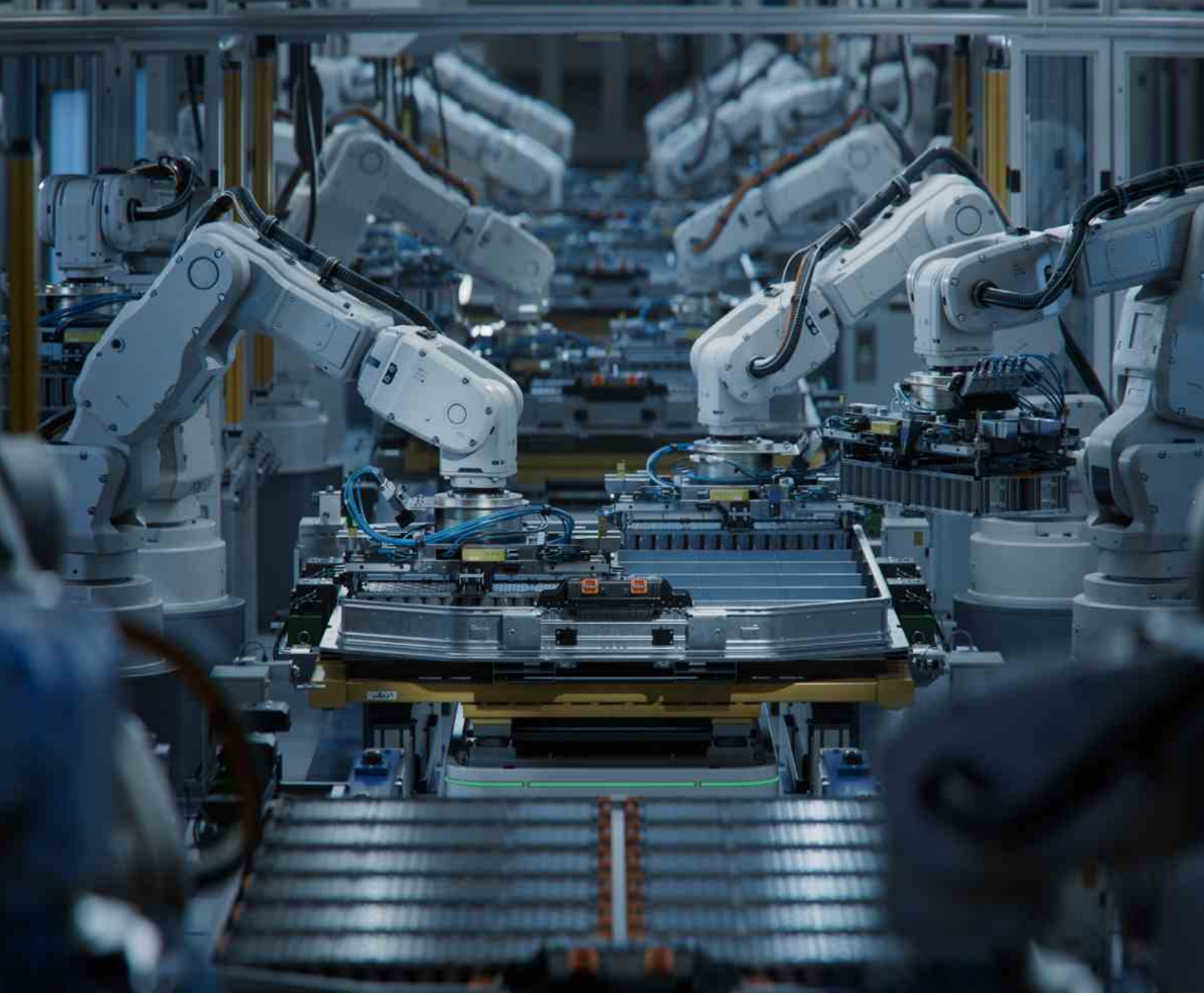


De staat van industriële cybersecurity

Kaspersky's inzichten in bedreigingen in de sector

kaspersky.com
www.securelist.com

kaspersky BRING ON THE FUTURE

Inleiding

De Vierde Industriële Revolutie heeft ongekende mogelijkheden voor innovatie en economische groei met zich meegebracht en heeft industrieën wereldwijd geherdefinieerd. Deze nieuwe golf van technologische vooruitgang is veelbelovend, maar brengt ook nieuwe risico's en uitdagingen met zich mee.

