CYBER-SECURITY

## VEILIG DIGITAAL ONDERNEMEN

# Ethical hacker helpt MKB-metaal

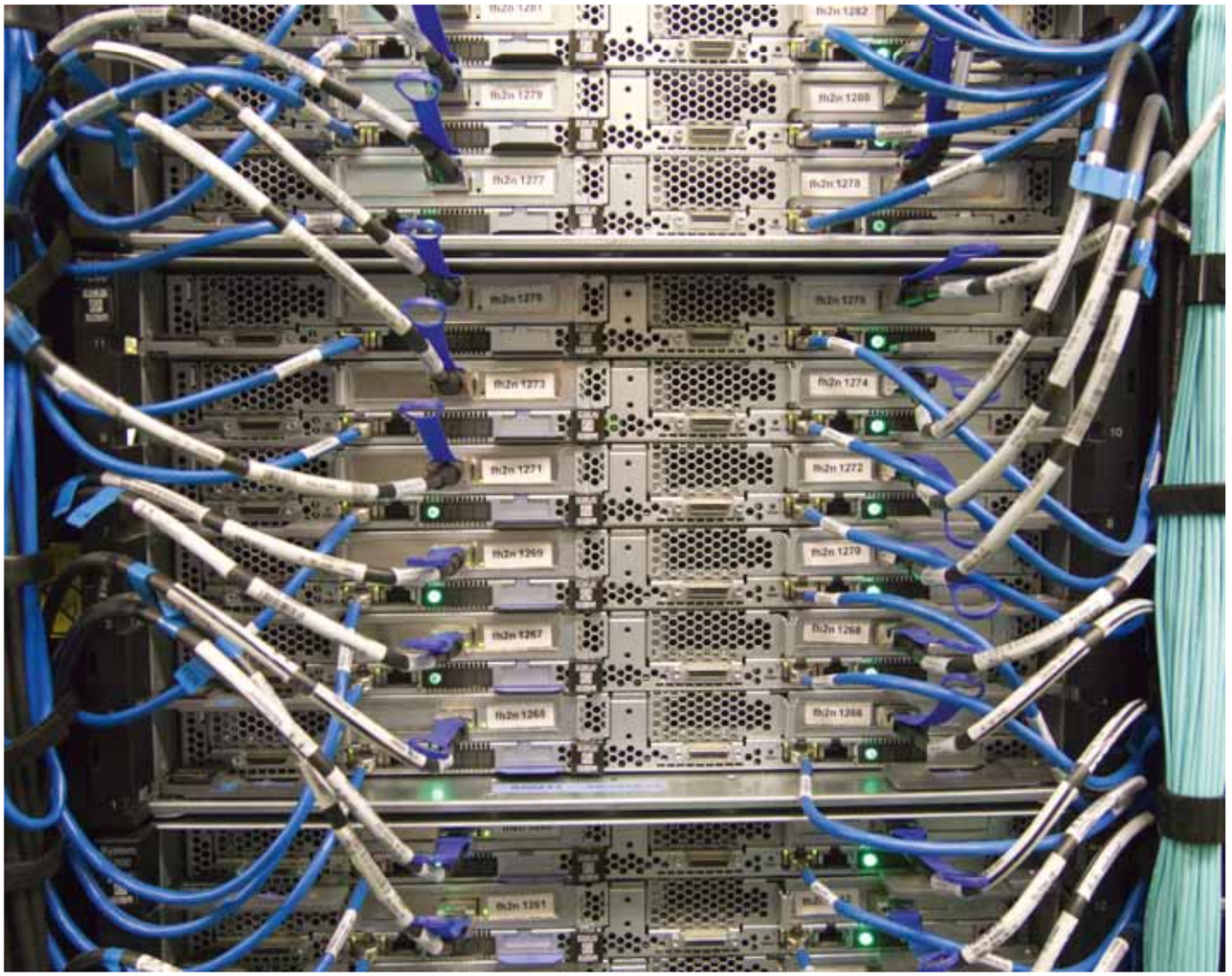
**Voor veel metaalondernemers is online veiligheid top of mind, maar zij weten vaak niet welke stappen ze het beste kunnen zetten. Teqnow heeft daarom in samenwerking met een ethical hacker van cyberdienstverlener Computest een workshop samengesteld die onder andere ingaat op de vijf basisprincipes van het Digital Trust Center.**

