

Cyber
Weerbaarheidscentrum
Maakindustrie Zuid-Holland

# Samen werken aan een digitaal veilige keten

7 oktober

Josephine van Luik

batenburg techniek

FME POWERED BY DUTCH TECHNOLOGY

HSD securitydelta.nl

BOERS&CO PRECISION SOLUTIONS

koninklijke metaalunie

Innovation Quarter

hitech

HiDelta! magneet voor duurzame groei

LELY

**Hackers bedreigen klanten van bezorgservice Flink: ‘Betaal of gegevens worden gelekt’**







**Politie en OM: cyberdreiging voor Nederland groeit door AI en nieuwe generatie hackers**

**MKB strijdt hard tegen hackers, maar verliest vaak**

NOS Nieuws • Zondag, 06:44 • Aangepast zondag, 09:50

**Odido-hackers publiceren resterende klantdata, ook miljoenen ID-nummers**

MAAK INDUSTRIE NIEUWS




ALGEMEEN / 07 MAART 2023

# MAAKINDUSTRIE VAAKST GETROFFEN DOOR RANSOMWARE

De maakindustrie is een populair doelwit voor cybercriminelen. Partijen in de sector zijn het vaakst doelwit van cybercriminaliteit van alle sectoren. Het gaat daarbij om diverse vormen van cybercriminaliteit.

Dit blijkt uit het onderzoek IBM X-Force Threat Intelligence index, op basis van data uit 2021. De maakindustrie is een geliefd doelwit van cybercriminelen. Van alle aanvallen die IBM X-Force voorkwam was maar liefst 23% gericht op maakbedrijven. Hiermee is een verschuiving zichtbaar; vorig jaar stonden juist financiële organisaties op de eerste positie.

## Opkomst van SCADA MODBUS en Internet of Things

De stijging is volgens IBM onder meer toe te schrijven aan de groeiende omarming van het communicatieprotocol SCADA MODBUS en Internet of Things (IoT)-apparaten. Zo blijken cybercriminelen veel vaker actief te zoeken naar kwetsbare SCADA MODBUS- en IoT-apparaten die verbonden zijn met het internet. Het aantal

AUTOMATION NL

Home Nieuws Artikelen Blogs Agenda Dossiers Edities Adverteren

# Maakindustrie het meest geraakt door ransomware met 30% van de aanvallen in Nederland

28 maart 2024 redactie AutomationNL



Unit 42, een onderzoeksteam van Palo Alto Networks, heeft zijn Ransomware Retrospective rapport uitgebracht. Hieruit blijkt dat het ransomware-landschap het afgelopen jaar te maken heeft gehad met belangrijke veranderingen en uitdagingen. In het rapport valt op



## Hacktivists

Ideologische motieven en maatschappelijke boodschappen.



## Hackers

Financieel gewin door datadiefstal, ransomware en fraude.



## Competitors

Bedrijfskritische informatie en innovaties stelen.



## Foreign nations

Spionage, strategische belangen en verstoring van vitale sectoren.



## Disgruntled employees

Ontevreden of nalatige medewerkers vormen een risico van binnenuit.

Cyber
Weerbaarheidscentrum
Maakindustrie Zuid-Holland

## Beperkte securitycapaciteit

IT en security zijn vaak bij een klein team of externe partij belegd.

## Verouderde systemen

Legacy IT en OT zijn niet altijd eenvoudig te patchen of vervangen.



## Waardevolle ketentoegang

MKB-bedrijven werken met grotere klanten, leveranciers en partners. Zo krijgen hackers toegang tot de hele keten.

## Continuïteit is cruciaal

Productiestilstand kost direct geld en verhoogt de druk bij een ransomware-aanval.

## Menselijke factor

Phishing, gestolen accounts en social engineering blijven aantrekkelijke ingangen.