Nergens is dit duidelijker dan in het industriële cyberlandschap. Industriële sectoren hebben al enige tijd te maken met een alarmerende toename van cybergerelateerde incidenten[1]. Hoewel industriële ondernemingen steeds volwassener worden op het gebied van cybersecurity, worden hun OT-systemen nog steeds blootgesteld aan cyberdreigingen[2]. Deze bedreigingen treffen vooral systemen die steeds meer onderling verbonden industriële activiteiten programmeren, bewaken en besturen, van technische werkstations, 3D- en fysieke modellering en CAD/CAM-systemen tot SCADA-servers, HMI's en andere soorten OT-gerelateerde computers.

De snelle implementatie van 'slimme' fabrieksinitiatieven over de hele wereld, ontworpen om de productie te stroomlijnen en te automatiseren, heeft de situatie verder verergerd. Naarmate deze verbonden technologieën de kern van industriële activiteiten worden, nemen ook de cyberrisico's toe. Dit probleem is niet onopgemerkt gebleven bij wereldwijde cybersecuritybedrijven, zoals Kaspersky, dat beschikt over een uitgebreid netwerk van threat intelligent experts die actief samenwerken met industrieën over de hele wereld.

Kritieke infrastructuur en productiesectoren zijn belangrijke doelwitten geworden voor cybercriminelen. Een van de belangrijkste incidenten in de recente geschiedenis was de aanval op Colonial Pipeline in mei 2021[3]. De ransomware-aanval leidde tot de sluiting van een belangrijke pijpleiding die bijna de helft van de brandstof aan de Amerikaanse oostkust levert, wat leidde tot wijdverspreide paniek, brandstoftekorten en miljoenen dollars aan schade.

Gebeurtenissen zoals deze benadrukken de catastrofale gevolgen van cyberaanvallen op kritieke infrastructuur: operationele downtime, financiële verliezen, reputatieschade en dreigingen voor de nationale veiligheid. Deze incidenten onderstrepen het belang om voorbereid te zijn op cybersecurity en hierop te reageren binnen de industriële sector.

Met haar uitgebreide ervaring in industriële cybersecurity heeft Kaspersky onderzocht hoe deze bedreigingen zich ontwikkelen en hoe C-level leidinggevenden deze waarnemen terwijl ze hun bedrijven verdedigen tegen talloze cyberaanvallen.

Dit rapport bespreekt de bevindingen van Kaspersky's onderzoek en schetst de cybersecurityuitdagingen waar de industrie tegenwoordig mee te maken heeft.

Methodologie

Kaspersky heeft in augustus 2024 een uitgebreid onderzoek uitgevoerd onder 203 C-level besluitvormers van grote ondernemingen met meer dan 1.000+ werknemers in sectoren zoals energie, productie en olie & gas. De respondenten werden ondervraagd over cybersecuritymaatregelen binnen hun organisaties, de barrières waar zij als managementteam mee te maken hebben en de uitdagingen die kwetsbaarheden in hun toeleveringsketens met zich meebrengen.

Belangrijkste bevindingen

Bewust van cybersecurity. maar onvoldoende voorbereid

Ondanks het bewustzijn van de noodzaak van cybersecurity was slechts 82% van de respondenten van mening dat hun verbonden en geautomatiseerde toeleveringsketens kwetsbaar waren voor cyberaanvallen, met opmerkelijke verschillen tussen sectoren:

- Olie & Gas: 94%
- Energie: 92%
- Productie: 69%

1 Industrial sector attacks on the rise: an annual overview by Kaspersky
2 www.kaspersky.com/about/press-releases/industrial-sector-attacks-on-the-rise-an-annual-overview-by-kaspersky
3 www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

De frequentie van cybersecurity-incidenten

Maar liefst 94% van de organisaties heeft in de afgelopen 12 maanden te maken gehad met een cybersecurityincident, waarvan 41% werd geclassificeerd als ernstige verstoring:

- Energie: 96%
- Productie: 90%
- Olie & Gas: 100%

IoT wordt gezien als de grootste bedreiging voor cybersecurity

De enquête onthulde de belangrijkste bedreigingen voor cybersecurity die door industriële organisaties worden ervaren:

- Kwetsbaarheden van verbonden/IoT-apparaten – 22%
- Fysieke beveiligingsinbreuken – 21%
- Bedreigingen van binnenuit – 21%

"Organisaties denken vaak dat ze minder kwetsbaar zijn omdat hun omgeving uit niet standaard systemen bestaat", legt Jornt van der Wiel, security-expert bij Kaspersky's Global Research and Analysis Team uit. "Als de aanvallers eenmaal binnen zitten, zijn ze vaak in staat om handleidingen of andere informatie te bemachtigen om zo een beter inzicht te krijgen in de omgeving van het doelwit, waarna zij over kunnen gaan tot de uiteindelijke aanval. Het zogenaamde "security through obscurity" is dus een slecht uitgangspunt."

