POLAR RISK

Rapportage Cyber Risk Assessment

ACME B.V.

Inleiding

Fictief rapport

ACME B.V.
t.a.v. Jan Peeters
Prinsengracht 20
1015 DV Amsterdam

10 maart 2026

Referentie: NL123456789

Geachte Jan Peeters,

Voor u ligt het Cyber Risk Assessment dat is uitgevoerd in de periode van [datum] tot [datum]. Het doel van dit assessment was het identificeren en kwantificeren van de meest relevante cyberrisico's voor ACME B.V.

Dit stelt ACME in staat om onderbouwde beslissingen te nemen over cybersecurityinvesteringen, risicoafweging en passende mitigerende maatregelen, om cyberrisico's effectief te beheersen.

De resultaten in dit rapport zijn gebaseerd op input uit interviews met verschillende stakeholders, waaronder de IT Manager, CISO, HR-manager en Hoofd Finance. Op basis van deze input zijn de relevante scenario's, dreigingen en potentiële impacts geïnventariseerd, beoordeeld en besproken.

De uitkomsten van dit assessment zijn op [datum] besproken met de CISO. Tijdens deze bespreking zijn de belangrijkste bevindingen, aannames en resultaten van de analyse doorgenomen.

Dit rapport bevat een overzicht van de geïdentificeerde risico's en de resultaten van de uitgevoerde analyse.

Mocht u naar aanleiding van dit rapport vragen hebben of behoefte hebben aan een nadere toelichting, dan kunt u vanzelfsprekend contact opnemen.

Met vriendelijke groet,
Polar Risk B.V.

Paul Permentier

Paul Permentier
Co-founder

Fictief rapport

Onze samenvatting

Staat van Cybersecurity

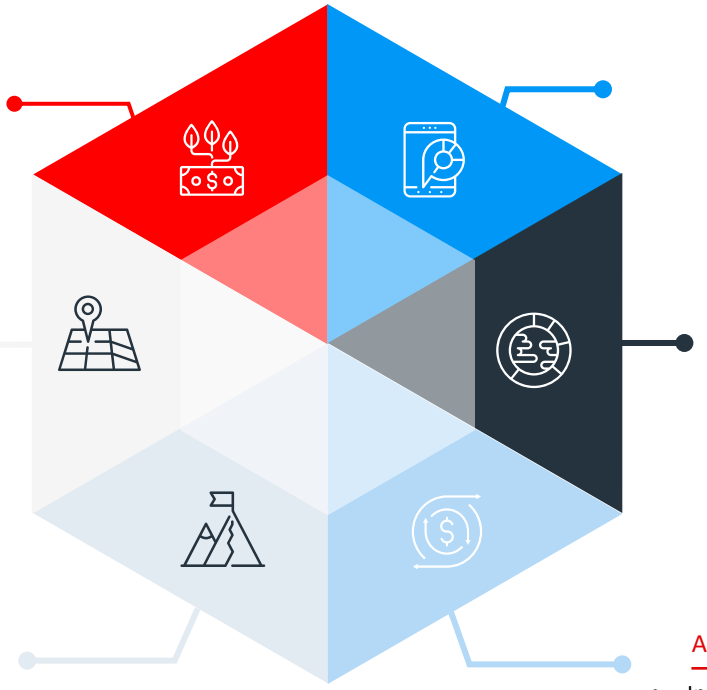
- ACME heeft een solide basis voor informatiebeveiliging, passend bij haar positie in de maakindustrie
- Volwassen basis met ingericht beleid, processen en technische maatregelen
- Informatiebeveiliging nog niet overal consistent geïmplementeerd
- Onvoldoende zicht op de afhankelijkheden binnen de supply chain

Belangrijkste cyberrisico's

- Drie relevante risicoscenario's gekwantificeerd (ransomware, diefstal IE, cloudverstoring)
- Ransomware en cloudverstoring zijn geïdentificeerd als hoogste impactscenario
- Ransomware heeft XXX als meest waarschijnlijke impact
- Cloudverstoring heeft XX als meest waarschijnlijke impact

Belangrijkste bevindingen

- Beperkte detectiecapaciteit vergroot zowel de kans op incidenten als de impact door vertraagde signalering en respons
- De beheersing van toegangsrechten op kritieke systemen en data kan worden verbeterd, wat het risico op misbruik en ongeautoriseerde toegang verhoogt
- Sterke afhankelijkheid van leveranciers en ketenpartners zonder volledig inzicht in risico's vergroot de kans op verstoringen in productie en levering



Risicobereidheid

- Risico op ransomware en verstoring van IT-cloudleverancier valt buiten de risicobereidheid en verreist opvolging
- Diefstal van intellectueel eigendom valt binnen de risicobereidheid

Advies: Direct aandacht

- Aanscherpen van toegangsrechten (least privilege) op kritieke systemen en ontwerpdata
- Periodiek reviewen en opschonen van accounts en autorisaties, met focus op high-risk users
- In kaart brengen van kritieke leveranciers en basismaatregelen afspreken

