cegeka

TRENDRAPPORT

CYBER SECURITY

DIGITALISERING

Hoe (cyber)weerbaar is de maakindustrie?

Een datagedreven onderzoek naar risico's, trends en verbeterkansen

WWW.CEGEKA.COM

Management Summary

De Nederlandse maakindustrie is een drijvende kracht achter innovatie en werkgelegenheid. Tegelijkertijd vormt deze sector een steeds aantrekkelijker doelwit voor hackers, cybercriminelen en geheime diensten. Ransomware, supply chain-aanvallen, spionage en sabotage van OT-systemen zijn geen hypothetische risico's meer, maar dagelijkse realiteit. Vooral kleine en middelgrote maakbedrijven zijn kwetsbaar. En dat terwijl de financiële impact van een aanval voor hen relatief het grootst is.

Cegeka onderzocht de cybersecurity van 245 maakbedrijven

Hoe kwetsbaar zijn maakbedrijven precies? Welke risico's lopen ze? En wat kunnen ze doen om die risico's af te wenden? Om antwoord te geven op die vragen, deed Cegeka onderzoek naar de cybersecurity van 245 Nederlandse maakbedrijven uiteenlopend in omvang van 500 tot 3000 FTE's.

Met dit onderzoek wil Cegeka niet alleen een helder beeld geven van de actuele staat van cybersecurity in de Nederlandse maakindustrie, maar ook bewustzijn creëren over de urgentie van dit onderwerp.

Lage volwassenheid op het gebied van cybersecurity

Uit onze analyse blijkt dat het gemiddelde cyber-security-volwassenheidsniveau in de maakindustrie lager ligt dan in andere sectoren.

- **Maakbedrijven zijn vooral kwetsbaar op het gebied van applicatiebeveiliging, web-encryptie, DNS-beveiliging, netwerkfiltering en patchbeheer.**

  Deze kwetsbaarheden vormen een direct bedrijfsrisico dat raakt aan continuïteit, concurrentiekracht en vertrouwen in de keten.

- **Opvallend is dat zeven bedrijven 101 systemen in Rusland hosten, wat aanzienlijke compliance en spionagerisico's oplevert.**

- **Wat betreft de voorbereiding op NIS2 en de Cybersecuritywet moeten de meeste bedrijven nog stappen zetten.**

  Veel bedrijven beschikken al wel over een basisniveau aan beveiligingsmaatregelen.

  Groeien in security-volwassenheid vraagt om een gestructureerde aanpak, waarin zowel strategische keuzes als dagelijkse operationele discipline samenkomen.

Inleiding

Nederland staat bekend als een echt maakindustrierijk land. Met één op de negen werkenden actief in deze sector en een aandeel van circa 60% in de totale innovatie van het land, vormt de maakindustrie het kloppende hart van de Nederlandse economie.

Van hoogtechnologische machinebouw tot innovatieve materialen en duurzame productiemethoden: de sector wordt wereldwijd geroemd om haar kwaliteit en vindingrijkheid.

Maakbedrijven lopen veel risico

Cybercriminelen en buitenlandse geheime diensten hebben het in toenemende mate voorzien op de IT- en OT-systemen van deze bloeiende Nederlandse sector. Bedrijven worden geconfronteerd met steeds slimmere aanvallen.

Maakbedrijven werken nauw samen met andere ketenpartijen. Vaak zijn de aanvallen gericht op de zwakste schakel in de keten, waarbij toeleveranciers of partners het doelwit vormen. Een verstoring in één schakel kan de hele keten stilleggen, met verstrekkende gevolgen voor leveringsbetrouwbaarheid en reputatie. Dat betekent dat maakbedrijven hun keten moeten managen en andere partijen moeten helpen om hun weerbaarheid te verhogen.

In tegenstelling tot wat in het verleden vaak gedacht werd, lopen maakbedrijven hoge risico's. Vergeleken met andere sectoren scoort de maakindustrie bovengemiddeld hoog op zowel incidentfrequentie als schadebedragen.

Geen organisatie is te klein om doelwit te zijn

Hoe groot het probleem is, blijkt onder meer uit recent onderzoek van het Cyentia Institute en Verizon Data Breach Investigations Report 2025. De cijfers van deze twee onderzoeksinstituten liegen er niet om. In 2024 werden 1.607 bevestigde datalekken in de maakindustrie geregistreerd. Dit is een verdubbeling ten opzichte van het jaar ervoor.

11%

kans dat een maakbedrijf het slachtoffer wordt van een ernstig cyberincident

Inmiddels is de kans dat een maakbedrijf het slachtoffer wordt van een ernstig cyberincident 11%. Vooral kleine en middelgrote maakbedrijven worden het slachtoffer van hackers en cybercriminelen. Geen enkele organisatie is te klein om doelwit te zijn.

Cybersecurity onder de loep

Hoe goed zijn de IT- en OT-omgevingen van Nederlandse maakbedrijven beveiligd? Om antwoord te kunnen geven op die vraag, deed Cegeka onderzoek naar de volwassenheid van cybersecurity in de Nederlandse maakindustrie.

Met dit rapport willen wij een helder beeld geven van de actuele staat van cybersecurity in de Nederlandse maakindustrie. Op basis van een datagedreven analyse van 245 bedrijven laten we zien waar de kwetsbaarheden liggen, welke trends zichtbaar zijn en welke risico's de meeste aandacht vragen. Ons doel is niet alleen inzicht te bieden, maar ook bewustzijn te creëren over de urgentie van dit onderwerp.