Industriële cybersecurity: Een momentopname

Regio's wereldwijd worden in verschillende mate blootgesteld aan cyberaanvallen. Maar volgens Evgeny Goncharov, hoofd van Kaspersky's ICS CERT[4], worden OT-infrastructuren minder blootgesteld aan cyberdreigingen door verbeteringen in hun cybersecurity-cultuur en investeringen in security-maatregelen.

"Desondanks blijft het algehele risico hoog, omdat voor geraffineerde hackers zelfs een kleine mate van blootstelling al genoeg is. En de zaken

3 Industrial cybersecurity in 2024: trends and forecasts

worden steeds gecompliceerder nu industrieën slimme technologieën gaan gebruiken die nieuwe toegangspunten voor aanvallers introduceren, evenals nieuwe manieren om de aanval uit te breiden naar vergelijkbare organisaties."

"Ransomware blijft een kritiek punt waarbij cybercriminelen zich steeds meer richten op industriële organisaties voor financieel gewin. Tegelijkertijd neemt hacktivisme toe, waarbij politiek gemotiveerde aanvallers ransomware tactieken gebruiken om industrieën te ontwrichten en aanzienlijke schade te veroorzaken," zegt Goncharov.

Recente voorbeelden van opvallende cyberaanvallen onderstrepen de potentiële financiële verliezen waarmee industriële bedrijven te maken kunnen krijgen. Johnson Controls bijvoorbeeld, een producent van automatiseringssystemen voor gebouwen, werd getroffen door een ransomware-aanval die resulteerde in een verlies van 30 miljoen dollar. Ook MKS Instruments, een chipfabrikant die de auto-industrie bedient, kreeg te maken met een schadepost van 200 miljoen dollar, terwijl Clorox, een grote producent van ontsmettingsmiddelen, zijn netto-omzet zag dalen met 357 miljoen dollar door productiestilstand als gevolg van een cyberaanval. Deze incidenten illustreren de verwoestende impact die cyberaanvallen kunnen hebben op bedrijven, vooral wanneer productie- en verzendactiviteiten worden verstoord.

De toenemende dreiging van OT boven IT

In het tweede kwartaal van 2024 laat het industriële dreigingslandschap zien dat cyberdreigingen nog steeds invloed hebben op OT-omgevingen, vooral in de energie- en productiesectoren[5]. Tot de belangrijkste bedreigingen behoren ransomware, gegevensdiefstal en de verspreiding van malware. Het rapport onthult dat kwaadaardige internetbronnen en phishing veelvoorkomende toegangspunten blijven voor aanvallers. Geavanceerde criminelen richten zich ook op de toeleveringsketen om doelwitten te infiltreren. Om deze kritieke infrastructuren te beschermen, worden versterkte cybersecuritymaatregelen geadviseerd.

Naarmate meer industriële systemen afhankelijk worden van onderling verbonden apparaten, neemt het risico op cyberaanvallen toe. Onlangs hebben aanvallers misbruik gemaakt van de kwetsbaarheden in kritieke systemen, wat operational downtime veroorzaakte in een watervoorzieningsysteem in Ierland.[6]

De integratie van telematica en fleetmanagementsystemen in voertuigen verhoogt het risico dat aanvallers de controle over hun logistiek overnemen, waaronder transportvloten. Afgelegen energie- en olie- en gasinstallaties kunnen ook kwetsbaar zijn voor een soortgelijke dreiging. Nu steeds meer industrieën overstappen op digitale systemen en systemen op afstand, wordt verwacht dat de kans op grootschalige cyberaanvallen met ernstige gevolgen alleen maar zal toenemen.