Advies: Lange termijn

- Inrichten van een detectie- en responsefunctie voor het detecteren van afwijkingen in het IT-landschap
- Structureel verbeteren van identity & access management, inclusief governance, processen en tooling
- Opzetten van een third-party risk management proces voor leveranciers en ketenafhankelijkheden
- Doorvoeren van netwerksegmentatie en versterken van recovery capabilities

Organisatieprofiel

Fictief rapport

Omzet

ACME is een metaalverwerker gevestigd in Amsterdam met een jaaromzet van 55.000.000 EUR. ACME heeft 250 medewerkers in dienst, waarbij het overgrote deel op locatie werkt. Een handjevol accountmanagers werken op afstand in de lokale afzetmarkten van ACME. Al deze afzetmarkten bevinden zich binnen de European Economic Area (EEA).

Het overgrote deel van de omzet (65%) maakt ACME met het op specificatie maken van complexe staalproducten voor de Nederlandse afzetmarkt. Hiermee vormt ACME een vitale schakel in de supply chain van hun afnemers. Nog eens 30% van de omzet wordt op dezelfde manier gemaakt, maar dan voor de Europese afzetmarkt. Een laatste 5% van de omzet komt uit diverse activiteiten waar ACME specifiek voor gevraagd wordt, zoals het meedenken aan het ontwerpen van staalproducten bij klanten zonder over te gaan tot productie ervan.

Doelstellingen

Door het hoog specialistische werk van ACME is de concurrentie klein. In Nederland zijn er 2 à 3 concurrenten en op Europees niveau maximaal 50. De onderlinge verhoudingen tussen ACME en hun concurrenten varieert van neutraal op Europees niveau en goed op Nederlands niveau. ACME heeft als strategische doelstelling om de komende vijf jaar de omzet met 10% te laten groeien en beoogt dit op twee manieren te realiseren:

1. Het verhogen van het aantal orders voor ultra-complexe staalproducten. Deze producten hebben een hogere winstmarge.
2. Het uitbreiden van de klantenkring in de BeNeLux, om zo tot meer ordervolume te komen.

Cyberdreigingen industrie

De maakindustrie is een gewild doelwit voor cybercriminelen, omdat bedrijfsstilstand als gevolg van een cyberaanval bijna altijd leidt tot een verlies van omzet. Organisaties in deze industrie zijn hiermee gevoelig voor de druk die cybercriminelen uitoefenen door de inzet van ransomware of DDoS-aanvallen. Het Norsk-Hydro ransomware-incident uit 2021 is hier een goed voorbeeld van.

In deze industrie worden op verzoek van eindklanten specialistische staalproducten vervaardigd. Variërend van eenvoudige, maar speciaal ontwikkelde schroeven tot aan complexe elementen voor de machines van ASML en diens toeleveranciers. Hiermee is de industrie in het vizier van kwaadwillende die interesse hebben in de specificaties, blauwdrukken of andere details van de producten die op verzoek van klanten vervaardigd worden. De industrie is vanuit hun positie in de supply chain van hun afnemers een mogelijk doelwit voor gerichte aanvallen door staatsgesponsorde aanvallers.

Deze aanvallers kenmerken zich door hun volhardendheid en de grote hoeveelheid middelen die zij tot hun beschikking hebben. Vrijwel alle grote mogendheden maken zich hier schuldig aan. Een aantal mogendheden staan hier expliciet om bekend: China, Iran, Noord Korea, Rusland en de Verenigde Staten.

Op een positieve noot kenmerkt de industrie zich ook door de grote hoeveelheid familiebedrijven en bedrijven met een hechte club werknemers. Bedrijfsonderbrekingen, datalekken of datadiefstal opzettelijk veroorzaakt door een medewerker komen onder gemiddeld voor deze industrie.

Fictief rapport

IT-omgeving

Overzicht van het IT-landschap

Het IT-landschap van ACME kenmerkt zich door een hybride inrichting waarin traditionele on-premise systemen worden gecombineerd met moderne cloudoplossingen. De kern van de bedrijfsvoering wordt ondersteund door het ERP-systeem SAP S/4HANA, dat verantwoordelijk is voor productieplanning, orderverwerking en logistiek. Voor kantoorautomatisering maakt ACME gebruik van Microsoft 365, terwijl identity- en toegangsbeheer wordt gefaciliteerd via Microsoft Entra ID in combinatie met een on-premise Active Directory. Binnen de productieomgeving spelen OT-systemen zoals Siemens WinCC en Siemens S7 een cruciale rol in de aansturing van fysieke processen.

