eye.security

De Cybersecurity-gids voor middelgrote maakbedrijven

Inzicht in wat belangrijk is

Bescherming tegen ransomware-aanvallen: je hoogste prioriteit

De snelle digitale transformatie binnen de maakindustrie heeft een unieke omgeving gecreëerd, met bijbehorende uitdagingen voor degenen die verantwoordelijk zijn voor de beveiliging ervan.

De meest voorkomende cyberaanval waar de maakindustrie mee te maken heeft, is vergelijkbaar met andere sectoren: ransomware.

26%

van alle wereldwijde cyberincidenten richt zich op maakbedrijven

71%

van alle aanvallen op maakbedrijven betreft ransomware

1.

Digitale transformatie brengt nieuwe uitdagingen voor informatiebeveiliging

Organisaties in de maakindustrie omarmen digitale transformatie om innovatie, groei, efficiëntie en winstgevendheid te stimuleren. Het tempo en de omvang van deze veranderingen hebben een unieke omgeving gecreëerd, waarin informatietechnologie (IT) en operationele technologie (OT) samensmelten. Dit gaat gepaard met complexe toeleveringsketens, medewerkers met uiteenlopende vaardigheden en diverse regelgevingsuitdagingen. Voeg hieraan toe dat bedrijven een grote hoeveelheid waardevolle informatie beheren en ernstige gevolgen kunnen ondervinden van bedrijfsstilstand, en het is duidelijk waarom cybercriminelen deze sector als doelwit kiezen.

Als reactie hierop bieden verschillende cybersecuritybedrijven een portfolio van producten die specifiek zijn ontworpen om maakbedrijven te beschermen, met de nadruk op operationele technologie (OT). Maar de realiteit is dat, hoewel er aanvallen zijn geweest die gericht waren op sabotage van OT, de belangrijkste dreiging voor maakbedrijven niet veel verschilt van andere sectoren. Volgens een rapport van het World Economic Forum, gepubliceerd in mei 2024, was de maakindustrie de afgelopen drie jaar het meest getroffen door cyberaanvallen, waarvan 71% ransomware betrof.

Maakbedrijven zijn zeer gewilde doelwitten voor cybercriminelen. Het beschermen van de informatie die zij proberen te stelen, te versleutelen of als losgeld te gebruiken, moet dan ook je hoogste prioriteit zijn. Hieronder lichten we de top 10 beveiligingsmaatregelen toe die je in overweging moet nemen. Maar om deze in perspectief te plaatsen, is het belangrijk om eerst te begrijpen waarom maakorganisaties zo vaak worden aangevallen.

2.

Een uniek technologisch ecosysteem

De maakindustrie heeft altijd al een unieke combinatie van IT en OT gekend, maar door digitale transformatie is deze complexer geworden, wat nieuwe kansen biedt voor cybercriminelen.

Snel uitbreidend aanvalsoppervlak

Het aanvalsoppervlak omvat alles wat een dreigingsactor kan benutten om zijn doelen te bereiken, zoals software, hardware, mensen en processen. In maakorganisaties groeit dit oppervlak door de introductie van nieuwe technologieën, de verspreiding van IoT, de opkomst van thuiswerken en de toename van BYOD (bring-your-own-device)-praktijken.

Toenemende onderlinge verbondenheid

Industriecontrolesystemen (ICS) die voorheen geïsoleerd waren, zijn nu vaak verbonden met het IT-netwerk en het internet. Daarnaast heeft IoT gezorgd voor uitgebreide netwerken van vaak heterogene apparaten. Hoewel goed ontworpen, gesegmenteerde en beveiligde netwerken aanvallers zouden moeten verhinderen om tussen OT- en IT-netwerken te bewegen, zijn geen beveiligingsmaatregelen 100% effectief.

Kwetsbare, verouderde OT-systemen

Veel OT-systemen worden al jaren gebruikt en zijn niet ontworpen volgens moderne beveiligingsstandaarden. Ze werden ooit niet als doelwit beschouwd en maken vaak gebruik van ingebouwde besturingssystemen en software die niet langer wordt ondersteund door de fabrikant. Deze systemen blijven in gebruik omdat ze een specifieke taak goed uitvoeren. Vervanging zou kostbaar zijn en bedrijfsprocessen verstoren. Hoewel ze zelden direct worden aangevallen, kunnen kwetsbaarheden in deze systemen door aanvallers worden benut om lateraal door het netwerk te bewegen en hun doelen te bereiken.

