

CYBERSECURITY

WHAT THE HACK?

Nederland digitaliseert. De ontwikkelingen binnen de digitalisering gaan razendsnel en zijn niet meer weg te denken uit het bedrijfsleven. Iedere ondernemer krijgt vroeg of laat te maken met de impact ervan. Cybersecurity, ofwel het waarborgen van veiligheid in het gebruik van digitale technologieën, is daarom ook steeds belangrijker om bijvoorbeeld Datalekken, DDoS-aanvallen en ransomware te voorkomen. Heeft een ondernemer de cybersecurity wel op orde, dan draagt dat bij aan het imago van het bedrijf, de efficiency en de dienstverlening.



Bedrijven zijn verplicht om te zorgen voor een adequate digitale beveiliging: software, mobiele telefoons en andere producten of diensten met een ICT-toepassing moeten voldoende beveiligd zijn tegen hacken. Je kunt als bedrijf verschillende technische en organisatorische maatregelen treffen om cyberincidenten te voorkomen. Maar hoe pak je dat nou aan?

10 TIPS

1. Maak een risico analyse om inzichtelijk te krijgen wat voor jouw bedrijf belangrijk is, wat je zou moeten beschermen en welke maatregelen getroffen worden. De meest kwetsbare schakel is de mens.
2. Stel regels voor medewerkers hoe zij zich 'online' moeten gedragen en welke informatie zij delen. Denk hierbij aan het delen van inloggegevens, dat ze niet zomaar op URL-linken moeten klikken of bestanden openen, en het stellen van voorwaarden aan de wachtwoorden.
3. Pas geregeld je wachtwoorden aan en maak sterke en unieke wachtwoorden. Hier kan je hulp bij krijgen door middel van wachtwoordgeneratoren, zoals LastPass.
4. Gebruik je 'gezonde boerenverstand'. Is iets te mooi om waar te zijn? Dan is dat vaak ook zo.
5. Maak offline back ups en zorg dat je geregeld back ups maakt van je belangrijke bestanden.
6. Bouw je gehele ICT omgeving opnieuw op nadat je gehackt bent.
7. Maak gebruik van Antivirus. Deze zoeken namelijk naar aanvallen die al hebben plaatsgevonden.
8. Zodra er een update beschikbaar is voor je

computer pas deze dan direct toe. De update is namelijk super belangrijk om kwetsbaarheden uit de systemen van de leveranciers te halen.

9. Maak geen gebruik van openbare Wi-Fi netwerken en verwijder openbare netwerken uit je apparaat. Gebruik een VPN verbinding, deze is het meest veilig.
10. Laat hackers jouw bedrijf onder de loep nemen, ze kunnen je namelijk helpen om inzicht te geven in de kwetsbaarheden binnen jouw bedrijf.

DE MEEST KWETSBARE SCHAKEL IS DE MENS

INFORMATIE EN TOOLS

VNO-NCW VeluweVallei richt zich op de preventie van cybercriminaliteit door de achterban bewust te laten worden van digitale risico's en hen praktisch te informeren over tools als de Cybersecurity Health Check voor middelgrote bedrijven. Met regelmaat organiseert de ondernemersvereniging bijeenkomsten over het thema.

CONTACTPERSOON

Rob Dal, regiomanager VNO-NCW VeluweVallei
dal@vno-ncwmidden.nl

AGENDA VNO-NCW VELUWEVALLEI

Woensdag 18 september 2019
Prinsjesdagbijeenkomst i.s.m. gemeente Barneveld, Rabobank en Schuiteman Accountants & Adviseurs
Spreker: Doekle Terpstra, voorzitter Techniek Nederland
Tijd: vanaf 07:00 uur
Locatie: Schaffelaartheater, Barneveld

25 t/m 29 september
Ledenreis naar Helsinki & Riga. Vijfdaags programma, waarbij je zakelijke kansen ontdekt door interessante bedrijfsbezoeken en netwerkgelegenheden én kennismaakt met de cultuur van beide bestemmingen.

Donderdag 10 oktober 2019
Bedrijfsbezoek bij SanoRice Veenendaal, samen met VNO-NCW regio Arnhem-Nijmegen en VNO-NCW Rivierenland
Gastheer: Marc Krams MSc RA, finance manager
Tijd: 15.30 – 18.00 uur
Locatie: SanoRice, Veenendaal

Maandag 25 november 2019
Bedrijfsbezoek Leadax, samen met VNO-NCW regio Zwolle en VNO-NCW Stedendriehoek
Gastheer: Roeland van Delden, directeur
Tijd: 15.30 – 18.00 uur
Locatie: Leadax, Wapenveld

Donderdag 28 november 2019
Veluwe Innovatieprijs