IT/OT-integratie en segmentatie

Een belangrijk kenmerk van het landschap is de toenemende integratie tussen IT en OT. Deze koppeling maakt efficiënte productie en realtime monitoring mogelijk, maar introduceert tegelijkertijd extra risico's. Segmentatie tussen netwerken is aanwezig, maar niet strikt doorgevoerd, waardoor laterale beweging van aanvallers van IT naar OT aannemelijk is. Daarnaast is de detectiecapaciteit binnen de OT-omgeving beperkt in vergelijking met de IT-omgeving, wat de kans vergroot dat incidenten onopgemerkt blijven en escaleren.

Externe toegang en leveranciers

Externe toegang vormt een aanvullend aandachtspunt. Leveranciers hebben in sommige gevallen remote toegang tot systemen, bijvoorbeeld voor onderhoud, waarbij autorisaties niet altijd consistent of sterk zijn ingericht. Dit verhoogt zowel de kans op ongeautoriseerde toegang als de complexiteit van het dreigingslandschap.

Data en impact op de bedrijfsvoering

De data binnen ACME bestaat voornamelijk uit productiegegevens, klantinformatie en intellectueel eigendom zoals technische ontwerpen. De grootste potentiële impact ligt echter niet primair bij datalekken, maar bij verstoring van productieprocessen. Stilstand van productie-installaties heeft directe financiële consequenties en kan leiden tot contractuele boetes en reputatieschade.

Toekomstige ontwikkelingen

Vooruitkijkend zijn er plannen om delen van het IT-landschap verder te moderniseren, waaronder gedeeltelijke cloudmigratie en uitbreiding van digitale integratie in de productieomgeving. Hoewel deze ontwikkelingen kansen bieden voor efficiëntie en schaalbaarheid, vergroten zij tegelijkertijd het aanvalsoppervlak.

Fictief rapport

Aanpak

Het Cyber Risk Assessment is uitgevoerd op basis van een gestructureerde en risicogedreven methodiek, gebaseerd op FAIR en in lijn met gangbare standaarden zoals NIST, ISO 27001 en ISO 27005. Hierbij zijn relevante risicoscenario's geïdentificeerd en gekwantificeerd. De analyse is gebaseerd op input uit interviews met stakeholders, aangevuld met interne documentatie en externe dreigingsinformatie. De belangrijkste risico's zijn vertaald naar concrete cyberrisicoscenario's.

Intake

Het assessment is gestart met een intake waarin de context, doelstelling en scope zijn vastgesteld. Hierbij is gekeken naar de specifieke behoefte van ACME, zijn de relevante stakeholders betrokken en is een globaal tijdspad bepaald. Daarnaast is inzicht verkregen in de bedrijfsactiviteiten en de ondersteunende rol van IT binnen de organisatie.

Onderzoek

In de onderzoeksfase zijn de kritieke bedrijfsprocessen geïdentificeerd en gekoppeld aan de IT-systemen die deze processen ondersteunen. Hierdoor is inzicht verkregen in welke systemen essentieel zijn voor de continuïteit van de organisatie.

Vervolgens zijn realistische cyberrisicoscenario's opgesteld op basis van essentiële dienstverlening, kritieke IT-systemen, relevante dreigingen, bestaande beheersmaatregelen en inzichten uit sector- en marktdata. Deze scenario's vormen concrete uitwerkingen van cyberrisico's en maken inzichtelijk op welke wijze cyberincidenten impact kunnen hebben, zoals bij uitval van systemen of compromittering van gevoelige informatie.

Kwantificatie

Per scenario zijn de dreiging, kwetsbaarheden, betrokken assets en potentiële effecten in kaart gebracht. Vervolgens zijn de waarschijnlijkheid en financiële impact bepaald. De impact is beoordeeld op basis van effecten op Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) en vertaald naar financiële schade.

Hierbij is onderscheid gemaakt tussen primaire verliezen (zoals omzetverlies, productieverlies en herstelkosten) en secundaire verliezen (zoals reputatieschade, boetes en aansprakelijkheid). Waar mogelijk is gebruikgemaakt van organisatiegegevens en externe marktdata van internationaal erkende onderzoeksinstituten.

De resultaten zijn vertaald naar een jaarlijkse verwachte schade (Annualized Loss Expectancy, ALE), waarmee risico's onderling vergelijkbaar zijn gemaakt.

Oplevering

De uitkomsten van het assessment zijn afgestemd met de stakeholders, waarbij onderbouwing en data expliciet zijn besproken. Dit rapport bevat de belangrijkste cyberrisicoscenario's, inzicht in kans en impact per scenario en concrete adviezen voor risicoreductie.