3.

Een uniek commercieel ecosysteem

De combinatie van technologische uitdagingen met de typische bedrijfsprocessen en structuren in de maakindustrie heeft een omgeving gecreëerd die cybercriminelen gretig misbruiken.

Complexe toeleveringsketens

Supply chain-aanvallen maken misbruik van vertrouwde zakelijke relaties om toegang te krijgen tot de systemen en netwerken van een organisatie. Dit kan variëren van het eenvoudig hacken van een e-mailaccount van een zakenpartner en het versturen van een link die malware downloadt, tot geavanceerdere aanvallen, zoals het compromitteren van een softwareleverancier en het toevoegen van achterdeurtjes in applicaties waarmee een aanvaller je netwerk kan binnendringen.

De maakindustrie kent complexe toeleveringsketens en een hoge mate van zakelijke verbondenheid. Veel maakbedrijven fungeren zowel als producent als consument en maken vaak gebruik van enkele, unieke leveranciers. Als een leverancier door een aanval niet kan leveren, kan dat verregaande gevolgen hebben voor de hele keten.

Ongeacht de volwassenheid van je beveiligingsprogramma ben je nooit veiliger dan je zakenpartners en klanten. Veel kleinere bedrijven onderschatten hun cyberrisico. Je kunt je leveranciers tot op zekere hoogte auditen, maar hoe waarborg je het beveiligingsniveau van hun partners?

Volgens het World Economic Forum is ransomware het grootste risico voor de maakindustrie, gevolgd door social engineering en supply chain-aanvallen. Beide vormen vaak de eerste stap in een aanval die uiteindelijk kan eindigen in ransomware.

54%

mist inzicht in kwetsbaarheden binnen hun toeleveringsketen

41%

wijt een datalek aan een derde partij

Organisatiestructuur en -cultuur

In vergelijking met sectoren zoals banken en financiële diensten hebben maakbedrijven vaak onvolwassen beveiligingsprogramma's die niet zijn meegegroeid met hun digitale transformatie. Daarnaast ontbreekt het vaak aan een cultuur van cyberbewustzijn.

Maakorganisaties bestaan uit veel verschillende afdelingen met diverse groepen mensen, elk met uiteenlopende ervaringen, vaardigheden en prioriteiten. Er is vaak een gebrek aan kennis en middelen op gebieden zoals IT, OT, cybersecurity, informatiebeveiliging en governance, risico en compliance (GRC). Het resultaat kan een gefragmenteerde transformatiestrategie en besluitvorming zijn, wat leidt tot hiaten in beveiligingsmaatregelen.

Regelgevingslandschap

Het regelgevingslandschap verandert mee met de veranderende bedrijfspraktijken en digitale transformatie. Veel regelgeving bevat specifieke clausules die de maakindustrie raken. Zo reguleert de EU-richtlijn Netwerk- en Informatiesystemen (NIS2) fabrikanten die aan kritieke infrastructuur leveren. De Cyber Resilience Act legt de nadruk op security-by-design-principes om risico's op cyberaanvallen in productieomgevingen te verminderen. Ook sectorspecifieke regelgeving evolueert, zoals de Machinerichtlijn (2023/1230), die recent is bijgewerkt met clausules die nieuwe risico's door cyberdreigingen adresseren.

Gezien de toename van ransomware-dreigingen is de regelgeving die voor alle bedrijven van belang is, de EU Algemene Verordening Gegevensbescherming (AVG). Ransomwaregroepen maken vaak gebruik van dubbele afpersing, waarbij data niet alleen wordt versleuteld maar ook gestolen met dreiging van openbaarmaking. Dit kan slachtoffers blootstellen aan zware boetes onder de AVG.

EU Agentschap voor Cyberbeveiliging (ENISA): Dreigingslandschap 2024

72% van de bedreigingen op maakbedrijven was ransomware

Ransomware is de grootste dreiging voor de maakindustrie.

De maakindustrie is de op één na meest getroffen sector door ransomware.

Maakbedrijven worden beschouwd als de meest frequente en zwaar getroffen slachtoffers van ransomware.

Veel dreigingsactoren richten zich op specifieke sectoren, maar de meeste hebben de maakindustrie als doelwit.

4.

