made !n Oost-Vlaanderen
nieuws voor ondernemers

Vijf cyberrisico's die ook uw bedrijf bedreigen

Door Geert Degrande op 12 juli 2016

 De almaar voortschrijdende digitalisering zorgt ervoor dat technologie in elke organisatie een steeds crucialere rol speelt. Dat zorgt via big data, cloud computing en apps voor onvermoede nieuwe kansen, maar er is ook een keerzijde van de medaille. De digitale opslag van de gegevens en het feit dat steeds meer apparaten met internet zijn verbonden, houden ook een toegenomen risico in dat belangrijke informatie plots onder onbedoelde ogen komt. We hebben vijf cyberrisico's op een rijtje gezet waaraan elke ondernemer moet denken.

Bring Your Own Device

De tijd dat technische gadgets duur waren is achter de rug. Omdat iedereen zijn eigen devices meebrengt, ontstaan daardoor steeds meer beveiligingsrisico's. Werknemers koppelen hun mobiele toestel achteloos aan het bedrijfsnetwerk, maar de gegevens die ze downloaden op het apparaat zijn vervolgens nauwelijks beveiligd. En als een telefoon gestolen wordt, kan dat problemen opleveren. Uiteraard zouden ondernemingen werknemers kunnen verbieden hun eigen toestellen mee te brengen, maar dan zullen deze werknemers niet lang in dienst blijven. Daarom moeten ze hun heil zoeken in speciale software die werknemers via een beveiligde app op hun smartphone toegang geeft tot bedrijfsgegevens. De data blijft online, op de server van de werkgever, staan en wordt niet gedownload op het eigen apparaat. Zo worden zakelijke en persoonlijke gegevens niet vermengd. Met deze zogenoemde container-apps, die beveiligd zijn met bijvoorbeeld een pincode, krijgen virussen moeilijker toegang tot het systeem. .

Veel te gemakkelijke wachtwoorden

Mensen zijn doorgaans niet zo creatief met het bedenken van wachtwoorden. Nog altijd gebruiken ze vaak "123456" of "654321" en dit voor verschillende diensten. Dat is gevaarlijk: er hoeft maar één website zijn beveiliging niet goed op orde te hebben en het wachtwoord dat je voor alle internetdiensten gebruikt, ligt op straat. En verschillende wachtwoorden zijn vaak

mogelijk te onthouden. Er zijn echter ook programma's zoals 1Password en KeePass waarbij je enkel het hoofdwachtwoord moet onthouden. Alle persoonlijke gegevens worden versleuteld opgeslagen zodat hackers de informatie niet kunnen lezen. Lastpass heeft zelf een wachtwoordengenerator, waarmee het voor jou moeilijk te kraken wachtwoorden kan bedenken voor bijvoorbeeld je Twitter-, Facebook of e-mailaccount. Via een browserplug-in worden de wachtwoorden uit de kluis gehaald en ingevuld wanneer je ze nodig hebt.

Niet versleutelde gegevens in de cloud

Gegevens opslaan in de cloud is reuzehandig: met alleen een internetverbinding heb je overal ter wereld toegang tot bedrijfsinformatie. Opslagdiensten als Dropbox, Drive iCloud en OneDrive zijn dan ook erg populair. Maar het blijft natuurlijk gevaarlijk om daar zomaar alle gegevens in op te slaan. Het is dus belangrijk om eerst duidelijk te bepalen wat in de cloud mag en wat niet. Als dat eenmaal duidelijk is, is het belangrijk de gegevens te versleutelen met AES-encryptie.

Verouderde software

Steeds meer apparaten in een bedrijf zijn verbonden met het internet. Niet alleen de desktops en laptops van het personeel, maar bijvoorbeeld ook routers, servers en printers. Dat betekent dat het aantal zwakke plekken in de beveiliging toeneemt. Hackers zullen niet zo snel proberen om via de voordeur binnen te komen, maar eerder op zoek gaan naar sluipwegen. Zorg daarom dat de software op alle apparaten is bijgewerkt tot de laatste versie. En maak duidelijke afspraken over wat er gebeurt met verouderde apparatuur. Het laatste wat je wil, is dat iemand inbreekt op jouw netwerk via een oude server die zonder dat jij het wist nog in de kelder stond te draaien.

Haatdragende medewerkers

ICT-beveiliging is met name voor de KMO vaak geen speerpunt. Hacken zal niemand wel bij ons doen, is een vaak gehoord uitgangspunt. Daarbij vergeten bedrijven dat één van de grootste bedreigingen voor cybersecurity niet de begaafde tiener is die vanuit zijn slaapkamer voor de lol inbreekt in computersystemen. De zwakste plek zit intern: ontevreden werknemers. Ze kunnen hun onvrede uiten door systemen te saboteren of gevoelige informatie naar buiten te brengen. Een groot risico is ook de ontslagen werknemer die uit wrok het complete klantenbestand meeneemt naar zijn volgende baan. Zorg er daarom te allen tijde voor dat je goed zicht hebt op wie toegang heeft tot welke informatie binnen je bedrijf.

Cyberrisico's maken vandaag dus ontegensprekelijk deel uit van het bedrijfsleven. Desondanks sluit slechts een beperkt aantal van de bedrijven een cyberrisicoverzekering af. Dat is ook gebleken uit een grote enquête van verzekeraar Aon, die ook een kantoor heeft in Gent.

Er is dus nog werk aan de winkel, zeker als we de Belgische situatie in beschouwing nemen. Herman Kerremans (foto), Chief Broking Officer & Managing Director Specialties Aon Belgium licht toe: "Als we onze portefeuille doorlichten en zowel grote als kleinere bedrijven in beschouwing nemen, stellen we vast dat slechts een 2% van de bedrijven effectief al een cyberrisicoverzekering heeft afgesloten. Bij andere makelaars en verzekeraars is dit niet anders. De tendens om cyberrisico's in overweging te nemen is er, de actie om over te gaan tot het afsluiten van polissen laat nog even op zich wachten."