01 Intake

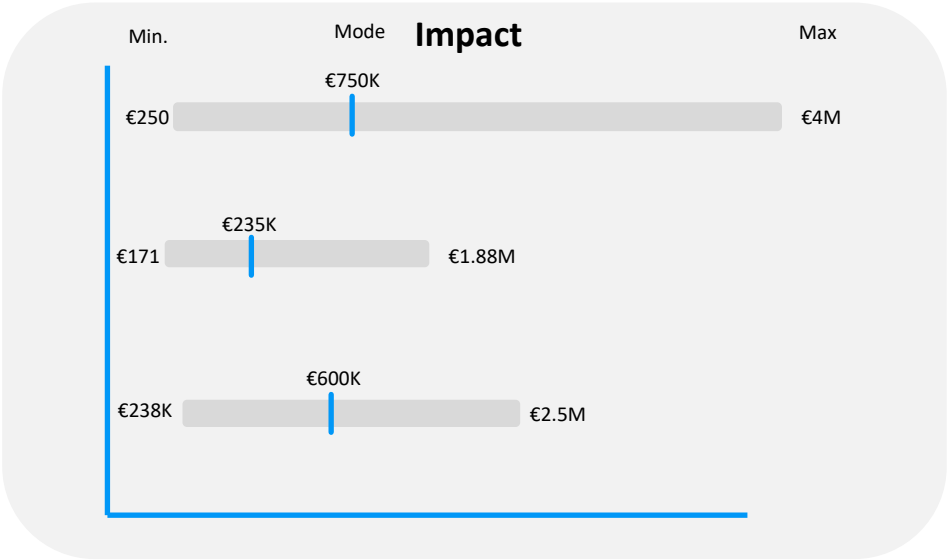
02 Onderzoek

03 Kwantificatie

04 Oplevering

Overzicht scenario's

Fictief rapport



Toelichting
De grafiek links toont drie risicoscenario's, waarbij per scenario de bandbreedte van de impact is weergegeven. Hierbij zijn de minimale impact, de maximale impact en de meest waarschijnlijke waarde opgenomen.

Hieruit is op te maken dat de scenario's ransomware en verstoring IT-cloudleveranicer de hoogste impact vertegenwoordigen.

Scenario	Kans	Impact	ALE
Ransomware	10% - 30%	€500K - €1M	**€113K**
Diefstal IE	5%-15%	€100K - €300K	**€24K**
IT-storing cloudleveranicer	10%-15%	€400K €800K	**€72K**

Toelichting
De tabel links toont drie risicoscenario's, waarbij per scenario de kans dat een verliesgebeurtenis optreedt, de financiële impact en de Annualized Loss Expectancy (ALE) zijn weergegeven. De ALE komt tot stand door de waarschijnlijkheid dat een gebeurtenis in 1 jaar plaatsvindt en impact op jaarbasis met elkaar te vermenigvuldigen. De ALE maakt het mogelijk om risico's onderling te vergelijken.

Ransomeware en verstoring van bij een IT-cloudleverancier vertegenwoordigen de hoogte jaarlijkse impact

Fictief rapport

Scenario ransomware

Scenario

Cybercriminelen verkrijgen toegang tot de IT-omgeving van ACME, bijvoorbeeld via zwakke toegangsrechten of een leverancier, en verspreiden ransomware. Hierdoor wordt het voorraadsysteem versleuteld en onbeschikbaar, wat leidt tot verstoringen in productie, en leveringen.

Asset	Dreiging	Effect
SAP Voorraadsysteem	Criminelen	Verlies van Beschikbaarheid

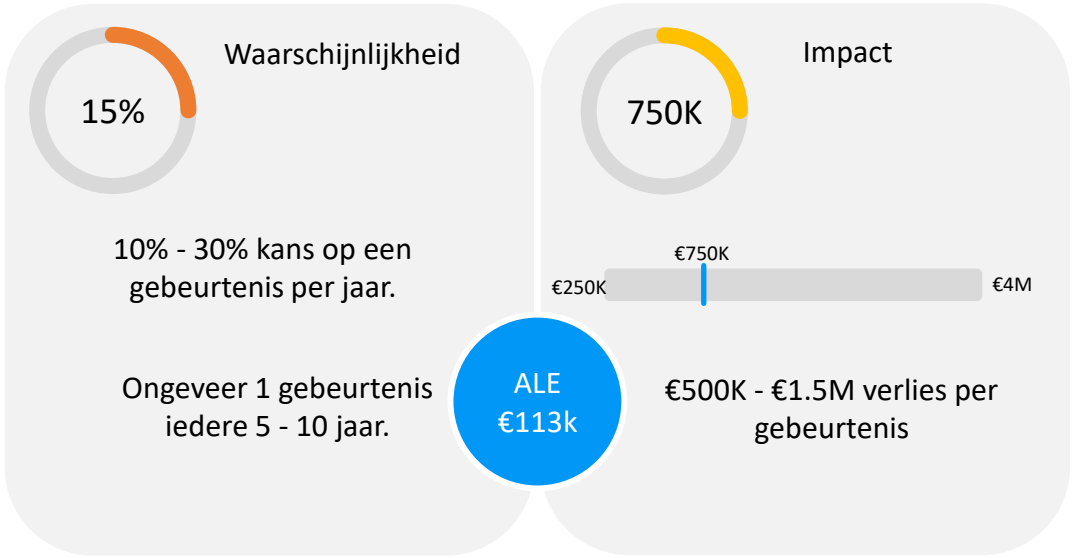
Belangrijkste motivaties voor risicoscenario

Detectie en Reponse capaciteit
Hoewel basismaatregelen aanwezig zijn, is detectie en respons niet volledig geoptimaliseerd, waardoor aanvallers zich mogelijk lateraal kunnen verplaatsen voordat ze worden gestopt.