Waarom is de maakindustrie zo'n aantrekkelijk doelwit voor cyberaanvallen?

Waarom worden maakbedrijven vaker aangevallen dan andere sectoren? Een groot deel van het antwoord ligt in de eerder beschreven uitdagingen: een uitgebreid aanvalsoppervlak, kwetsbare systemen en een hoge mate van technologische en zakelijke verbondenheid. In combinatie met minder volwassen beveiligingsprogramma's in vergelijking met sectoren zoals financiële dienstverlening en banken, wordt de maakindustrie een makkelijk doelwit voor ransomwaregroepen.

Waarom ransomware?

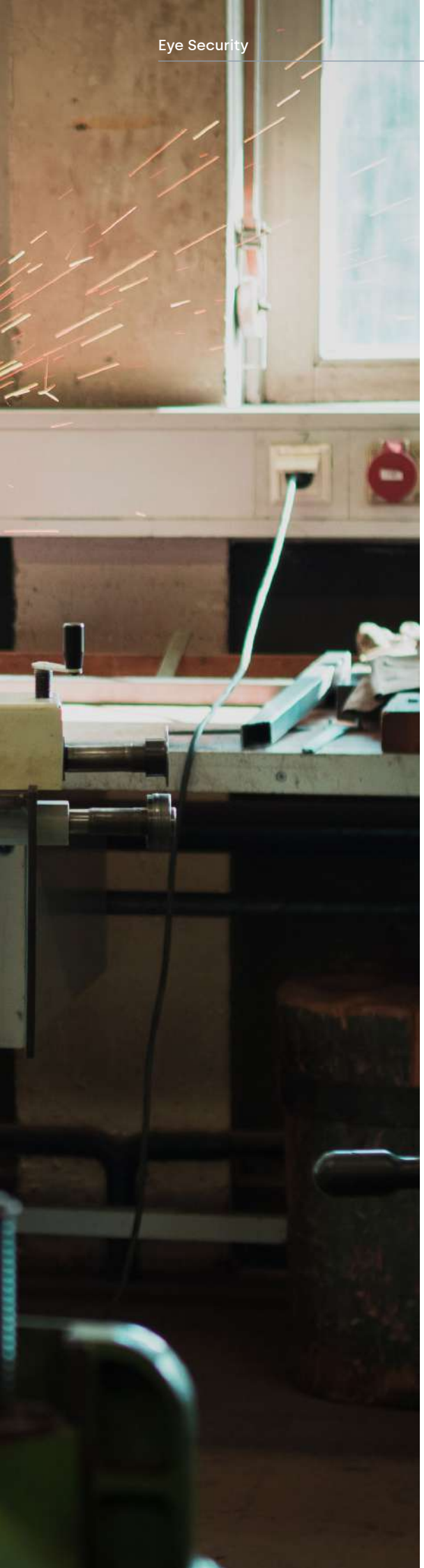
1. In de maakindustrie kan aanhoudende bedrijfsstilstand door een aanval veel ernstigere gevolgen hebben dan in andere sectoren. Dit maakt fabrikanten eerder geneigd om losgeld te betalen. Maakbedrijven zijn sterk afhankelijk van ononderbroken operaties en het missen van vaste leverdata kan rampzalig zijn voor de hele toeleveringsketen.

2. Naast gevoelige persoonlijke en zakelijke informatie beschikken maakbedrijven over grote hoeveelheden waardevolle data, waaronder handelsgeheimen en intellectueel eigendom. Deze kunnen op het dark web aan de hoogste bieder worden verkocht.

5.

Bescherm je maakbedrijf met 9 cruciale beveiligingsmaatregelen

Hieronder vind je de negen belangrijkste beveiligingsmaatregelen om jezelf te beschermen tegen ransomware.



1. Volg best practices

Er zijn verschillende cyber- en informatiebeveiligingskaders ontwikkeld door overheidsorganisaties, zoals het Amerikaanse National Institute of Standards and Technology (NIST), het Duitse Bundesamt für Sicherheit in der Informationstechnik (BSI) en het Nederlandse Nationaal Cyber Security Centrum (NCSC). Kies een framework dat past bij het beveiligingsniveau en de omvang van je organisatie, en houd rekening met eventuele budget- en resourcebeperkingen.