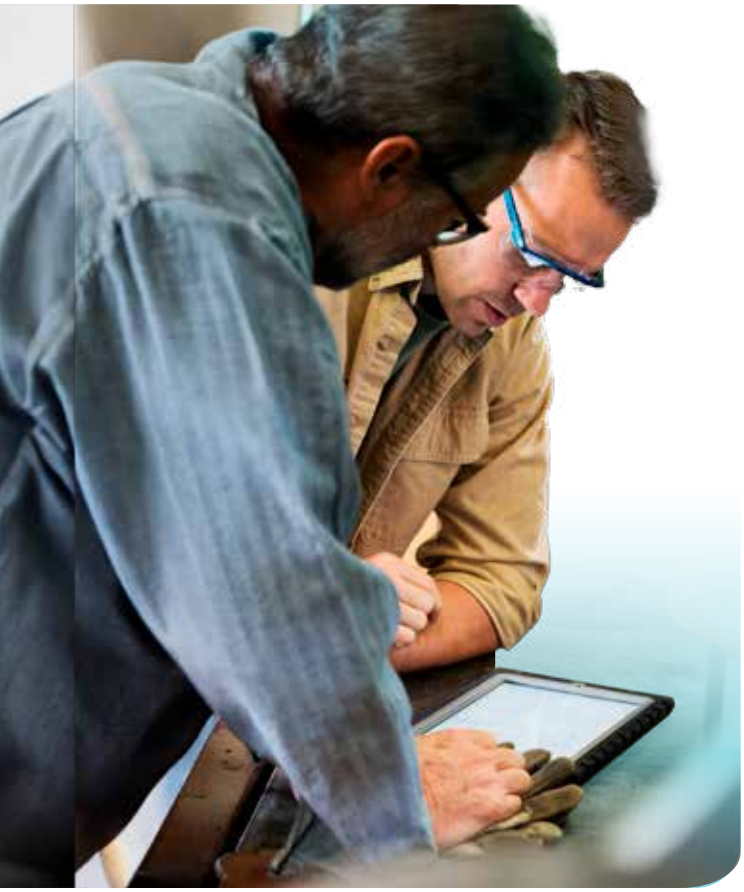
Hoe voerden we dit onderzoek uit?

Om een goed beeld te krijgen van het cybersecurityniveau van de maakindustrie in Nederland, maakten we een representatieve selectie van 245 maakbedrijven. Deze organisaties analyseerden we gedurende een periode van 90 dagen in de zomer van 2025.

We onderzochten allerlei aspecten van de hardware- en software-infrastructuur die 'van buitenaf' zichtbaar zijn. Denk daarbij aan web encryptie, application security, software patching en system hosting. Ook keken we naar zaken als netwerk filtering, DNS security, e-mail security en systemen die communiceren met dubieuze IP-adressen. Dit is een volledig online proces op basis van publiek beschikbare data; informatie waar iedere internetgebruiker toegang toe heeft.

Security Rating platform

Voor dit onderzoek maakten we onder meer gebruik van een geavanceerd Security Rating platform. Dit platform geeft een score aan de verschillende veiligheidsdomeinen op basis van de kwetsbaarheid en de assetwaarde, wat uiteindelijk resulteert in een overkoepelende security rating. Dit eindcijfer geeft een indicatie van de cybersecurity van een organisatie.



De in dit onderzoek geanalyseerde maakbedrijven scoren in de range van 1 (laag) tot 10 (hoog). De scores worden vervolgens vertaald naar ratings A tot en met F. Bedrijven die hoger scoren dan een 8,5 krijgen een A-rating, bedrijven die lager scoren dan een 4 krijgen een F.

Hoe moet je de ratings lezen?

Wanneer bedrijven een C, D, E of F scoren, is dat een indicatie van een lage(re) cybersecurity. Voor bedrijven met een A- of een B-rating geldt dat ze hackers, spionnen en cybercriminelen naar alle waarschijnlijkheid makkelijker buiten kunnen houden.

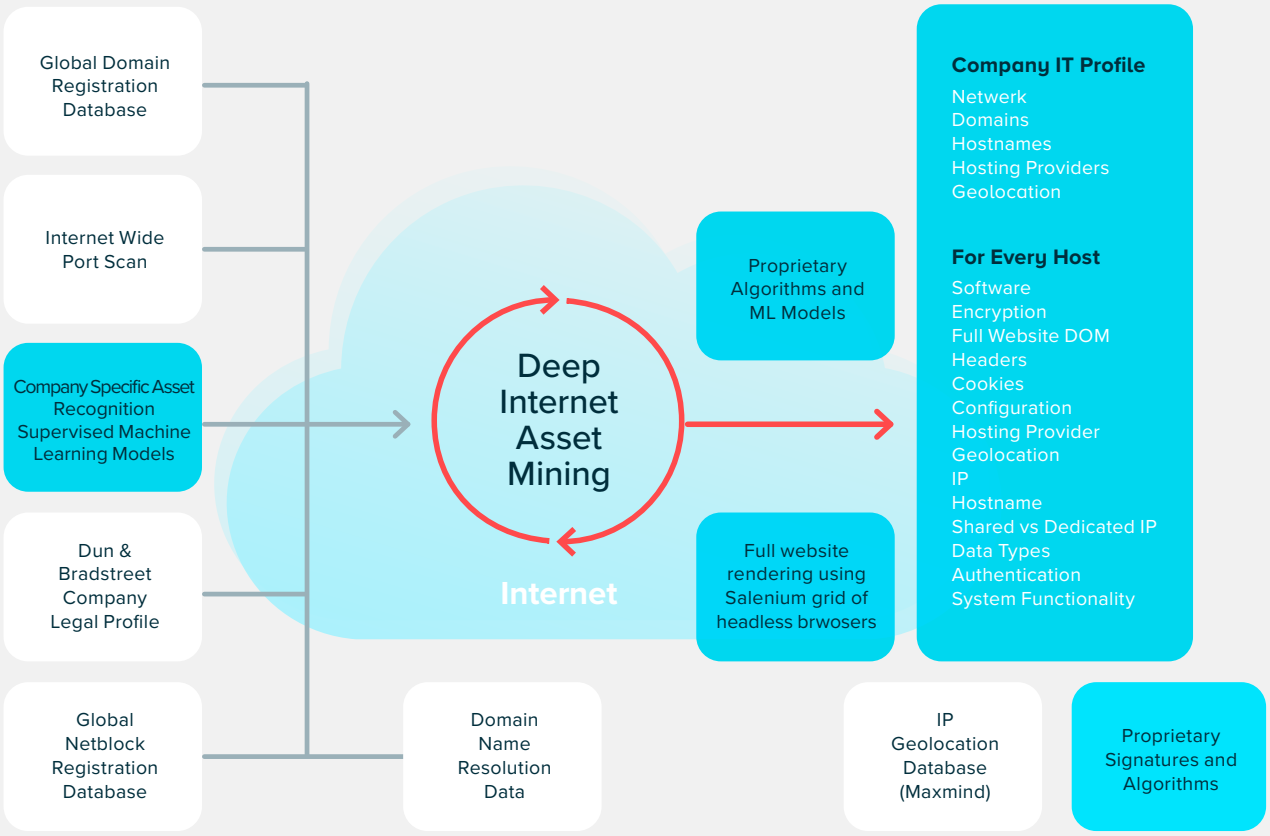
De security rating is óók een indicatie van de security-volwassenheid. Voor bedrijven met een A-rating is statistisch aangetoond dat ze significant minder kans op ransomware-events of datalekken hebben ten opzichte van bedrijven met een F-rating.