Herstelvermogen
Back-ups zijn aanwezig, maar herstelprocedures zijn beperkt getest, wat leidt tot langere hersteltijden en hogere kosten zoals forensics.

Waarschijnlijke aanvalsvectoren
Phishing en kwetsbaarheden in externe toegang (zoals Citrix) worden gezien als de meest realistische entry points, gebaseerd op incidentdata binnen vergelijkbare organisaties

Impact op bedrijfsvoering
De organisatie is sterk afhankelijk van IT-systemen, waardoor uitval direct leidt tot verstoring van kritieke processen en productiviteitsverlies over meerdere dagen.



Fictief rapport

Scenario diefstal intellectueel eigendom (IP)

Risico Scenario

Cybercriminelen verkrijgen toegang tot de IT-omgeving van ACME, bijvoorbeeld via zwakke toegangsrechten, en stelen ontwerpdata of productspecificaties uit kritieke systemen. Hierdoor gaat intellectueel eigendom verloren, wat kan leiden tot concurrentienadeel, reputatieschade en omzetverlies.

Asset	Dreiging	Effect
Ontwerpdata / productspecificatie	Criminelen	Verlies van vertrouwelijkheid

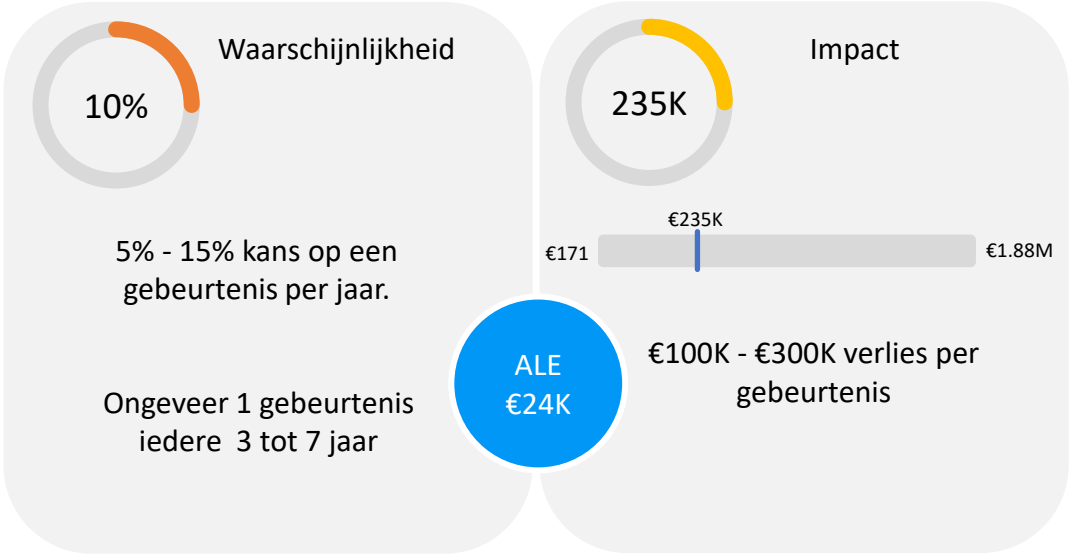
Belangrijkste motivaties voor risicoscenario

Logging en monitoring
Hoewel logging en monitoring deels zijn ingericht, ontbreekt specifieke detectie op datalekken en ongebruikelijke datastromen, waardoor exfiltratie van intellectueel eigendom via legitieme accounts of cloud langere tijd onopgemerkt kan blijven.

Reputatieschade
Zodra intellectueel eigendom is gestolen, is herstel niet mogelijk en is de organisatie afhankelijk is van juridische en reputatieherstelmaatregelen die vaak kostbaar en tijdrovend zijn.

Beveiliging van accounts
Spear phishing, misbruik van gecompromitteerde accounts en onvoldoende beveiligde samenwerkingsplatformen vormen de meest waarschijnlijke aanvalsroutes, aangevuld met risico's vanuit insiders en externe partijen met toegang.

Concurrentievoordeel
Diefstal van intellectueel eigendom leidt tot verlies van concurrentievoordeel en omzet, met langdurige negatieve effecten op marktpositie en bedrijfswaarde.



Scenario IT-storing cloudleverancier

Fictief rapport

Risico Scenario

Een cloud dienstverlener valt uit door een storing of incident, waardoor kritieke systemen en data van ACME tijdelijk niet beschikbaar zijn. Dit leidt tot verstoringen in bedrijfsprocessen, productie en leveringen, met directe impact op omzet en klanttevredenheid.

