TE ZIEN IN:
INNOVATIE NU | MAART 2021

CYBERSECURITY

A WAY TO IMPROVE BUSINESS CONTINUITY IN DIGITAL TRANSFORMATION

In samenwerken met:

The Cyber Partners

ADVANCED MANUFACTURING CENTER

ISSN 2772-4255

CYBER SECURITY

> ***Cyber security is not a goal, nor will it ever be. Business continuity, however, is.***
>
> ***Accordingly, cyber security is a topic that should be addressed every once in a while. Cyber security - digital safety & security - is a precondition for safely using the opportunities digital transformation offers.***

Cybersecurity is geen doel op zich. En toch is het belangrijk om er voldoende aandacht aan te besteden. Cybersecurity - en daarmee digitale veiligheid - is een voorwaarde om de kansen van Industry 4.0 te benutten.

Het is de realiteit dat ondernemers tegenwoordig dagelijks te maken hebben met cyberdreigingen. Men moet zich weten te weren tegen deze dreigingen en voldoende investeren in beveiliging.

Voor wat betreft de beste aanpak, zijn er net zoveel invalshoeken als dat er bedrijven zijn. Een paar voorbeelden:

- Voor grote en beursgenoteerde bedrijven is het toezicht op cyberveiligheid beschreven in de ‘corporate governance code’.

NIET HET DOEL, MAAR EEN MANIER OM DE KANSEN VAN DIGITALISERING TE BENUTTEN

- In dit soort organisaties wordt vaak al voldoende geïnvesteerd in technologie, processen en opleidingen. Toch zijn deze bedrijven vaak alsnog kwetsbaar, door digitale verbindingen met de partners met wie ze samenwerken.
- In sommige gevallen moet er nog een manier gevonden worden om de nieuwste dreigingen voor te blijven.
- De meeste middelgrote bedrijven hebben al een aantal maatregelen getroffen. De scans van The Cyber Partners laten wel zien dat in ongeveer 60% van de gevallen het urgentiegevoel bij slechts een enkele functionaris in de organisatie aanwezig is.
- Kleinere bedrijven zijn meer afhankelijk van hun technologieleveranciers. Voor hen is het vooral zaak de juiste vragen te stellen en heel nauwgezet de instructies te implementeren. Daarnaast zal er een aantal snelle oplossingen geïmplementeerd moeten worden op het gebied van wachtwoordbeveiliging en het splitsen van het netwerk.
- Als u internationaal zakendoet, kunt u te maken krijgen met wetgeving die uw cyberveiligheid beïnvloedt.
- Verschillende branches, zoals defensie en de medische branche, hebben hun eigen standaarden.

We zien dat de noodzaak om te investeren sterk gestegen is sinds de start van de COVID-19-pandemie

Wist u dat de hoeveelheid cyberaanvallen sinds het uitbreken van de COVID-19-pandemie meer dan vervijfvoudigd is? En wist u dat, door de toename van het thuiswerken, de afhankelijkheid van digitalisering is vergroot? En dat de meeste incidenten (80%) ontstaan door of met (onbewuste) medewerking van een van de eigen medewerkers of diens account?

Voor alle bedrijven - klein of groot en in alle branches - geldt dat bewustwording van het personeel een continu proces is. Door de snelle ontwikkelingen is het noodzaak dat men blijft leren en de processen blijft aanpassen. Men moet ermee aan de slag.

Maar gelukkig hoeft niemand helemaal opnieuw te beginnen. Er zijn voldoende bedrijven die al ervaring hebben opgedaan met de verschillende aspecten van cyberveiligheid, zoals met “Phishing”-mails. Uit ervaring weten we dat een phishing-aanval vrijwel altijd uit drie onderdelen bestaat:

1. **De afzender is een persoon (CEO) of een instantie (belastingdienst, bank), die gezag heeft.**
2. **De geadresseerde is iemand met een digitale bevoegdheid, bijvoorbeeld iemand in de organisatie die een financiële transactie of een software-update mag uitvoeren.**
3. **Er wordt gebruikgemaakt van een drukmiddel, bijvoorbeeld tijd: “Zou u snel….”, “Vóór morgen, want anders….”**

Hoe traint u uw personeel in het herkennen hiervan? En - eenmaal herkend - wat adviseert u uw personeel om te doen?

Specifiek voor Industry 4.0 zijn er nog meer weetjes. Het is belangrijk dat de productie altijd door kan blijven draaien en dat de tekeningen en data die u van uw klanten krijgt ook bij u goed beschermd zijn. En dat terwijl in de meeste productieomgevingen niet alle updates uitgevoerd worden, of soms zelfs niet beschikbaar zijn.

In Industry 4.0-omgevingen bent u meer afhankelijk van de leverancier van de systemen. Welke vragen kunt u aan hen stellen en hoe richt u vervolgens uw netwerk in?

Cybersecurity is niet het doel, maar een manier om de kansen van digitalisering te benutten.

Did you know?

- that since the start of the COVID-19 crisis, the amount of cyber attacks has increased five fold?
- that remote working has significantly increased the dependency on digital infrastructure?
- that most cyber incidents (80%) are (unkowingly) caused by own staff or from their account?

Evelien Bras

Director

The Cyber Partners

De menselijke factor is de meest belangrijke om uw bedrijf veilig te houden.

The Cyber Partners is opgericht door Evelien Bras.

Evelien heeft haar opleiding Technische Informatica reeds meer dan 25 jaar geleden afgerond. Na haar afstuderen begon ze met de implementatie van oplossingen om internationale telecomnetwerken te beveiligen. Hierna ging haar carrière verder in de aerospace en defensie, waar ze innovatie en publiek-private samenwerkingsinitiatieven heeft geleid. Samenwerking en cybersecurity werden meer en meer de speerpunten van haar activiteiten.

Vandaag de dag is ze commissaris bij een multinational in de automotive industry, gastdocent bij de Universiteit Leiden voor de parttime executive master Cyber Security, ze is voorzitter van een beoordelingscommissie van NWO (Nederlandse Organisatie voor Wetenschappelijk Onderzoek) en is recent benoemd als directeur-bestuurder van FERM, een initiatief om de cyberweerbaarheid van de Rotterdamse haven te vergroten.

The Cyber Partners is een samenwerking tussen professionals, welke zich richt op het organiseren van cybersecurity binnen commerciële organisaties.