Zo werkt het Security Rating platform

Voor dit onderzoek maakten we gebruik van een Security Rating platform. Hiermee brengen we het externe aanvalsoppervlak van organisaties in kaart.

Op basis van een bedrijfsnaam en een domeinnaam bouwt het systeem een volledig profiel op van de organisatie en de internet-facing systemen. Het platform gebruikt hiervoor alleen publieke data die voor iedereen zichtbaar is.

Op basis van een bedrijfsnaam en een domeinnaam bouwt het systeem een volledig profiel op van de organisatie en de internet-facing systemen. Het platform gebruikt hiervoor alleen publieke data die voor iedereen zichtbaar is.



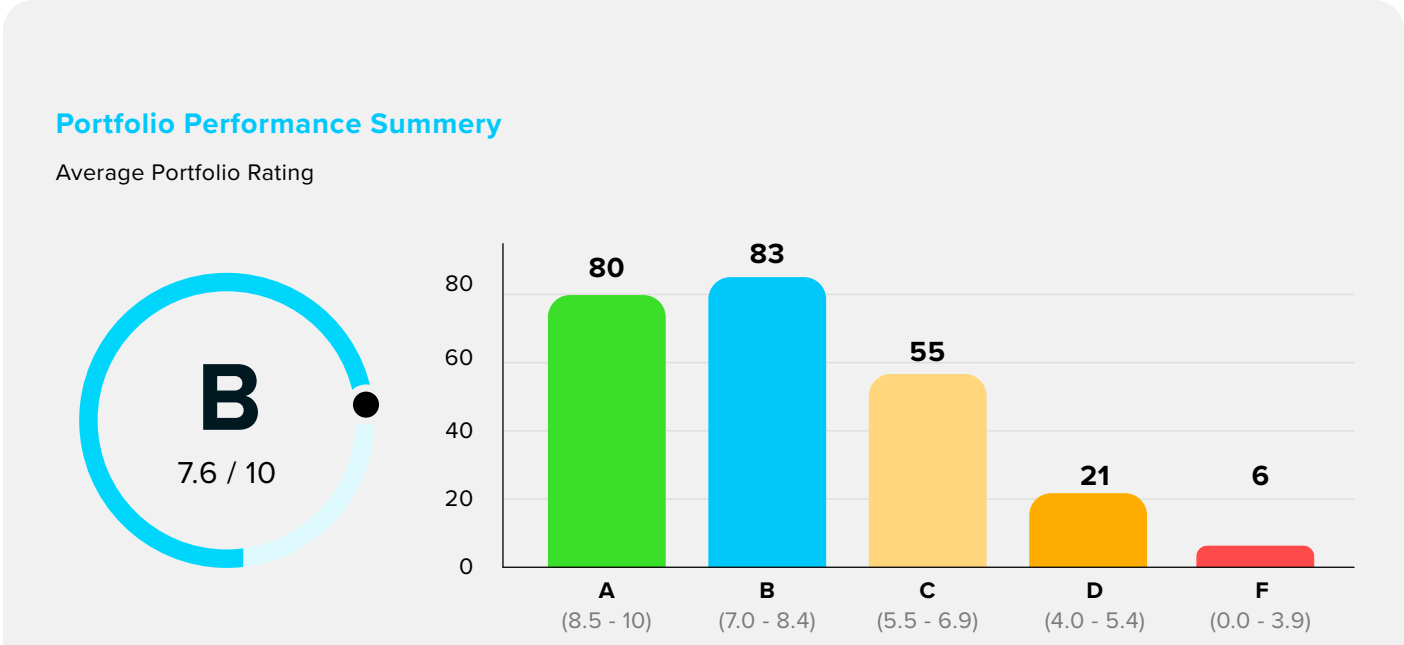
Bevindingen

Wat is de algemene cybersecuritystatus van maakbedrijven in Nederland?