Cyber Weerbaarheidscentrum
Maakindustrie Zuid-Holland

# Cyber = meer dan techniek




**Security Awareness**
Bewustwording, gedrag, kennis en vaardigheden.

**Beleid & Management**
Rollen en verantwoordelijkheden, processen, procedures en continuïteit.

**Software, Systemen & Netwerken**
Technische maatregelen, systemen, infrastructuur en data.

**Kennis & vaardigheden**

**Inzicht in dreiging**

**Risicomanagement**




Wet en regelgeving
**NIS2, RED & CRA**

**Awareness**

**Leverancier management**

Cyber Weerbaarheidscentrum
Maakindustrie Zuid-Holland

# Wet- en regelgeving




Cyber Weerbaarheidscentrum
Maakindustrie Zuid-Holland

# Hoe kun je aan de slag?

1. Inventariseer kwetsbaarheden
2. Kies veilige instellingen
3. Voer updates uit
4. Beperk toegang
5. Voorkom virussen en malware
6. Omgaan met een cyberincident



# Tip 1: Inventariseer kwetsbaarheden

1

## Wat zijn jouw kroonjuwelen?

- Breng apparaten, software, accounts en koppelingen in kaart.
- Bepaal welke systemen cruciaal zijn voor de bedrijfsvoering.
- Leg vast wie eigenaar is en welke kwetsbaarheden prioriteit hebben.

# Tip 2: Kies veilige instellingen

2

**Veilige standaardinstellingen verkleinen de kans op misbruik.**

- Gebruik sterke, unieke wachtwoorden of een wachtwoordmanager.
- Schakel multifactorauthenticatie in voor belangrijke accounts.
- Zet onnodige functies, accounts en externe toegang uit.



Cyber Weerbaarheidscentrum
Maakindustrie Zuid-Holland

# Tip 3: Voer updates uit

3

**Updates dichten bekende beveiligingslekken.**

- Houd apparaten, besturingssystemen en software up-to-date.
- Schakel automatische updates in waar dat kan.
- Installeer beveiligingspatches zo snel mogelijk.

# Tip 4: Beperk toegang

4

**Geef medewerkers alleen toegang tot wat zij echt nodig hebben.**

- Werk met persoonlijke accounts en passende gebruikersrechten.
- Beperk fysieke toegang tot technische ruimtes en apparatuur.
- Vergrendel systemen automatisch na een korte periode van inactiviteit.



Cyber Weerbaarheidscentrum
Maakindustrie Zuid-Holland

# Tip 5: Voorkom virussen en malware

5

**Combineer techniek met veilig gedrag van medewerkers.**

- Stimuleer alert gedrag bij links, bijlagen, downloads en USB-media.
- Gebruik actuele endpoint- en antivirusbeveiliging.
- Beperk installatierechten en installeer alleen vertrouwde software.



Cyber Weerbaarheidscentrum Maakindustrie Zuid-Holland

# Incident?

**MEDEWERKERS** Weten medewerkers wat ze moeten melden — en wie ze bellen?

**AFSPRAKEN** Wie beslist bij uitval, datalek, communicatie en herstel?

**BASIS OP ORDE** Kun je accounts blokkeren, systemen isoleren en herstellen vanaf een goede back-up?

# Cyber Weerbaarheidscentrum Maakindustrie Zuid-Holland

## Initiatiefnemers:

BOERS&CO PRECISION SOLUTIONS

hitech

batenburg techniek

LELY

koninklijke metaalunie

FME

HSD securitydelta.nl

HiDelta! magneet voor duurzame groei

Innovation Quarter

## In samenwerking met:

Cyber Weerbaarheidscentrum BRAINPORT

Centrum voor Veiligheid en Digitalisering

CYBER NETWERK DRECHTSTEDEN

DE HAAGSE HOGESCHOOL

Digitalzh

MRDH METROPOOLREGIO ROTTERDAM DEN HAAG

digital trust center.