De vijf basisprincipes van veilig digitaal ondernemen zijn opgesteld om ondernemers te helpen de basisbeveiliging op orde te krijgen. De maatregelen zijn toegankelijk en praktisch: ieder ondernemer kan ermee uit de voeten. De eerste stap is een inventarisatie van de kwetsbaarheden en een inschatting van de gevolgen. Aan de hand van een uitgebreide checklist moeten de deelnemers zelf een eerste invuloefening uitvoeren. Ook wordt ingegaan op het kiezen van veilige computerinstellingen, het toepassen van software-, virus- en firewallupdates. En wordt aandacht besteed aan het gebruik van standaard instellingen in de hardware of routers en het gebruik van 2-factor authenticatie.

### BACK-UP NIET VOLDOENDE

Een belangrijk onderdeel van de workshop is hoe men virussen en malware kan herkennen en wat ertegen te doen is. Als voorbeeld wordt ook het de recent verschenen SamSam ransomware besproken. Aanvallers die gebruik maken van SamSam gijzelsoftware gaan zeer doortrapt te werk.


*Aanvallers die gebruik maken van SamSam gijzelsoftware gaan zeer doortrapt te werk.*



*Tijdens de workshop wordt aandacht besteed aan het gebruik van standaard instellingen in de hardware of routers en het gebruik van 2-factor authenticatie.*

De aanvallers slaan niet direct toe, maar doen eerst goed onderzoek naar het potentiële slachtoffer. Dit alles om zo veel mogelijk schade aan te kunnen richten. Vervolgens verwijdert de gijzelsoftware de back-ups in alle stilte, zodat de besmetting niet ongedaan gemaakt kan worden. Als dat is gebeurd worden de bestanden vergrendeld. Doordat de back-ups zijn verwijderd vergroot de aanvaller de kans dat het slachtoffer zal betalen.

*'IoT-toepassingen zijn op dit moment vaak slecht beveiligd'*

Het is cruciaal om afspraken in een service level agreement met IT-leveranciers en websitebouwers vast te leggen. Uit onderzoek van De Haagse Hogeschool en Teqnow is gebleken dat metaalbedrijven twee keer vaker het slachtoffer zijn van cybercriminaliteit. Op basis van de verontrustende resultaten is een vervolgonderzoek opgezet. Begin 2019 volgt het eindrapport. Wat in de voorlopige resultaten naar voren komt, is dat het overgrote deel van de mkb-bedrijven of geheel of gedeeltelijk afhankelijk is van de expertise van een externe IT-leverancier. Maar ook als men alles op IT-gebied intern regelt, behoort dit eigenlijk niet tot de core-activiteiten van de onderneming.

## STANDAARD VEILIGHEIDSEISEN

Internet of things (IoT)-toepassingen zijn op dit moment vaak slecht beveiligd en vormen daarmee een bedreiging voor de veiligheid en privacy. De Cyber Security Raad stelt in een adviesrapport dat er meer toezicht op IoT-apparaten en de fabrikanten hiervan moeten komen. Ook onderschrijft de Raad het belang van het voorstel van de Europese Commissie om met een Europese certificering voor de digitale beveiliging van ICT-producten en -diensten te komen. De overheid zou verder standaard veiligheidseisen aan leveranciers moeten stellen en hen wettelijk aansprakelijk houden onder meer voor eventuele economische schade.•

## Bijeenkomst

Op 16 april a.s. organiseert Teqnow een bijeenkomst waarbij ingegaan wordt op de beveiliging van IoT en alles wat daarmee samenhangt. Interesse? Meld je gratis aan op de Teqnow-website zodat we je kunnen uitnodigen.

**www.teqnow.nl**