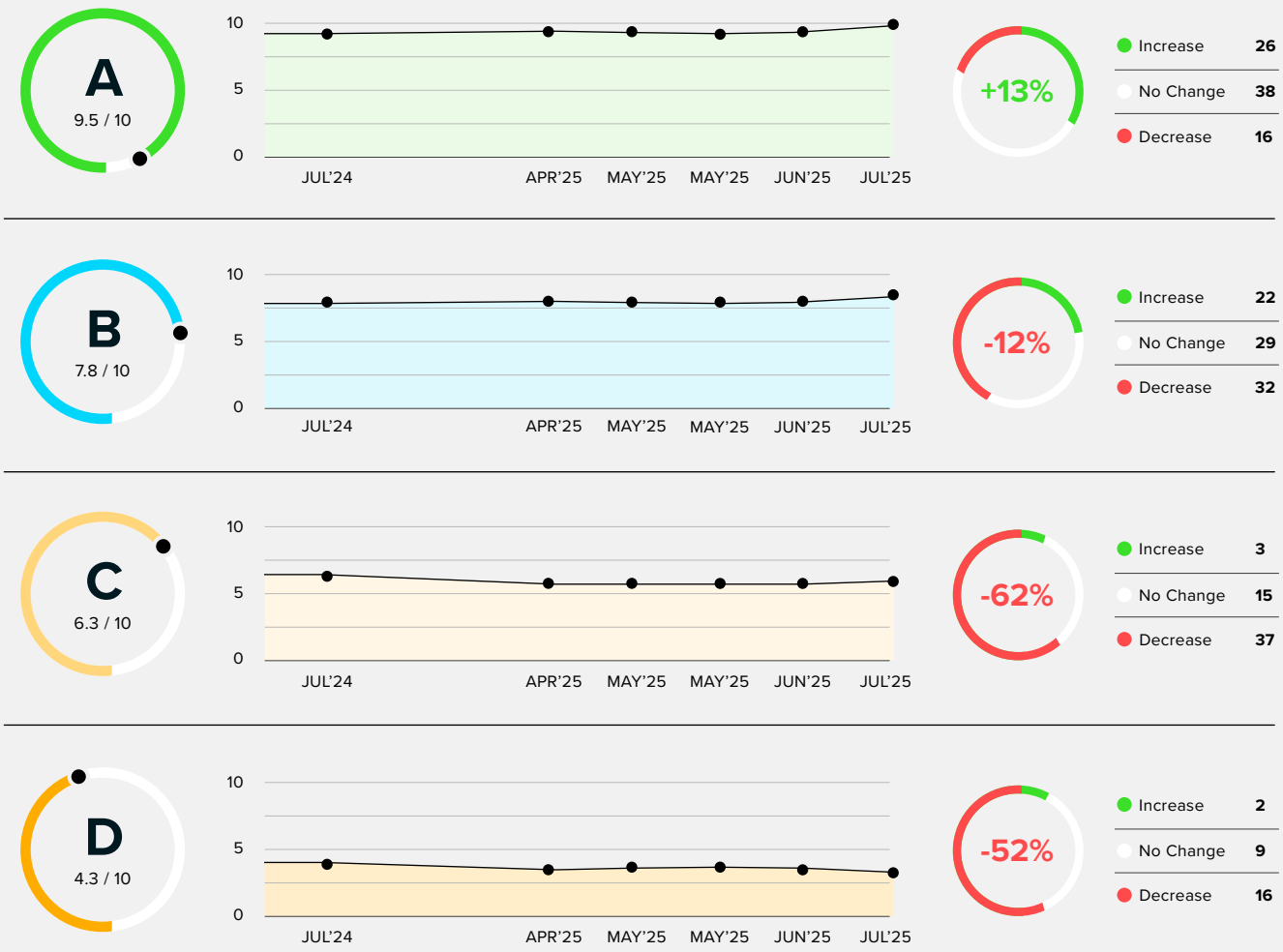
Onderstaand figuur laat zien hoe de 245 onderzochte organisaties gemiddeld presteren. In totaal 163 organisaties (68%) scoren hoger dan een 7 en vallen in categorie A of B. De tachtig bedrijven in categorie A hebben een gemiddelde rating van 9,5. Over een periode van 90 dagen zien we bij deze bedrijven een algehele verbetering van 13%. Bedrijven in categorie D, E en F zijn samengevoegd en scoren gemiddeld 4,3. Binnen deze categorie is een afname zichtbaar van 52% over een periode van 90 dagen.

Bedrijven met een hoge security rating blijven hun cybersecurity verbeteren.

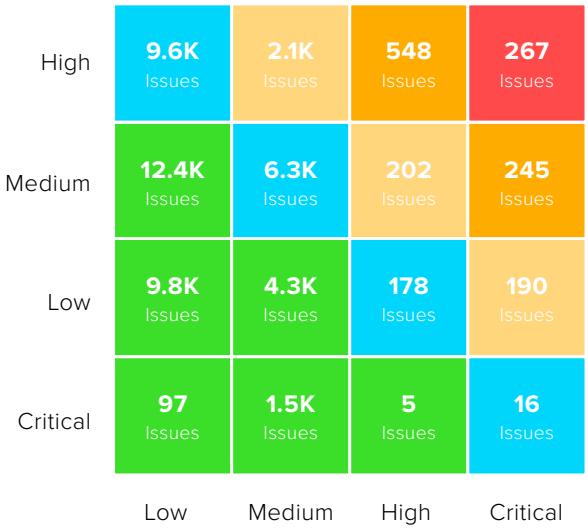
Bij maakbedrijven die lager scoren, zien we een sterke afname van de security rating. Dat komt omdat een hoge security rating ook iets zegt over de mate van security-volwassenheid. Volwassen cybersecurity is geborgd in een continu proces. Voor de bedrijven met een A-rating is statistisch aangetoond dat ze een 35,1x lager percentage ransomware-events hebben en 16,6x lager percentage datalekken dan bedrijven met een F-rating.



Portfolio Overall Rating



Asset Values



245 bedrijven met 267 kritische issues

Niet ieder probleem levert evenveel risico op. Sommige issues wegen zwaarder dan andere. Dit heeft alles te maken met de ernst van het probleem (Issue Severity) en de waarde van het systeem waarin het probleem zich voordoet (Asset Value). Issues met een hoge value en een critical severity, verdienen de meeste aandacht.

Security Domain Ratings

Binnen ons onderzoek, kijken we naar verschillende veiligheidsdomeinen zoals netwerkbeveiliging, applicatiebeveiliging, patchbeheer en encryptie. De Security Domain Ratings laten zien hoe een organisatie presteert op deze veiligheidsdomeinen.

Deze grafiek laat zien hoe de 245 onderzochte bedrijven scoren op de verschillende domeinen. Op de volgende pagina's gaan we dieper in op deze domeinen. We lichten toe wat de verschillende domeinen inhouden, wat er wordt beoordeeld en welke conclusies we daaruit kunnen trekken.

Security Domain Ratings

Dit betekenen de kleuren

- zeer hoog risiconiveau
- hoog risiconiveau
- gemiddeld risiconiveau
- laag risiconiveau
- zeer laag risiconiveau

Application Security

De Nederlandse maakindustrie scoort laag op Application Security

Het Application Security Domain richt zich op het beoordelen van de beveiliging van de applicaties die via het internet toegankelijk zijn. Meestal zijn dit webapplicaties.

Binnen de maakindustrie zijn webapplicaties niet alleen marketing- en klantportalen, maar ook steeds vaker toegangspoorten tot productieomgevingen, leveranciersportalen, configuratietools en IoT/OT-dashboards. Dit vergroot het belang van Application Security, omdat kwetsbaarheden direct kunnen doorwerken op de kern van de bedrijfsvoering.

We analyseren de publieke websites en webapplicaties van de 245 organisaties om te onderzoeken in welke mate kwetsbaarheden, configuratiefouten of verouderde software misbruikt kunnen worden door aanvallers.