Asset	Dreiging	Effect
Kritieke dienstverlening	Leverancier	Verlies van Beschikbaarheid

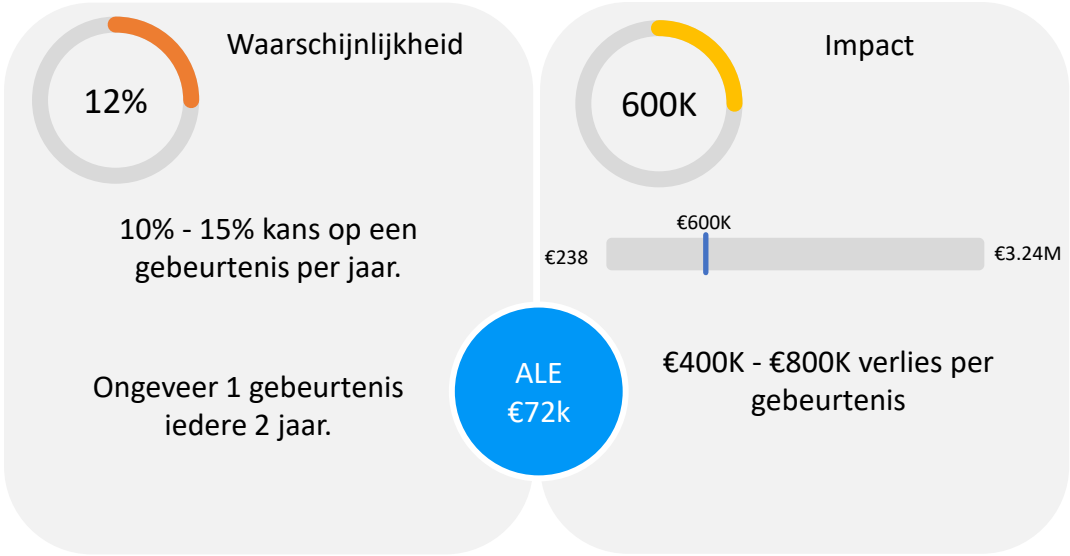
Belangrijkste motivaties voor risicoscenario

Leveranciers Management
Hoewel monitoring deels is ingericht, ontbreekt volledig inzicht in de beschikbaarheid en prestaties van externe IT-dienstverleners, waardoor verstoringen in de keten niet tijdig worden gesignaleerd en afhankelijkheden onvoldoende beheerst zijn.

Continuïteitsplannen
Bij uitval is de organisatie sterk afhankelijk van de leverancier voor herstel, terwijl uitwijkmogelijkheden en fallback-scenario's beperkt zijn en continuïteitsplannen niet altijd integraal met leveranciers zijn getest.

Waarschijnlijke oorzaken
Technische storingen, cyberincidenten en afhankelijkheden van onderliggende cloud- of netwerkproviders vormen de meest realistische oorzaken van uitval, gebaseerd op incidenten bij vergelijkbare organisaties.

Impact op bedrijfsvoering
Uitval van een IT-dienstleverancier leidt tot verstoring van produtieprocessen en productiviteitsverlies, met financiële gevolgen bij langdurige onbeschikbaarheid.



Fictief rapport

Bevindingen

Algemene volwassenheid

ACME beschikt over een solide basis aan beveiligingsmaatregelen, met ingericht beleid, processen en technische controles die passend zijn voor een organisatie binnen de maakindustrie. Er is betrokkenheid vanuit zowel IT als de business en er is aandacht voor risicomanagement en compliance, met name in relatie tot de rol van ACME als schakel in de supply chain. Variatie in implementatie en borging tussen onderdelen zorgt er echter voor dat risico's niet overal consistent worden beheerst, wat de waarschijnlijkheid van verstoringen in productie of dienstverlening verhoog.

Logging en monitoring

Logging en monitoring zijn ingericht voor kritieke systemen binnen de IT- en productieomgeving, maar de dekking en diepgang zijn nog niet volledig. Met name op het gebied van datastromen, cloudomgevingen en gebruikersgedrag bestaat het risico dat afwijkingen of ongeautoriseerde toegang tot ontwerpgegevens en productspecificaties niet tijdig worden gesignaleerd. Dit vergroot de kans dat incidenten, zoals ransomware of datadiefstal, langer onopgemerkt blijven en zich uitbreiden, waardoor de uiteindelijke impact op productiecontinuïteit en klantleveringen toeneemt.