OT omvat het beheer van fysieke processen en machines, waardoor het gevoeliger is voor gerichte cyberaanvallen met reële gevolgen. Veel organisaties worstelen met de beveiliging van hun OT-omgevingen nu deze zich uitbreiden naar geautomatiseerde en onderling verbonden systemen. Deze verschuiving heeft een aanzienlijk gat in de cyberbeveiliging blootgelegd, waarbij bedreigingen zich verplaatsen van IT-domeinen naar OT-infrastructuren, waardoor kritieke industriële activiteiten kwetsbaar worden voor aanvallen.

Condor Carpets stond voor precies deze uitdaging[7]. Als bedrijf met meerdere productiefaciliteiten en een complex netwerk van machines en automatiseringssystemen, zag men de noodzaak van een op maat gemaakte oplossing voor industriële cybersecurity in. De bestaande IT-beveiligingen waren niet langer voldoende om het groeiende OT-netwerk met meer dan 30 machines en proceslijnen te beheren.

Door de implementatie van Kaspersky Industrial CyberSecurity kon Condor een kritisch inzicht krijgen in het OT-netwerk en potentiële kwetsbaarheden in de programmeerbare logische controllers identificeren.

5 Threat landscape for industrial automation systems, Q2 2024
6 H2 2023 – a brief overview of main incidents in industrial cybersecurity

"Naarmate onze activiteiten zich uitbreidden, realiseerden we ons dat onze bestaande IT-beschermingen niet langer toereikend waren voor het beheer van ons groeiende OT-netwerk, dat nu meer dan 30 machines en proceslijnen omvat," aldus Patrick de Haan, IT Manager bij Condor Carpets. *"We stonden voor grote uitdagingen bij het verkrijgen van volledige zichtbaarheid en controle over onze complexe OT-omgeving zonder onze continue productiecycli te verstoren. Het beheer van legacy-systemen die draaien op software die niet wordt ondersteund, was een belangrijk punt van zorg - we hadden een oplossing nodig die robuuste beveiliging garandeerde zonder de functionaliteit in gevaar te brengen.*

De complexiteit van ons OT-netwerk, met gespecialiseerde SCADA-protocollen zoals Modbus en OPC UA, betekende dat standaard IT-securityoplossingen niet toereikend waren. Bovendien moesten we door onze snelle uitbreiding en aankoop van nieuwe faciliteiten de cybersecurity op alle locaties standaardiseren om uniforme beveiligings—protocollen te waarborgen. Efficiënt gebruik van hulpbronnen was ook van het grootste belang; we hadden een effectieve, beheersbare en lean cybersecurityoplossing nodig.

Door Kaspersky Industrial CyberSecurity te implementeren, kregen we kritisch inzicht in onze OT-omgeving en konden we potentiële kwetsbaarheden in onze programmeerbare logische controllers identificeren. Hun oplossing pakte al onze uitdagingen aan: het gaf ons uitgebreide zichtbaarheid en controle, beheerde onze oudere systemen effectief en verstoorde onze productie-workflows niet. De oplossingen van Kaspersky hebben een revolutie teweeggebracht in ons netwerk- en cybersecurityprofiel. We hebben vertrouwen in hun vermogen om onze complexe activiteiten nu en in de toekomst te beschermen."

De belangrijkste cybersecuritydreigingen voor productie, energie en olie & gas

Kwetsbaarheden in verbonden/ IoT-apparaten	22%
Onbevoegde toegang of diefstal van inlog-gegevens (criminelen krijgen toegang tot productiesystemen of gevoelige gegevens door zich voor te doen als legitieme gebruikers)	19%
DDoS-aanvallen (Distributed Denial of Service)	16%
Bedreigingen van binnenuit (werknemers, ingehuurden, partners met kwade bedoelingen)	21%
Ransomware	15%
Phishing en social engineering-aanvallen.	16%
Kwetsbaarheden in legacy systemen	15%
Zero day exploits	18%
Fysieke beveiligingsinbreuken (fysieke inbraken/knoeien met apparatuur die leiden tot cyberrisico's/verstoringen)	21%
Aanvallen op de supply chain	14%
Malware en botnets	12%
Niet-naleving van regelgeving (niet-naleving van sectorspecifieke regelgeving)	19%
Gebrek aan zichtbaarheid van het netwerk (d.w.z. het risico dat je niet op de hoogte bent van sommige machines in je infrastructuur).	17%
Cyberspionage	17%
Gebrek aan beveiligingsbewustzijn en training	18%
Datalekken	15%
N.v.t. Geen bijzondere bedreigingen	0%
Niet zeker	0%