Conclusies

Het onderzoek laat zien dat Application Security één van de laagst scorende securitydomeinen is voor de maakindustrie. Dit sluit aan bij internationale cijfers die laten zien dat webapplicatie-exploits sterk toenemen en vaak het startpunt vormen van ernstige incidenten.

Voor de maakindustrie betekent dit concreet:

Datalekken en IP-verlies zijn een reëel risico, juist omdat de sector afhankelijk is van hoogwaardige kennis en ontwerpen. Waar in andere sectoren persoonsgegevens centraal staan, draait het in de maakindustrie om intellectueel eigendom (ontwerpen, recepturen, productietekeningen). Een lek via een webapplicatie kan direct leiden tot concurrentievoordeel voor kwaadwillenden of chantage via ransomware.

Kwetsbaarheden in webapplicaties kunnen leiden tot verstoringen van productieprocessen, omdat aanvallers via deze route toegang krijgen tot interne systemen of zelfs OT-omgevingen. Veel maakbedrijven bieden klanten toegang tot portals voor orders, tekeningen of onderhoudsinformatie. Wanneer CMS-authenticatie niet met MFA is beschermd, kan een aanvaller eenvoudig toegang krijgen tot vertrouwelijke informatie of zelfs orderstromen manipuleren.

Supply chain-afhankelijkheden vergroten de impact: een kwetsbaarheid bij één partij kan snel doorwerken naar meerdere schakels in de keten. Maakbedrijven zijn sterk verweven met toeleveranciers en logistieke partners. Kwetsbaarheden in applicaties kunnen misbruikt worden om via de keten binnen te dringen, wat supply chain-aanvallen vergemakkelijkt.

Application Security vormt in de maakindustrie niet alleen een IT-vraagstuk, maar een direct bedrijfsrisico dat raakt aan continuïteit, concurrentiekracht en vertrouwen in de keten.

Web Encryption

Een fundamenteel knelpunt in de Nederlandse maakindustrie

Correct geconfigureerde webversleuteling is essentieel om ervoor te zorgen dat communicatie wordt beschermd tegen afluisteren en dat de authenticiteit van een systeem geverifieerd kan worden.

In het kader van ons onderzoek onderzochten we zes specifieke criteria die bepalen of de encryptie betrouwbaar en veilig is ingericht.

Een lage score op dit domein wijst op zwakke of foutieve encryptie, wat leidt tot risico's zoals gegevensdiefstal, identiteitsfraude en verlies van vertrouwen bij gebruikers. Correct ingestelde encryptie is een fundamenteel onderdeel van een veilige digitale infrastructuur.

Zwakte in web-encryptie correleert statistisch met ransomware incidenten, ondanks dat dit geen directe aanvalsvector is voor ransomware. Organisaties die basisbeveiliging op webniveau niet op orde hebben, blijken in veel gevallen ook intern een zwakkere security-hygiëne te hebben. Dit vergroot de kans dat ransomware zich eenvoudiger verspreidt in het IT-landschap en mogelijk zelfs in OT-omgevingen.

Conclusies

Web Encryptie is een fundamenteel knelpunt in de maakindustrie.
Slecht ingestelde certificaten en verouderde protocollen tasten het vertrouwen in digitale interacties met klanten, leveranciers en partners aan.

Encryptieproblemen zijn vaak een indicator voor bredere kwetsbaarheden binnen de organisatie.
Dit maakt het niet alleen een technisch vraagstuk, maar ook een signaal van onvoldoende security governance.

Voor de maakindustrie is correcte web-encryptie essentieel om concurrerend en betrouwbaar te blijven
binnen de sterk verweven supply chain. Het vormt een basislaag om ransomware, datalekken en reputatieschade te voorkomen.

Verlopen of foutief ingestelde certificaten leveren waarschuwingen in browsers en ondermijnen het vertrouwen
van klanten en partners in digitale portals. Voor maakbedrijven, die vaak werken met leveranciers- en klantenportalen, kan dit leiden tot verstoringen in bestellingen of serviceprocessen.

Gebruik van verouderde algoritmes en protocollen (zoals SHA-1 of TLS 1.0) komt nog voor.
Dit maakt communicatie kwetsbaar voor onderschepping en spoofing, wat gevolgen kan hebben bij overdracht van ontwerpbestanden, productiedata of inloggegevens.

DNS Security

DNS-beveiliging verdient aandacht

Het domein DNS Security beoordeelt het gebruik van controles om ongeoorloofde wijzigingen van domeinrecords te voorkomen die leiden tot domeinkaping.

Daarom controleren we of domeinen zijn beschermd tegen domeinkaping. Ook onderzoeken we hoeveel en welke DNS-providers een organisatie gebruikt voor haar domeinen.

Conclusies

Onvoldoende DNS-beveiliging vormt een risico voor de maakindustrie.
Als domeinen niet goed zijn beschermd, kunnen aanvallers deze kapen en klanten of leveranciers omleiden naar malafide sites. Dit leidt tot phishing, fraude, datadiefstal en verlies van vertrouwen in de keten.

Een fout in het DNS-beheer kan portals en systemen onbereikbaar maken, met directe impact op productie en leveringen. Omdat de sector sterk afhankelijk is van digitale communicatie en just-in-time processen, kan de schade groot zijn. Correct ingerichte DNS Security is daarom een eenvoudige maar essentiële maatregel om continuïteit en betrouwbaarheid te waarborgen.

Network Filtering

IoT-apparaten moeten volledig afgeschermd worden

Het domein Network Filtering analyseert de netwerken en systemen van een bedrijf op services die onveilig zijn of geen businessfunctie hebben.

We onderzoeken of systemen open netwerkpoorten hebben op services die als onveilig worden beschouwd. Ook onderzoeken we of Internet of Things (IoT)-apparaten via het internet bereikbaar zijn.

IoT-apparaten zijn ingebedde systemen die fysieke processen aansturen, zoals camera's, liften, HVAC-systemen of opslagsystemen. Deze apparaten zijn doorgaans niet ontworpen met sterke beveiliging en vormen een eenvoudig doelwit voor aanvallers. Het is zelden noodzakelijk of wenselijk dat IoT-apparaten publiek toegankelijk zijn. Daarom wordt aanbevolen om internettoegang voor IoT-apparaten zoveel mogelijk te beperken.