Toegangsbeheer

Toegangsbeheer is grotendeels ingericht op basis van rollen, passend bij de verschillende functies binnen ACME. In de praktijk komen echter brede autorisaties en beperkt inzicht in het gebruik van rechten voor. Hierdoor neemt de kans op misbruik van accounts toe, met name bij accountcompromittering of interne dreigingen. Daarnaast kan dit leiden tot een grotere impact, doordat gebruikers toegang hebben tot meer systemen, productiedata en ontwerpdocumentatie dan strikt noodzakelijk, wat risico's oplevert voor zowel continuïteit als vertrouwelijkheid.

Ketenafhankelijkheden

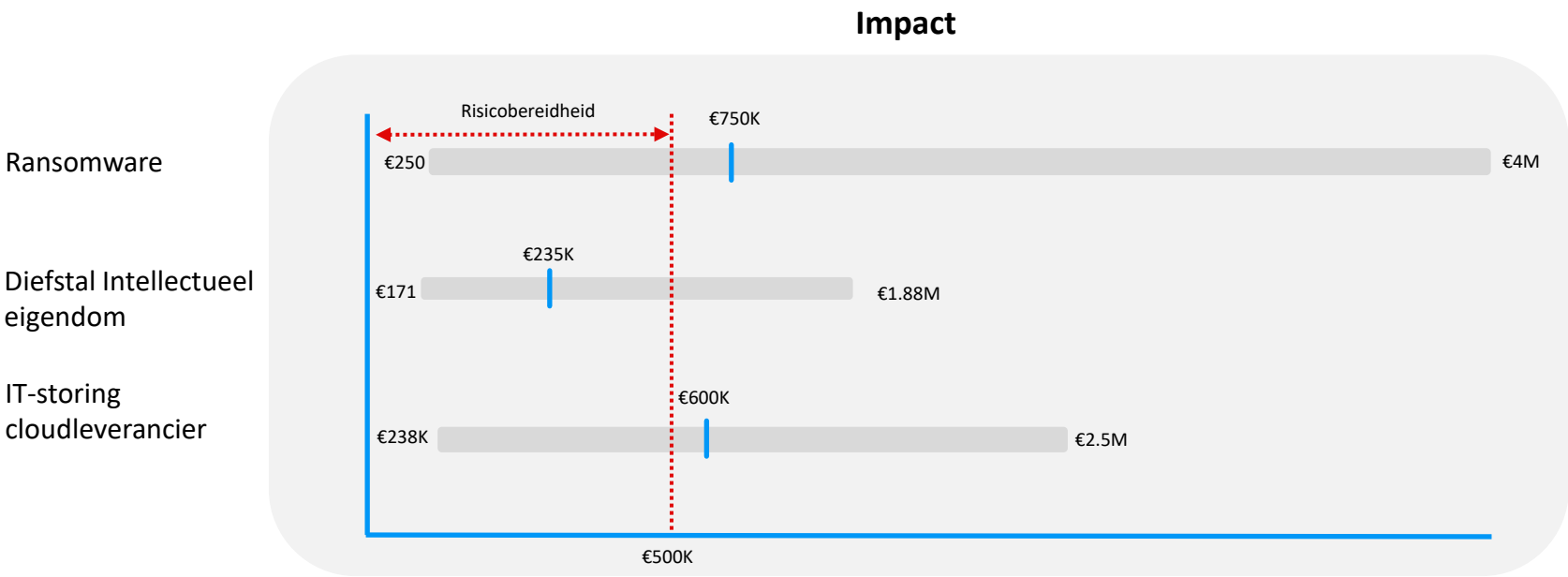
Het gebruik van cloudoplossingen en externe IT-dienstverleners biedt ACME flexibiliteit en ondersteunt de groeidoelstellingen binnen de BeNeLux. Het inzicht in afhankelijkheden en risico's binnen de keten is echter nog in ontwikkeling. Hierdoor is de organisatie kwetsbaarder voor verstoringen buiten de directe invloedssfeer, wat met name de impact van incidenten vergroot en herstel complexer maakt, zeker gezien de afhankelijkheid van tijdige levering binnen de supply chain van klanten.

Incidentrespons en herstelvermogen

Processen voor incidentrespons en herstel zijn aanwezig en rollen zijn belegd, wat een goede basis vormt voor het omgaan met verstoringen. Deze worden echter nog beperkt getest in realistische scenario's, zoals uitval van productiesystemen of ransomware-aanvallen. Dit verhoogt de kans dat incidenten minder effectief worden afgehandeld en verlengt de hersteltijd, wat direct bijdraagt aan een grotere operationele en financiële impact door stilstand en vertraging in leveringen.

Risicobereidheid

Fictief rapport



Risicobereidheid

Uit gesprekken met stakeholders blijkt dat ACME een jaarlijks verlies van circa €500.000 als maximaal acceptabel beschouwt. Op basis hiervan vallen de doorgerekende scenario's voor ransomware en verstoring van IT-voorzieningen buiten de risicobereidheid van de organisatie.

Dit betekent dat deze risico's als onacceptabel worden beschouwd en gerichte maatregelen vereisen om zowel de kans op optreden als de potentiële impact te reduceren.