Groeiende bedreigingen voor IoT-apparaten

Het toegenomen gebruik van IoT-apparaten in industriële activiteiten heeft het aanvalsoppervlak vergroot, waardoor deze systemen aan grotere risico's worden blootgesteld. 22% van de respondenten noemde kwetsbaarheden in IoT als

7 Condor Carpets: Securing operations with Kaspersky

hun grootste zorg, wat de urgentie voor robuuste IoT-specifieke beveiligingsprotocollen benadrukt. Het enorme aantal aangesloten apparaten bemoeilijkt de beveiligingsinspanningen, omdat elk apparaat een potentieel toegangspunt vormt en vaak niet gemakkelijk kan worden bijgewerkt zonder de bedrijfsvoering te verstoren. Om deze risico's aan te pakken is een allesomvattende aanpak nodig, inclusief voortdurende monitoring, netwerksegmentatie en strikt patchbeheer, om industriële omgevingen te beschermen tegen de toenemende dreigingen van IoT-kwetsbaarheden.

Menselijke factoren vormen nog steeds een aanzienlijk risico

Bedreigingen van binnenuit en phishing blijven hardnekkige problemen in de industriële sector, waarbij 16% van de respondenten social engineering als grootste zorg noemt. Dit benadrukt de noodzaak voor strenge toegangscontroles en voortdurende monitoring van de activiteiten van werknemers en ingehuurden. Effectieve maatregelen zijn onder andere het implementeren van strenge toegangscontroles, regelmatige training van werknemers om phishing-pogingen te herkennen en voortdurende controle van activiteiten van werknemers en ingehuurden. Door deze menselijke kwetsbaarheden aan te pakken, kunnen organisaties het risico van bedreigingen van binnenuit en social engineering aanzienlijk verkleinen en een veerkrachtigere beveiligingspostuur voor al hun activiteiten bevorderen.

Legacy systemen

Legacy systemen, die vaak moeilijk te patchen en te onderhouden zijn, zijn bijzonder kwetsbaar voor aanvallen. Omdat deze legacy-systemen vaak geïntegreerd zijn in essentiële industriële processen, zijn ze moeilijk te vervangen of aan te passen zonder het risico te lopen dat de bedrijfsvoering wordt verstoord. Als gevolg hiervan kunnen organisaties securityoplossingen voor de korte termijn aannemen, die na verloop van tijd voor nog meer complexiteit kunnen zorgen. Deze afhankelijkheid van verouderde technologie onderstreept de dringende behoefte aan een strategische aanpak om verouderde systemen in industriële omgevingen te upgraden of te beveiligen, waarbij veerkracht tegen opkomende cyberdreigingen prioriteit heeft.

DDoS-aanvallen

DDoS-aanvallen (Denial-of-Service) vormen een groeiend risico voor industriële activiteiten, waarbij 16% van de respondenten aangeeft zich grote zorgen te maken over de mogelijke impact ervan. Deze aanvallen overweldigen netwerken door ze te overspoelen met buitensporig verkeer, waardoor essentiële diensten worden verstoord en de productie mogelijk wordt stilgelegd. In industriële omgevingen, waar continue uptime van cruciaal belang is, kan een DDoS-aanval leiden tot ernstige operationele en financiële gevolgen, waaronder inkomstenverlies, hogere herstelkosten en het vertrouwen van klanten beschadigen.

Menselijke factoren vormen nog steeds een aanzienlijk risico

Bedreigingen van binnenuit en ongeoorloofde toegang blijven hardnekkige problemen in de industriële sector, waarbij 19% van de respondenten ongeoorloofde toegang of diefstal van inlog-gegevens als grootste zorg noemt. Dit benadrukt de noodzaak van strenge toegangscontroles en voortdurende controle van de activiteiten van werknemers en ingehuurden.

Kwetsbaarheid van supply chain

De kwetsbaarheid van toeleveringsketens blijft een kritiek punt voor industrieën. Ondanks aanzienlijke investeringen in technologie en infrastructuur vindt 74% van de respondenten dat hun supply chains gevoelig zijn voor cyberaanvallen. Sectorspecifieke cijfers tonen een nog grotere bezorgdheid in Olie & Gas (94%) en Energie (47%).