Conclusies

Onveilige netwerkservices en IoT-apparaten zijn een veelgebruikte aanvalsvector door cybercriminelen.
We zien vooral bij de bedrijven die met een C- en D/F-rating dat het aantal kwetsbaarheden toeneemt. Dit maakt die bedrijven kwetsbaar voor aanvallen die kunnen leiden tot datadiefstal, sabotage of het stilleggen van productieprocessen.

Het beperken van netwerktoegang tot alleen strikt noodzakelijke diensten, het volledig afschermen van IoT-apparaten, detectie van verdachte activiteiten, veilige (externe) toegang en identiteitsbeheer zijn belangrijke maatregelen om de digitale- en operationele continuïteit te waarborgen.

Software Patching

Een groot en vaak onderschat risico

Het domein Software Patching inventariseert systemen waarop verouderde en kwetsbare software draait.

Zodra verouderde software niet meer door de leverancier wordt ondersteund, kan deze niet worden gepatcht tegen bekende beveiligingsproblemen of nieuwe kwetsbaarheden die worden ontdekt. Daardoor neemt de kans op een hack, gijzeling of datalek toe.

In het kader van dit onderzoek kijken we naar Application Server Patching, OpenSSL Patching, CMS Patching en Web Server Patching.

Conclusies

Software Patching bepaalt de security rating voor 30%.
Het belang komt ook terug in de rapporten van Cyentia en Verizon. We zien dat het aantal issues vooral toeneemt bij de bedrijven die een D/F-score hebben.

Binnen de maakindustrie vormt verouderde software een groot en vaak onderschat risico.
Veel productiebedrijven maken gebruik van legacy-systemen, gespecialiseerde applicatieservers en embedded software die niet regelmatig worden bijgewerkt. Hierdoor ontstaan kwetsbaarheden die eenvoudig door

Aanvallers kunnen makkelijker toegang krijgen tot klantportalen, leverancierssystemen of productiedashboards
wanneer applicatie- en webservers of CMS-systemen niet tijdig worden gepatcht. Vooral de koppeling tussen IT- en OT-omgevingen maakt dit risicovol: een ogenschijnlijk klein lek in een webserver of OpenSSL-bibliotheek kan uiteindelijk leiden tot verstoring van productielijnen of zelfs volledige stilstand.

Reputatie speelt een belangrijke rol.
Klanten en ketenpartners verwachten dat bedrijven hun digitale omgeving up-to-date en veilig houden. Ongepatchte systemen verhogen niet alleen de kans op datalekken of ransomware, maar ondermijnen ook het vertrouwen in de hele supply chain.

Software patching is voor maakbedrijven een belangrijke graadmeter voor volwassenheid.
Bedrijven die onvoldoende investeren in patchmanagement lopen niet alleen achter op compliance-eisen (zoals NIS2), maar vergroten ook hun kans op disruptieve incidenten.

Voor de maakindustrie is structureel patchmanagement essentieel om productiestilstand, datalekken en ketenschade te voorkomen. Het vraagt om een strategische aanpak waarbij ook legacy- en OT-systemen worden meegenomen in lifecyclemanagement en security governance.

System Hosting

101 systemen in Rusland

Het domein System Hosting geeft inzicht in het aanvalsoppervlak van een organisatie op het internet. Het toont onder andere het aantal systemen en de gebruikte hostingproviders.

Binnen dit domein beoordelen we de mate van fragmentatie in systeemhosting en het gebruik van gedeelde IP-adressen (shared hosting). De manier waarop een organisatie haar internetaanwezigheid heeft ingericht, bepaalt in belangrijke mate de complexiteit van het beheer van IT-beveiliging, privacy en naleving van regelgeving.

De geografische locatie van assets is daarbij een belangrijk aandachtspunt. In het kader van geopolitieke spanningen en strengere Europese regelgeving, waaronder de NIS2-richtlijn, is het van groeiend belang dat bedrijven in de maakindustrie niet alleen hun directe IT-omgeving beveiligen, maar ook aandacht besteden aan de geografische locatie van hun digitale infrastructuur.

Conclusies

Zeven maakbedrijven hebben opgeteld 101 systemen in Rusland draaien.
Denk daarbij aan servers, domeinen of netwerkcomponenten die gekoppeld zijn aan Russische hostingproviders. Dat kunnen actieve componenten zijn die nog dagelijks gebruikt worden. Het kan ook gaan om verouderde websites, mailservers, API's of testomgevingen die onbedoeld in stand zijn gebleven.

Dit brengt aanzienlijke risico's met zich mee. Data of systemen die zich fysiek of netwerkmatig binnen de Russische grenzen bevinden, vallen onder de Russische wet. Dat betekent dat de Russische overheid toegang kan eisen tot die informatie. Daarnaast lopen bedrijven risico op operationele verstoring bij geopolitieke escalaties. Bovendien kunnen ze in conflict komen met de Europese sanctiewetgeving.

E-mail Security

Configuratie op orde, blijvende behoefte aan monitoring én gebruikersbewustzijn

Het domein E-mail Security analyseert de beveiligingsconfiguratie van e-maildiensten. E-mailservers moeten zodanig zijn ingesteld dat e-mailcommunicatie wordt versleuteld, zodat berichten beschermd zijn tegen ongeautoriseerde toegang.

Daarnaast moeten domeinen zo worden geconfigureerd dat de authenticiteit van verzonden e-mails kan worden bevestigd, om spoofing te voorkomen.

De afgelopen jaren zagen we een sterke verbetering op het gebied van e-mail security.

Conclusies

E-mail is nog altijd hét primaire communicatiekanaal
in de maakindustrie, zowel richting klanten als leveranciers. Hoewel de basismaatregelen (SPF, DKIM) de afgelopen jaren breed zijn ingevoerd en de sector hier gemiddeld steeds beter scoort, blijft e-mail de meest gebruikte aanvalsvector.

Vooral de afhankelijkheid van een uitgebreid leveranciersnetwerk maakt de sector kwetsbaar voor phishing en spoofing.
Een vervalst bericht dat lijkt te komen van een vaste leverancier of klant kan leiden tot financiële fraude, datadiefstal of het openen van kwaadaardige bijlagen die ransomware in het netwerk verspreiden. Ook kunnen aanvallers via e-mail proberen toegang te krijgen tot vertrouwelijke ontwerpbestanden of inloggegevens voor productie- en leverancierspportalen.