2. Begrijp je beveiligingspositie

Het is lastig je bedrijf te beveiligen als je niet weet wat je beschermt. Identificeer je kritieke assets en informatie, beoordeel je infrastructuur en breng de kwetsbaarheden met hoge prioriteit in kaart. Stel een plan op om deze te mitigeren.

3. Maak immutable, externe back-ups

Als het ergste gebeurt en een ransomware-aanval succesvol is, biedt het betalen van losgeld geen garantie dat je versleutelde data terugkrijgt. Betrouwbare en onaangetaste back-ups van je cruciale gegevens zijn essentieel.

4. Implementeer preventieve beveiligingsmaatregelen

Deze vormen de basis van je beveiliging. Denk aan technologieën die aanvallen blokkeren, zoals endpoint protection platforms (EPP), firewalls en e-mail- en webbeveiliging. Segmenteer je IT-, OT-, BYOD- en gastnetwerken en overweeg een microsegmentatiestrategie voor verschillende beveiligingszones.

5. Creëer een cultuur van cyberbewustzijn

Stel een programma voor security awareness-training (SAT) op. Veel bedrijven zien dit als een verplicht "afvinklijstje" om te voldoen aan regelgeving of verzekeringscriteria. Om echter gedragsverandering te stimuleren en een cultuur van cyberbewustzijn te creëren, kies je een SAT-aanbieder met aantrekkelijke trainingen, ontwikkeld door onderwijsexperts in samenwerking met ethische hackers en cybersecurityprofessionals.

6. Beveilig identiteiten

Volgens het Verizon Data Breach Investigations Report 2024 was 25% van de datalekken in de maakindustrie het gevolg van gestolen inloggegevens, en werd bij 55% van de systeeminbreuken phishing gebruikt. Verminder dit risico door sterke wachtwoordbeleid en multi-factor authenticatie (MFA) in te voeren.

Implementeer Cloud Detection and Response (CDR) om verdachte activiteiten in je cloudtoepassingen te monitoren, zoals inlogpogingen vanuit meerdere onmogelijke locaties. Controleer ook je licenties voor Microsoft-toepassingen; mogelijk heb je al toegang tot Microsoft Sentinel, dat Entra ID-bescherming biedt.

7. Assume breach

Preventieve maatregelen voorkomen niet elke aanval. Bereid je voor op het scenario waarin een aanvaller je netwerk of applicaties weet binnen te dringen.

Een ransomware-actor zal lateraal door je netwerk bewegen op zoek naar waardevolle informatie om te stelen en versleutelen. Om deze activiteit te detecteren, implementeer je Endpoint Detection and Response (EDR).

Als je een toonaangevend EPP gebruikt, zoals CrowdStrike of Microsoft Defender, heb je deze functies waarschijnlijk al. Als je EPP geen EDR bevat, overweeg dan een upgrade naar een oplossing die dit wel biedt.

8. Besteed uit aan een MDR-provider met een 24/7 SOC

Om volledig te profiteren van je investeringen heb je getraind SecOps-personeel nodig dat de tijd en tools heeft om aanvallen te beantwoorden. Gezien het wereldwijde tekort aan cybervaardigheden besteden veel organisaties deze verantwoordelijkheid uit aan een Managed Detection and Response (MDR)-provider.

Een MDR-provider monitort je CDR- en EDR-systemen en reageert om aanvallen in te dammen. Sommige bieden ook incident response-diensten en uitgebreide ondersteuning voor je beveiligingsprogramma, inclusief de eerder genoemde maatregelen.

9. Schaf een cyberverzekering aan

Dit is je laatste, maar uiterst belangrijke beveiligingsmaatregel. Zelfs als je voorbereid bent op aanvallen, moet je ook rekening houden met de financiële gevolgen van een succesvol incident.

Een verzekering moet directe en indirecte kosten dekken, inclusief aansprakelijkheden binnen je complexe toeleveringsketen. Veel MDR-providers hebben nauwe samenwerkingen met verzekeringsmakelaars, waardoor je kunt profiteren van lagere premies en een eenvoudiger aanvraagproces.

Deze gids heeft zich gericht op ransomware en je organistie hiertegen beschermen, moet je hoogste prioriteit zijn, maar houd er rekening mee dat je ook te maken kunt krijgen met andere dreigingen, zoals bedrijfsspionage en sabotage.