Deze hoge mate van kwetsbaarheid is te wijten aan de snelle digitale transformatie binnen industriële activiteiten. Systemen die voorheen om veiligheidsredenen van externe netwerken waren afgesloten, zijn nu opengesteld voor betere gegevensdeling en -integratie. Helaas heeft dit ook nieuwe cyberdreigingen mogelijk gemaakt. Onderzoek van Kaspersky laat zien dat de toename in connectiviteit niet gepaard is gegaan met een evenredige investering in cybersecurity, waardoor toeleveringsketens kwetsbaar blijven.

Cybersecurityincidenten: Een terugkerend probleem

94% van de respondenten gaf aan in de afgelopen 12 maanden een cybersecurityincident te hebben

meegemaakt. Voor veel sectoren waren deze incidenten geen incidentiele, maar terugkerende gebeurtenissen. 96% van de energiebedrijven was bijvoorbeeld aangevallen, wat leidde tot aanzienlijke operationele verstoringen en productiestilstand.

Deze cijfers weerspiegelen een zorgwekkende trend: bedrijven bereiden zich voor op cyberaanvallen in plaats van ze te voorkomen. Veel organisaties accepteren dat aanvallen onvermijdelijk zijn en richten zich meer op het reageren op incidenten en het beperken van de schade dan op preventie. Deze reactieve aanpak is echter op de lange termijn onhoudbaar.

Van der Wiel vervolgt: “Organisaties en risico-managers vinden de verzekeringskosten onbetaalbaar. Velen weten niet wat ze anders moeten doen. Er is een zwart gat van onbegrip. Het is een echte zorg voor hen. Ze maken zich zorgen, maar ze vertrouwen erop dat IT alles regelt. Het is als een tikkende tijdbom.”

Barrières voor effectieve cybersecurity

Gevraagd naar de barrières voor verkrijgen van een volledig begrip van cybersecurity op managementniveau, noemden de respondenten verschillende belangrijke uitdagingen:

- Moeite om het snel veranderende bedreigings-landschap bij te houden- 30 %
- Moeite met het kwantificeren van risico’s - 30%
- Balanceren tussen naleving en operationele doelstellingen - 30%

Interessant genoeg werden budgettaire beperkingen, die vaak als een belangrijk probleem bij het plannen van cybersecurity worden genoemd, in dit onderzoek minder vaak als zorg genoemd. 24% van de respondenten noemde het als een belemmering, wat nog steeds een aanzienlijk percentage is.

De belangrijkste barrières voor een volledig en uitgebreid begrip van cybersecurity

Het gebruik van jargon/onduidelijke termen	24%
Moeilijkheid bij het kwantificeren van risico’s (bijvoorbeeld het beoordelen van de impact van een cyberincident op productietijd, inkomsten en reputatie).	30%
Last om te voldoen aan sectorspecifieke regelgeving en tegelijkertijd operationele doelstellingen in evenwicht te houden	30%
Gebrek aan expertise en technische kennis op het gebied van cyberbeveiliging	28%
Complexiteit van onderling verbonden industriële besturingssystemen en operationele technologie	26%
Moeite om het snel veranderende bedreigingslandschap bij te houden	30%
Culturele en/of organisatorische barrières	23%
Algemeen tijdgebrek	21%
Laag risico op cyberaanvallen	24%
Budgettaire beperkingen	24%

Een proactieve benadering van cybersecurity ontwikkelen

De reis van de industriële sector door de Vierde Industriële Revolutie biedt zowel enorme kansen als aanzienlijke cyberrisico’s. Met de groeiende connectiviteit neemt de kwetsbaarheid toe en de gevolgen van niets doen zijn al merkbaar.

De boodschap is duidelijk: industriële bedrijven moeten een mentaliteit van onvermijdelijkheid inruilen voor een mentaliteit van preventie. Door te investeren in de juiste tools, training en informatie over bedreigingen, kunnen ze hun activiteiten beveiligen, hun toeleveringsketens beschermen en zorgen voor langdurige veerkracht tegen evoluerende cyberbedreigingen.