Fictief rapport

Conclusie

Huidige staat van cyber security

ACME beschikt over een solide basis voor informatiebeveiliging, passend bij haar rol als specialistische speler in de maakindustrie. Tegelijkertijd leiden variaties in implementatie, beperkte detectiecapaciteit en afhankelijkheden van externe partijen ertoe dat zowel de kans op incidenten als de potentiële impact verhoogd zijn.

Versterkende factoren

Met name de combinatie van beperkte zichtbaarheid op kwaadwillende activiteiten, brede toegangsrechten en afhankelijkheid van leveranciers zorgt ervoor dat incidenten niet alleen waarschijnlijker zijn, maar zich ook sneller kunnen ontwikkelen tot verstoringen met directe impact op productie, leverbetrouwbaarheid en omzet.

Impact op bedrijfsvoering

Voor een organisatie als ACME, die een kritische schakel vormt in de supply chain, betekent dit dat cyberrisico's direct kunnen doorwerken naar klanten en contractuele verplichtingen. Gerichte verbeteringen op deze punten zullen aantoonbaar bijdragen aan het verlagen van zowel de kans op incidenten als de gevolgen ervan, en daarmee het totale beeld op cybersecurity.

Toekomstige ontwikkeling

Tegelijkertijd zal de verdere ontwikkeling van het IT-landschap, waaronder toenemende cloudadoptie, verdere integratie tussen IT en OT en uitbreiding van digitale ketenintegraties, het aanvalsoppervlak vergroten en de afhankelijkheid van externe partijen verder versterken. Dit vraagt om een meer proactieve en toekomstgerichte inrichting van cybersecurity, waarbij niet alleen huidige risico's worden gemitigeerd, maar ook structureel wordt gestuurd op weerbaarheid in een steeds complexer en meer verbonden landschap.

Fictief rapport

Advies

Uit het assessment is gebleken dat een deel van de geïdentificeerde cyberrisico's de risicobereidheid van ACME overschrijdt. Voor deze risico's zijn vier handelingsopties beschikbaar: mitigeren, verplaatsen, accepteren of vermijden.

Polar Risk heeft een set mitigerende maatregelen geïdentificeerd die gericht zijn op het verlagen van zowel de kans op incidenten als de potentiële impact. De effectiviteit hiervan is sterk afhankelijk van consistente implementatie en borging binnen de organisatie.

Ransomware

De potentiële verliezen in het ransomwarescenario worden voornamelijk gedreven door omzetverlies als gevolg van productiestilstand. De grootste risicoreductie ligt daarom in het beperken van de impact van verstoringen. Door te investeren in Business Continuity Management (BCM) en IT Disaster Recovery kan ACME de hersteltijd significant verkorten en de continuïteit van kritieke processen waarborgen. Dit verlaagt met name het maximale verlies (circa €4.000.000) en draagt direct bij aan het beperken van operationele en financiële schade.

Diefstal van intellectueel eigendom

Diefstal van intellectueel eigendom vindt voornamelijk plaats via gecompromitteerde accounts of samenwerkingsplatformen. Hoewel de impact hiervan beperkt beïnvloedbaar is, kan de waarschijnlijkheid van dit scenario substantieel worden verlaagd.

Het consistent implementeren en afdwingen van phishing-resistente Multi-Factor Authentication (MFA) vormt hierbij een sleutelmaatregel. In combinatie met periodieke controle en aanscherping van autorisaties wordt de kans op ongeautoriseerde toegang significant gereduceerd.

IT-storing bij leverancier

ACME heeft beperkte invloed op de kans dat een IT-leverancier een storing ondervindt. Wel kan de organisatie de impact van dergelijke verstoringen reduceren door de eigen IT-architectuur robuuster in te richten. Maatregelen richten zich op het vergroten van beschikbaarheid en redundantie, zoals:

- Geografisch gespreide en redundante IT-voorzieningen
- High Availability voor kritische systemen, waaronder het ERP-systeem
- Spreiding van IT-diensten over meerdere gespecialiseerde leveranciers

Aanvullend geldt, net als bij het ransomwarescenario, dat investeringen in Business Continuity Management bijdragen aan het beperken van de totale impact van verstoringen.

Korte en lange termijn prioriteiten

Korte termijn:

- Implementeren van phishing-resistente MFA voor kritieke systemen en accounts
- Aanscherpen en opschonen van autorisaties
- Verhogen van monitoring en detectie op kritieke omgevingen
- Opstellen en testen van incidentrespons- en herstelprocedures

Lange termijn

Inrichten en borgen van Business Continuity Management en IT Disaster Recovery

- Doorvoeren van architectuurverbeteringen gericht op redundantie en segmentatie
- Verminderen van afhankelijkheden door spreiding van IT-leveranciers
- Structureel verbeteren van ketenrisicomanagement en leveranciersbeheer

Fictief rapport

Bijlagen