Hoewel de technische configuraties vaak redelijk op orde zijn, blijft gebruikersbewustzijn belangrijk.
Werknemers in productie-omgevingen zijn doorgaans minder getraind in het herkennen van phishing dan kantoormedewerkers, terwijl zij wel toegang hebben tot kritieke systemen.

Voor de maakindustrie is e-mailbeveiliging meer dan alleen techniek. Het vraagt om een combinatie van correcte configuraties, voortdurende monitoring én gebruikersbewustzijn. Alleen zo kan de sector zich beschermen tegen de financiële, operationele en reputatierisico's van e-mailaanvallen.

System Reputation

Een belangrijke indicator van betrouwbaarheid

Het domein System Reputation beoordeelt of systemen van een bedrijf betrokken zijn bij of gelinkt worden aan ongewenste activiteiten. Denk daarbij aan botnets, phishing, spam of communicatie met command-and-control servers.

Het platform dat we gebruiken baseert deze beoordeling op een breed scala aan threat intelligence. De aanwezigheid van IP-adressen uit een organisatie binnen deze dreigingsfeeds wijst vaak op onvoldoende of inconsistente beveiligingsmaatregelen.

Conclusies

System Reputation is een belangrijke indicator van de betrouwbaarheid van systemen op internet.
Omdat de sector sterk afhankelijk is van ketensamenwerking en just-in-time processen, is het essentieel dat systemen schoon en betrouwbaar opereren om productie en handelsrelaties niet in gevaar te brengen.

Een slechte 'system reputation' vormt een risico voor de maakindustrie, waar vertrouwen in digitale samenwerking cruciaal is.
Als systemen van een fabrikant in dreigingsfeeds opduiken, bijvoorbeeld door botnetcommunicatie, spam of phishing, wijst dit vaak op onvoldoende beveiliging of misbruik van infrastructuur. Dit kan leiden tot reputatieschade, blokkades van communicatie en verlies van vertrouwen bij klanten en leveranciers.

Veel bevindingen hebben te maken met gedeelde infrastructuur, gastennetwerken of spoofed verkeer.
Hoewel deze onderwerpen onder de verantwoordelijkheid van het bedrijf vallen, is het risico vaak klein.

Is de Nederlandse maakindustrie klaar voor NIS2 en de Cyberbeveiligingswet?

Naar alle waarschijnlijk treedt de Cyberbeveiligingswet in het tweede kwartaal van 2026 in werking. Met deze wet implementeert Nederland de Europese NIS2-richtlijn.

De wet is al een paar keer uitgesteld, maar de wettekst is klaar, de politieke druk neemt toe en de technische- en organisatorische voorbereidingen voor toezicht zijn gereed.

Veel van de bedrijven die we in ons onderzoek hebben meegenomen zijn NIS2-plichtig. Zeker is dat álle bedrijven met NIS2 te maken krijgen. Waar NIS1 zich richtte op een selecte groep bedrijven, kijkt NIS2 naar organisaties die betrokken zijn bij het produceren of leveren van goederen, diensten, software of systemen binnen de essentiële diensten of vitale sectoren. NIS2-plichtige bedrijven dienen niet alleen hun eigen systemen te beveiligen, maar ook om cyberrisico's in de toeleveringsketen te beheersen. **Dat betekent dat zij:**

- **Risicoanalyses moeten uitvoeren over hun IT-leveranciers, onderaannemers en partners.**
- **Moeten kunnen aantonen dat hun leveranciers voldoen aan minimale beveiligingsnormen.**
- **Mogelijk contractuele eisen stellen aan leveranciers of partners over securitymaatregelen, monitoring, incidentrespons en rapportage.**
- **Verantwoordelijk blijven voor de continuïteit en beveiliging van uitbestede processen.**

Dus zelfs als een bedrijf geen NIS2-verplichting heeft, kan een klant of partner die verplichting wel hebben en zijn partners verplichten om aan specifieke securityvereisten te voldoen. Met NIS2 wordt nog eens benadrukt dat digitale veiligheid een gezamenlijke verantwoordelijkheid is van ecosystemen en ketens.

In hoeverre zijn de 245 onderzochte organisaties voorbereid op NIS2?

Onze analyse op basis van publiek beschikbare data levert een objectieve security rating op. Deze analyse geeft een indicatie van de cybersecurity volwassenheid en zegt daarmee ook iets over de mate waarin deze bedrijven aan de NIS2-eisen voldoen.

Het onderzoek laat zien dat de meeste onderzochte bedrijven weliswaar niet vanaf nul beginnen, maar nog wel het nodige werk te doen hebben om in de lente van 2026 te voldoen aan de Cyberbeveiligingswet.

Op weg naar volwassen cybersecurity

8x

adviezen voor organisaties die veiliger willen ondernemen

01

Advies 1
Benader cybersecurity als een strategisch risico

Bedrijven met een hoge cybersecurity-volwassenheid benaderen datalekken, gijzelsoftware en andere cyberincidenten als een strategisch risico. Waar veel organisaties nog werken met losse, ad-hoc investeringen vanuit de IT-afdeling, hebben de voorlopers cybersecurity daarom verankerd in hun governance-structuur. Wanneer de directie expliciet eigenaarschap neemt over security en een formele security of risicomanager benoemt, ontstaat er richting en draagvlak. Een vastgesteld informatiebeveiligingsbeleid, waarin zowel IT- als OT-processen zijn meegenomen, biedt houvast voor prioritering en investeringen. Dit beleid wordt versterkt door een goed begrip van de kritische assets: de systemen, processen en data die het hart vormen van de productie en de bedrijfscontinuïteit.

De maakindustrie digitaliseert in hoog tempo. Slimme fabrieken, verbonden machines en datagedreven productieprocessen vormen het hart van moderne concurrentiekracht.

Maar deze digitale transformatie heeft ook een keerzijde: een structurele toename van cyberdreigingen. Ransomware, supply chain-aanvallen, spionage en sabotage van OT-systemen zijn geen hypothetische risico's meer, maar dagelijkse realiteit.

Uit onze analyse blijkt dat het gemiddelde cybersecurity-volwassenheidsniveau in de maakindustrie lager ligt dan in andere sectoren. Dit maakt de sector een aantrekkelijk doelwit voor cybercriminelen.