Van der Wiel concludeert: “Ons onderzoek toont aan dat IT de verantwoordelijkheid voor security krijgt, maar niet weet hoe ze een OT-omgeving effectief moeten beveiligen. Er is een gebrek aan training, vooral in OT-specifieke cybersecurity en het begrijpen van de bijbehorende cyberrisico’s,

wat ook wijst op een tekort aan vaardigheden in Nederland. De meeste mensen in OT zijn netwerkingenieurs - ze zijn goed in netwerken, maar niet in cybersecurity. Zowel OT als cybersecurity zijn specifieke vakgebieden, en een combinatie van deze twee expertisegebieden is zeldzaam."

Met 25 jaar ervaring in het beschermen van meer dan 400 miljoen gebruikers en 240.000 bedrijven wereldwijd, beschikt Kaspersky over een schat aan sectorspecifieke kennis en expertise. Dit plaatst hen in een unieke positie om voorlichting te geven en het bewustzijn te vergroten over de reële dreiging van cybercriminelen voor de industriële sector.

Kaspersky benut haar uitgebreide ervaring in het beschermen van organisaties binnen deze sector en grijpt nu de kans om een bewustwordingscampagne te leiden. Deze campagne richt zich op hoe de toenemende connectiviteit van industriële systemen niet alleen een nieuwe innovatiegolf teweegbrengt, maar ook een nieuw tijdperk van cyberrisico's. Het benadrukt waarom actuele dreigingsinformatie en nauwkeurige endpointsecurity cruciale onderdelen moeten zijn van de verdedigingsstrategie van elke moderne productieorganisatie.

Beter voorkomen dan genezen

Kaspersky's visie richt zich op het voorkomen van aanvallen, in plaats van simpelweg te reageren nadat een hack heeft plaatsgevonden. Het bedrijf erkent dat veel leveranciers weliswaar uitblinken in het opsporen en herstellen van incidenten, maar dat de echte waarde ligt in het voorkomen van cyberaanvallen.

Deze proactieve aanpak is vooral van cruciaal belang in industriële omgevingen waar downtime kan leiden tot aanzienlijke financiële en operationele verliezen. Volgens gegevens van Kaspersky kost het een onderneming gemiddeld meer dan een half miljoen US dollar om te herstellen van een inbreuk op de beveiliging. Terwijl het gemiddelde verwachte verlies voor het MKB 38.000 dollar is[8].

De oplossingen van Kaspersky zijn ontworpen om de unieke uitdagingen van industriële activiteiten aan te gaan, met name in OT-omgevingen waar beveiligingspraktijken vaak achterlopen op die in IT.

8 Damage Control: The Cost of Security Breaches IT Security Risks Special Report Series

Oplossingen voor een veiligere industriële toekomst

KICS (Kaspersky Industrial CyberSecurity)

OT- en IT-omgevingen raken steeds meer geïntegreerd, waardoor systemen worden blootgesteld aan nieuwe cyberdreigingen en een allesomvattende cybersecurityoplossing van één leverancier nodig is. Voor een betrouwbare bescherming van industriële netwerken en automatiseringssystemen gebruiken bedrijven Kaspersky Industrial CyberSecurity (KICS), een OT XDR-platform, dat gecentraliseerd asset- en risicobeheer, beveiligings- en compliance-audits, ongeëvenaarde schaalbaarheid en IT - OT-convergentie met het Kaspersky-ecosysteem biedt.

Intelligentie digitale voetafdruk

Kaspersky biedt digital footprint intelligence om organisaties te helpen kwetsbaarheden en misconfiguraties binnen hun netwerken te identificeren. Met deze tool kunnen bedrijven begrijpen waar ze het meest kwetsbaar zijn en proactief maatregelen nemen om hun infrastructuur te beveiligen.

ICS-training en bijscholing

Kaspersky's cybersecuritytraining voor industriële besturingssystemen (ICS) voorziet werknemers van de benodigde kennis en vaardigheden om effectief te reageren op cyberincidenten. Dit is van cruciaal belang, aangezien steeds meer industriële bedrijven hun OT-beveiliging overlaten aan IT-teams, wat vaak resulteert in hiaten in begrip en bescherming.