FERM Rotterdam Port Cyber Resilience Platform

Cyber Weerbaarheidscentrum Greenport

CYBER WEERBAAR NL

provincie Zuid-Holland

Rijksdienst voor Ondernemend Nederland

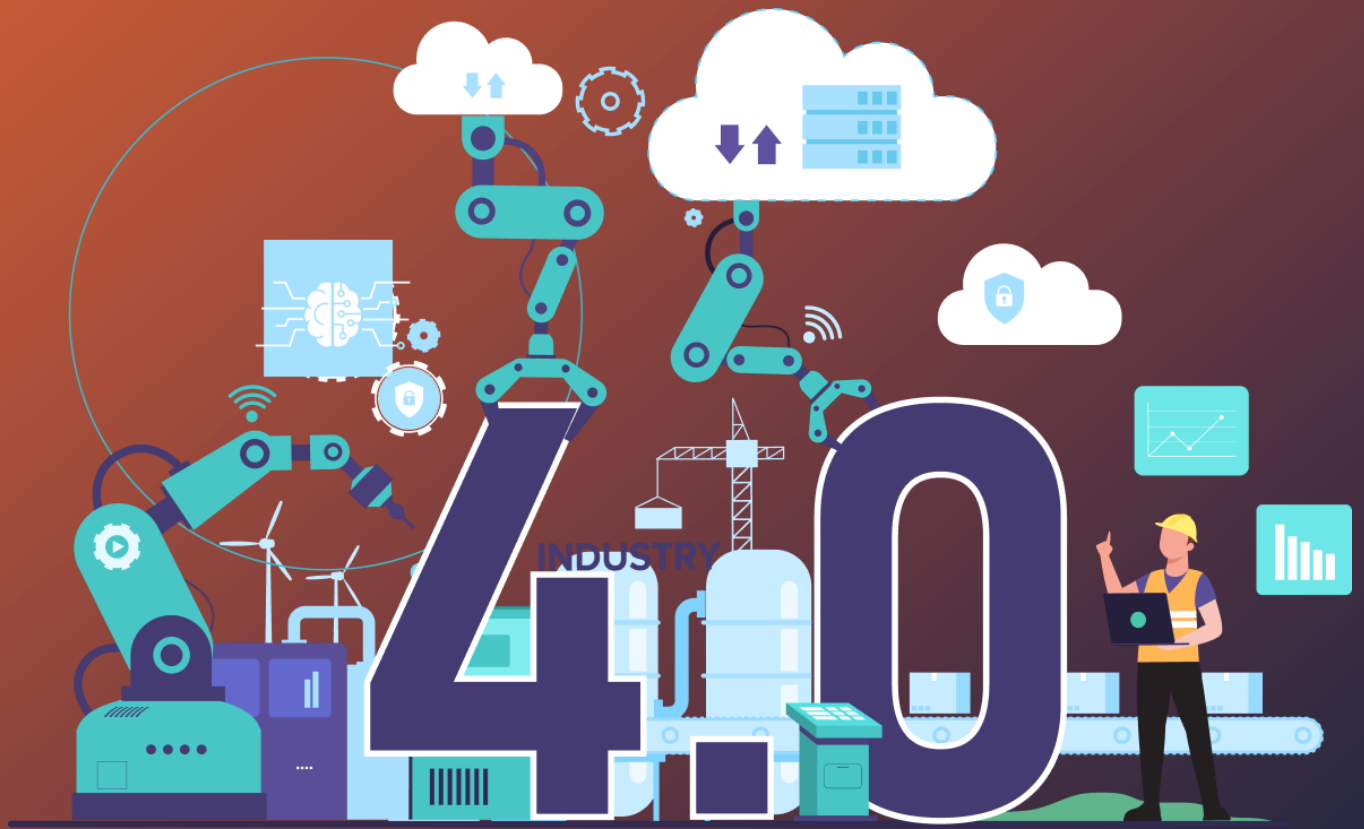
# Aan de slag met IT- en OT-security

- Concrete handvatten en tools
- Praktische begeleiding
- Beveiligingsadvies
- Nul-meting en stappenplan
- Dreigingsinformatie
- Hulp van experts
- ISAC Overleggen
- Kennisuitwisseling

www.cwmaakindustrie.nl

Cyber
Weerbaarheidscentrum
Maakindustrie Zuid-Holland

# Samen werken aan een digitaal veilige keten!




**Meer weten?**
programmateam@cwmaakindustrie.nl
**www.cwmaakindustrie.nl**

Josephine van Luik
josephine.vanluik@securitydelta.nl