete." Een bijkomend nadeel met verstrekkende gevolgen is imagoschade. Pascal Menick, mede-eigenaar EyeXS: "Als klanten lucht krijgen van wat er zich heeft afgespeeld, zal hun vertrouwen als sneeuw voor de zon verdwijnen. De financiële gevolgen zijn dan niet meer te overzien en het zal niet de eerste keer zijn dat een ondernemer om die reden de stekker eruit moet trekken."

In control

Om te zorgen dat kwetsbare bedrijfsgegevens niet zomaar op straat terecht komen, is meer nodig dan alleen het optimaal inrichten van een website of e-mailomgeving. Jeffrey Menick: "Elke organisatie die gebruik maakt van computers, laptops en smartphones wil zorgen dat ze in control zijn en blijven. Als medewerkers bijvoorbeeld een laptop verliezen dan moet de data voor de vinder onbruikbaar zijn. In het geval van tablets of smartphones moet het toestel traceerbaar zijn. Het wordt dan mogelijk om gevoelige data op afstand te wissen."

De redenen van het inschakelen van de expertises van EyeXS zijn divers. Jeffrey Menick: "Een aantal bedrijven maakt zich zorgen als op een gegeven moment het klantenbestand enorm is gegroeid. Ze realiseren zich dan dat ze inmiddels met veel gevoelige informatie bezig zijn. Ze willen er zeker van zijn dat alles veilig is en wij nemen daarom hun hele ICT-werkwijze onder de loep. Dit kan zijn: analyseren van de ICT-omgeving, monitoren van de dagelijkse procedures en zorgen dat een bedrijf zo min mogelijk kwetsbaar is voor internetcriminelen. Helemaal voorkomen is helaas niet mogelijk, maar we kunnen er wel voor zorgen dat MKB-bedrijven optimaal beveiligd zijn tegen de nieuwste strategieën van internetcriminelen."

Net als in de normale wereld kampt ook de digitale wereld met een onderwereld. Jeffrey Menick: "Wij kijken hoe internetcriminelen zich bewegen en zien welke tools allemaal in omloop zijn. Wij analyseren de gebruikte codes en zetten deze kennis preventief in bij onze klanten, zodat zij minimaal kans lopen om slachtoffer te worden."

Jeffrey Menick en Pascal Menick

"Klanten vallen vaak bijna van hun stoel van verbazing."

Digitale veiligheid

De kracht van EyeXS is de expertise op het gebied van digitale security. "Wij zijn een klein en informeel team van vijftien medewerkers en begrijpen de digitale uitdagingen van MKB-bedrijven in Noord-Limburg. Iedere medewerker heeft zijn eigen specialisatie. Door een balans van hard werken en elkaars kennis delen, leren we constant van elkaar", aldus Pascal Menick.

Jeffrey Menick: "Wij willen bij het opzetten van een ICT-omgeving meedenken om te zorgen dat problemen worden voorkomen. Neem bijvoorbeeld het bouwen van een nieuwe website. Deze moet functioneren, er goed uitzien en goed vindbaar zijn. We zien dat pas daarna de beveiliging van een website volgt, als daar al aan gedacht wordt. De overtuiging is vaak dat het wel veilig zal zijn. 54% van de websites op het internet is gemaakt met standaard-programma's als Drupal, WordPress of Joomla met plugins die iedereen gebruikt. Internetcriminelen weten dit en ontwikkelen maar al te graag codes om deze grote groep te misbruiken. Als je een website niet of nauwelijks voorziet van updates dan kun je op je klompen aanvoelen dat het een keer misgaat. We kennen ook nog voldoende bedrijven die met verouderde besturingssystemen als Windows XP werken, waarvoor geen updates meer worden ontwikkeld." Pascal Menick: "Middels een audit confronteren we ondernemers met alle informatie die wij via hun bedrijfswebsite vinden. Ze vallen dan vaak bijna van hun stoel van verbazing, maar ze zijn tevens blij dat wij de zwakheden en bedreigingen ontdekken en internetcriminelen voor zijn."
Om te zorgen dat een MKB-ondernemer in een verantwoorde ICT-omgeving werkt, zijn er verschillende mogelijkheden.
Jeffrey Menick: "Voorheen werden belangrijke gegevens als klantgegevens en financiële administratie op lokale systemen opgeslagen. Vandaag de dag gebeurt dat steeds meer in de cloud. Het is een term die aangeeft dat de informatie wordt opgeslagen in een virtuele omgeving. Wij bieden software op maat aan, enerzijds om verantwoord de digitale snelweg op te gaan en anderzijds om volledig in de cloud te kunnen werken. Voordeel hiervan is dat medewerkers overal en altijd en op elk gewenst apparaat toegang hebben tot hun gegevens. Dit is een zeer efficiënte manier van werken."

Het opvoeden van medewerkers is hierbij essentieel. "Een van onze collega's legt het altijd heel mooi uit. Als je een traditioneel bedrijf start, zonder veel online gegevens, dan heb je deuren, ramen, sleutels en wellicht zelfs een alarmsysteem. Na werktijd moeten alle ramen dicht, deuren afgesloten zijn en het alarm worden geactiveerd. Als medewerkers de afgesproken procedures niet volgen, dan kan een bedrijf kwetsbaar worden. Waar vroeger een crimineel precies kon zien welke ramen en deuren niet goed beveiligd waren en het openen van een archiefkast gesneden koek bleek, zit hij tegenwoordig comfortabel achter zijn computer en kijkt ongevraagd mee, tenminste als een ondernemer hem daartoe de gelegenheid geeft", aldus Jeffrey Menick tot slot. ■

www.eyexs.com