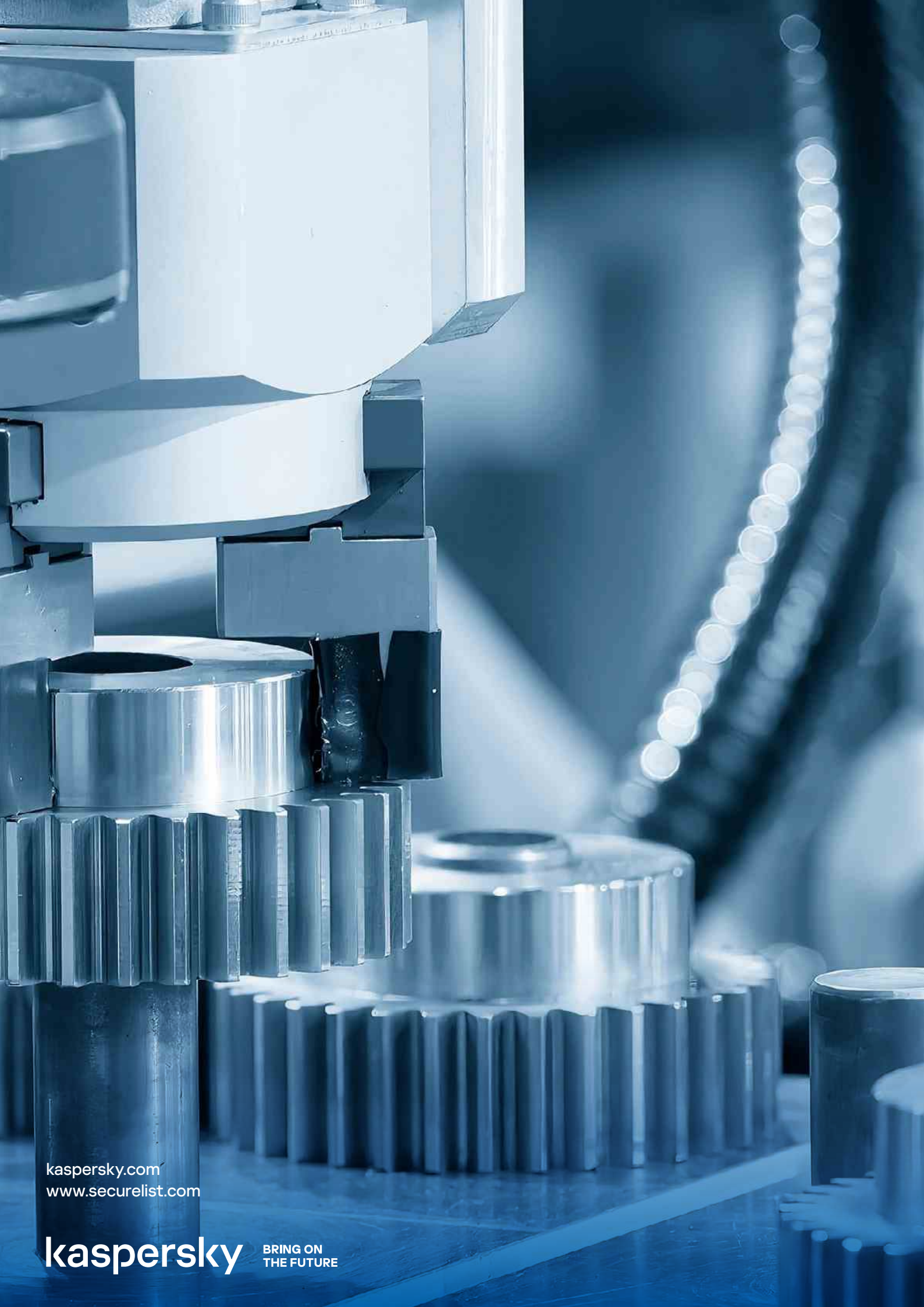
ICS-kwetsbaarheidsfeed

Om de trage reactietijden van leveranciers bij het patchen van kwetsbaarheden aan te pakken, biedt Kaspersky realtime feeds van kwetsbaarheden. Ze helpen bedrijven zwakke plekken te identificeren en te patchen voordat ze kunnen worden uitgebuit.

Uitgebreide opsporing en reactie (XDR)

Kaspersky's XDR-mogelijkheden bieden een uitgebreide oplossing voor het detecteren van en reageren op geavanceerde bedreigingen zoals zero-day exploits en ransomware. Deze technologie combineert dreigingsinformatie met geautomatiseerde responsmechanismen om bedrijven te ondersteunen bij het beperken van risico's in realtime.

9 Industrial sector attacks on the rise: an annual overview by Kaspersky



kaspersky.com
www.securelist.com

kaspersky BRING ON THE FUTURE