# Week van de veiligheid in teken van internetcriminaliteit bij bedrijven

17-09-2018 13:10

*Eén op de vijf mkb'ers is al eens getroffen door internetcriminaliteit, blijkt uit onderzoek van het lectoraat Cybersecurity in het mkb van Haagse Hogeschool en MKB-Nederland. Omdat de kans toeneemt dat mkb'ers geraakt worden door internetcriminaliteit, staat dit jaar tijdens de Week van de Veiligheid bescherming tegen*

*internetcriminaliteit centraal.*

Maandag 8 oktober 2018 start de Week van de Veiligheid met als thema 'Ben jij voorbereid op criminaliteit?'. Uit onderzoek blijkt dat veel mkb'ers hun internetveiligheid niet op orde hebben. De meeste getroffen mkb'ers zijn slachtoffer van computervirussen en ransomware. "Ransomware is gijzelsoftware die computerbestanden ontoegankelijk maakt," vertelt Patrick van den Brink, directeur van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Wie slachtoffer is van ransomware kan pas weer bij zijn bestanden, zoals de administratie of klantendatabase, als hij losgeld heeft betaald aan de internetcrimineel. Van den Brink: "Het dringende advies is niet te betalen. Want daarmee houd je deze vorm van criminaliteit in stand. Wie automatische back-ups maakt van zijn bedrijfsgegevens hoeft niet te onderhandelen met de internetcrimineel. Deze ondernemers hebben dankzij hun back-up al hun bedrijfsgegevens nog." Tijdens de Week van de Veiligheid kunnen mkb'ers deelnemen aan tal van activiteiten om hun kennis en vaardigheden op het gebied van internetveiligheid te vergroten. Dat kan bijvoorbeeld tijdens een van de cybercrimeontbijtjes. Een overzicht van activiteiten staat op deweekvandeveiligheid.nl. Wie nu aan de slag wil, kan in drie minuten de tijdelijk kosteloze Cyber Risico Scan op www.veiligzakelijkinternetten.nl invullen. Binnen 24 uur weten mkb'ers hoe het met hun zakelijke online veiligheid is gesteld en wat zij kunnen doen om de zwaktes in hun systemen aan te pakken. **Tips voor een betere internetveiligheid** Met de volgende tips zetten mkb'ers en hun werknemers de eerste stappen om zich beter te beschermen tegen internetcriminelen:

1. Maak back-ups. En doe dit regelmatig. Bewaar de back-up op een veilige plek. Zo beperk je de schade

als bijvoorbeeld door ransomware je bedrijfsdata gegijzeld wordt.
2. Draai updates direct. Van al je software en op alle apparaten die je werknemers voor het werk gebruiken. Zo voorkom je dat virussen gebruikmaken van kwetsbaarheden in oude versies van programma's. Het helpt om hiervoor automatisch updaten in te stellen.
3. Klik niet zomaar op bijlagen of links in e-mails. Leer jezelf en ook je medewerkers valse e-mails te herkennen. Daarmee proberen criminelen zakelijke informatie te ontfutselen of malware op je computer en bedrijfsnetwerk te installeren.
4. Gebruik niet zomaar openbare wifi-netwerken. Hoe handig ook, openbare wifi is niet veilig. Laat je werknemers onderweg alleen 4G gebruiken of verbinding maken via een beveiligde VPN-verbinding.
5. Maak afspraken en train je medewerkers. Zorg dat zij weten wat zij moeten doen en hoe zij dat moeten doen om internetcriminaliteit te voorkomen.

Ga voor meer tips naar: www.digitaltrustcenter.nl www.veiligzakelijkinternetten.nl https://www.alertonline.nl/tips/voor-werkgevers https://www.deweekvandeveiligheid.nl/ De Week van de Veiligheid wordt georganiseerd door het ministerie van Justitie en Veiligheid, VNO-NCW, MKB Nederland, Koninklijke Horeca Nederland, Detailhandel Nederland, Transport en Logistiek Nederland en het Centrum voor Criminaliteitspreventie en Veiligheid. De Week van de Veiligheid is onderdeel van de Europese maand van de cyberveiligheid.

Redactie