Groeien in security-volwassenheid vraagt daarom om een gestructureerde aanpak, waarbij zowel strategische keuzes als dagelijkse operationele discipline samenkomen.

Door de volgende negen adviezen op te volgen, bouwen maakbedrijven aan een robuuste, toekomstbestendige beveiliging. Niet alleen om te voldoen aan wet- en regelgeving, maar vooral om te zorgen dat de fabriek blijft produceren, ongeacht de digitale dreigingen die op hen afkomen.

02

Advies 2
Zorg voor inzicht in je assets en verminder de risico's

Zonder een volledig en actueel overzicht van alle assets – inclusief PLC's, robots, IoT-apparaten en leveranciersapparatuur – is effectief beveiligen onmogelijk. Kwetsbaarheden moeten niet alleen technisch worden opgespoord, maar ook worden geprioriteerd en gepatcht op basis van het werkelijke bedrijfsrisico. Standaardconfiguraties, het beperken van onnodige diensten en het gebruik van golden images verkleinen de kans op succesvolle aanvallen. Back-ups spelen hierin een sleutelrol: ze moeten offline, getest en snel herstelbaar zijn, ook voor OT-configuraties en productielogica.

Advies 3
Zorg voor Security by Design

Bij het ontwerp en de implementatie van nieuwe systemen en productieprocessen wordt beveiliging direct meegenomen. Minimale toegangsrechten, versleuteling, hardening en logging zijn niet optioneel, maar standaard ingeschakeld. Hierdoor worden potentiële zwakheden al vóór ingebruikname verminderd, wat de kans op incidenten aanzienlijk verkleint.

04

Advies 4
Deel het netwerk op in zones

Maakbedrijven kennen vaak een complexe mix van IT- en OT-netwerken. Zonder netwerksegmentatie kan een hacker die binnenkomt via het kantoornetwerk eenvoudiger doordringen tot systemen die machines in de fabriekshal aansturen. Door het netwerk op te delen in zones en strikte toegangsregels in te stellen, worden dit soort laterale beweging van aanvallers bemoeilijkt. Toegang tot OT-systemen verloopt bij voorkeur via jumpservers met multifactor-authenticatie. Externe leveranciers krijgen alleen tijdelijk toegang tot de systemen die zij echt nodig hebben.

cegeka

05

Advies 5
Deel het netwerk op in zones

Het beveiligen van het productieproces vraagt om een zorgvuldige balans tussen preventie, detectie, respons en herstel.

Ook OT-specifieke maatregelen verdienen aandacht. Het versleuteld opslaan en regelmatig controleren van back-ups van PLC-programma's en robotconfiguraties, het fysiek beveiligen van kasten en het beperken van USB-toegang zijn maatregelen die het verschil kunnen maken.

Detectie wordt versterkt door het centraal verzamelen en analyseren van logs, aangevuld met threat intelligence en OT-specifieke detectieregels. Wanneer er toch een incident plaatsvindt, maakt een goed getest incidentresponsplan het verschil. In zo'n plan staan ook OT-scenario's uitgewerkt, bijvoorbeeld het isoleren van een besmette productielijn of het veiligstellen van de productierecepturen. Menselijk gedrag blijft uiteraard een kritieke factor. Operators, engineers en kantoormedewerkers hebben elk hun eigen rol in de beveiliging. Rolgerichte trainingen, praktijkgerichte simulaties en interne security champions zorgen dat alertheid geen eenmalige actie is, maar een vaste gewoonte.

06

Advies 6
Veiligheid stopt niet bij de muren van het maakbedrijf

Ketenbewustzijn en leveranciersbeheer maken het verschil in de maakindustrie. In een sector waar productielijnen sterk afhankelijk zijn van externe partners, monitoren de meest volwassen organisaties actief de beveiligingsstatus van hun leveranciers.

Het uitvragen van minimale beveiligingseisen bij leveranciers, het opnemen van incidentmeldplichten in contracten en het differentiëren van eisen per type leverancier versterken de weerbaarheid van de hele keten. Dit sluit aan bij de NIS2-richtlijn, die niet alleen direct plichtige bedrijven treft, maar ook eisen stelt aan hun toeleveranciers. Bedrijven die nu al werken volgens NIS2-principes zijn straks beter voorbereid op audits, boetes en imagoschade.

07

Advies 7
Maak cybersecurity meetbaar

Security-volwassenheid moet meetbaar zijn. KPI's zoals de dekking van MFA, het percentage gepatchte kritieke systemen binnen afgesproken termijnen, de gemiddelde detectie- en responstijd en de herstelsnelheid bij incidenten maken voortgang zichtbaar. Zo wordt duidelijk waar nog gaten zitten en waar investeringen het meeste effect hebben.

08

Advies 8
Zorg voor een realistische roadmap

Volwassenwording vraagt om een realistische roadmap. In de eerste maanden ligt de focus op stabiliseren: inventariseren, MFA activeren, back-ups veiligstellen en basisdetectie inrichten. Daarna volgt segmentatie, het invoeren van striktere toegangscontroles en het automatiseren van monitoring. In de laatste fase worden processen geborgd met playbooks, leveranciersmanagement en periodieke audits, zodat beveiliging niet afhankelijk is van losse projecten, maar onderdeel wordt van de bedrijfsvoering.

Dit onderzoek is mede mogelijk gemaakt door RiskRecon.

CYBER RESILIENCE IN DE MAAKINDUSTRIE

Zet de volgende stap naar volwassen cybersecurity

Wil je stappen zetten op het gebied van jouw cybersecurity volwassenheid? Ben je benieuwd hoe jouw organisatie scoort op het gebied van cybersecurity? Dan helpt Cegeka jou daar graag bij.

Plan vandaag nog een scan in van jouw organisatie en kijk door de bril van een hacker naar jouw kwetsbaarheden en die van jouw leveranciers.

Remco Geerts
Business Unit Manager Cyber Security & Networking
Remco.Geerts@cegeka.com

Neem contact op

Jac-Rice van Brunschot
Industry Director Manufacturing
Jac-Rice.vanBrunschot@cegeka.com

Neem contact op

cegeka

WWW.CEGEKA.COM