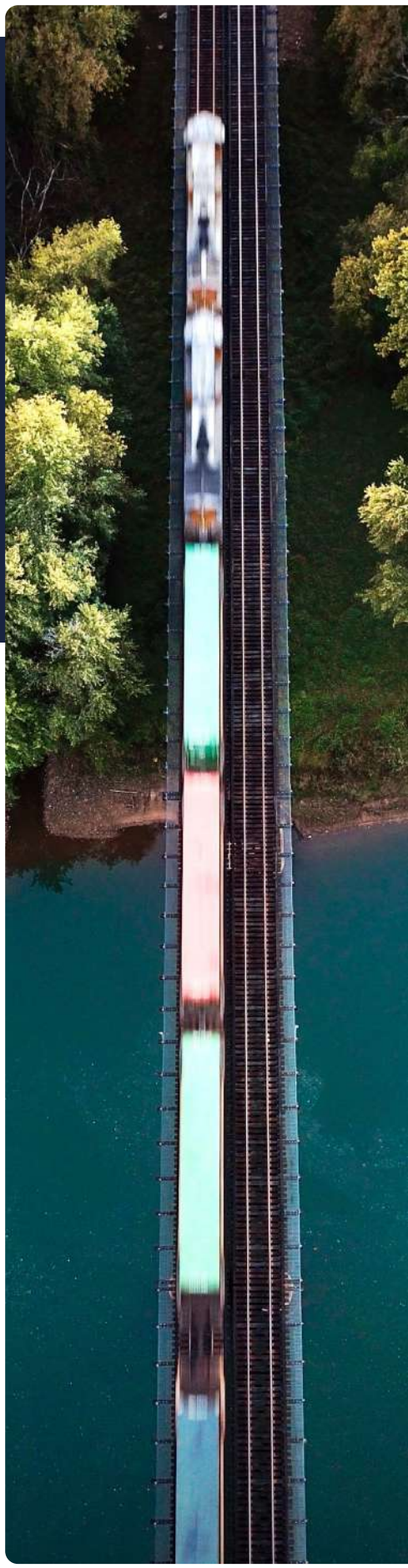
Zodra de basismaatregelen op orde zijn, kun je je richten op bescherming tegen deze minder voorkomende dreigingen. Overweeg om een eigen Security Operations Center (SOC) op te zetten met de juiste tools en specialistisch SecOps-personeel. Daarnaast kun je je OT-omgeving beter beveiligen door specialistisch asset- en kwetsbaarhedenbeheer in te zetten. Netwerkdetectie en -respons (NDR)-tools bieden diepgaand inzicht in al het netwerkverkeer, maar vereisen experts om deze te implementeren en te monitoren.

6. Conclusies en vervolgstappen

Waarschijnlijk heb je al veel van de aanbevolen beveiligingsmaatregelen geïmplementeerd of staan ze op je planning. Om je prioriteiten voor aanvullende beveiliging te bepalen, moet je ransomwarebescherming zien als je belangrijkste focus. De meeste aanvallen zullen inloggegevens en/of endpoints compromitteren, gecombineerd met datadiefstal.

Richt je inspanningen daarom op het detecteren, reageren op en indammen van dergelijke aanvallen.

Deze gids heeft je geholpen te begrijpen waarom je een doelwit bent, welke maatregelen je kunt nemen om het risico van een succesvolle aanval te verkleinen, en hoe je de impact van het ergste scenario kunt beperken.



Ontdek hoe andere maakbedrijven zich wapenen tegen cyberdreigingen

Case study: KeyTec Netherlands

Toen het aantal ransomware-aanvallen in hun sector sterk steeg, besloot maakbedrijf KeyTec actie te ondernemen. Ontdek hoe Eye Security hen hielp hun verdediging proactief te versterken en een cyberbewuste werkcultuur te creëren.

Case study: Signature Foods

Nu cybercriminaliteit steeds geavanceerder wordt, wenden bedrijven zich tot externe partners om bij te blijven. Ontdek hoe Eye Security Signature Foods binnen enkele weken complete cyberbeveiliging bood.

Eye Security helpt maakbedrijven veilig te blijven met 24/7 dreigingsmonitoring, snelle incidentresponse en geïntegreerde cyberverzekeringen. Wij maken cybersecurity eenvoudig en effectief, zodat jij je kunt richten op het draaiend houden van je operaties en het halen van je productiedoelen, zonder zorgen.

Over www.eye.security