VOORBEELD RAPPORT

Atlas Insight 360

Threat Assessment & Management Rapport

Opgesteld voor	Sector	Assessment datum
Testbedrijf B.V.	**Maakindustrie**	**4 april 2026**
	Aantal FTE	Adviseur
	85	**Robert Meulenhoff**

Dit rapport bevat vertrouwelijke informatie. Uitsluitend bestemd voor de directie van Testbedrijf B.V..

Atlas Cybersecurity
www.atlas-cybersecurity.nl · rtsb@atlas-cybersecurity.nl

INLEIDING

Over dit rapport

Dit rapport presenteert de uitkomsten van een Atlas Insight 360 assessment voor Testbedrijf B.V.. Het assessment brengt in kaart welke dreigingen relevant zijn voor uw organisatie, hoe kwetsbaar u bent voor elk van deze dreigingen, en wat de potentiële impact is op uw bedrijfscontinuïteit.

Het rapport is geschreven voor de directie en het management. Het bevat geen technische details of implementatie-instructies — die zijn opgenomen in een apart operationeel actieplan voor uw IT-partner.

Scope van het assessment

Organisatie	**Testbedrijf B.V.**
Sector	Maakindustrie
Omzet/jaar	€ 12,4 miljoen
Aantal FTE	85
Assessmentdatum	4 april 2026
Adviseur	Robert Meulenhoff
Classificatie	Vertrouwelijk — uitsluitend voor directie
Methode	Interview-gedreven assessment aangevuld met externe Atlas Sentinel scan

Beoordeelde dreigingen

Het assessment dekt zes dreigingscategorieën die relevant zijn voor MKB-organisaties in de maakindustriesector:

ID	Dreiging	Voorbeelden
T1	**Social Engineering**	CEO-fraude, phishing, identiteitsvervalsing
T2	**External Intrusion**	Inbraak via internet, malware, onbeveiligde toegang
T3	**Insider Risk (opzettelijk)**	Datadiefstal, misbruik bevoegdheden, fraude
T4	**Insider Risk (onopzettelijk)**	Verloren apparaten, zwakke wachtwoorden, menselijke fouten
T5	**DDoS & Uitvalbeheer**	Botnet-aanvallen, service-uitval, netwerkverzadiging
T6	**Third Party Compromise**	SaaS-inbreuk, leverancierscompromittering, supply chain

OVERZICHT

Risicoverdeling

Onderstaande tabel toont de risicoverdeling over de zes beoordeelde dreigingen. De scores zijn gebaseerd op het dreigingslandschap voor maakindustrie-organisaties, de getroffen maatregelen en de potentiële impact op Testbedrijf B.V..

0	2	2	1	1
Kritiek	Hoog	Gemiddeld	Laag	Zeer laag

Risico-overzicht per dreiging

#	Dreiging	Type	Dreigingsniveau	Impact	Risicoscore	Prioriteit
T1	**Social Engineering**	Deliberate	Low	Gemiddeld	Gemiddeld	P3
T2	**External Intrusion**	Deliberate	Observed	Hoog	Hoog	P2
T3	**Insider Risk (opzettelijk)**	Deliberate	Expected	Hoog	Hoog	P2
T4	**Insider Risk (onopzettelijk)**	Accidental	Confirmed	Kritiek	Kritiek	P1
T5	**DDoS & Uitvalbeheer**	Deliberate	Low	Laag	Laag	P4
T6	**Third Party Compromise**	Deliberate	Low	Gemiddeld	Gemiddeld	P3

Dreigingsniveau: inschatting van de kans dat deze dreiging zich voordoet. Impact: verwachte bedrijfsschade bij realisatie. Risicoscore: combinatie van dreigingsniveau en impact.

ANALYSE

Dreigingsanalyse

T1 — Social Engineering

Gemiddeld P3

Dreigingscontext	Phishing, CEO-fraude en WhatsApp-fraude zijn de meest voorkomende aanvalsmethoden voor maakindustrie-organisaties. Criminelen doen zich voor als directie, leveranciers of de bank om betalingen te onderscheppen of inloggegevens te stelen.
Potentiële impact	Bij een succesvolle CEO-fraudeaanval bedraagt de directe financiële schade voor een organisatie van de omvang van Testbedrijf B.V. gemiddeld €15.000–€80.000. Operationele verstoring is beperkt maar reputatieschade richting leveranciers is reëel.
Huidige situatie	Awareness-training is aanwezig maar niet structureel geborgd. Technische e-mailbeveiliging (DMARC) is onvolledig. Meldprocedure voor verdachte berichten is bekend maar niet afdwingbaar.

T2 — External Intrusion

Hoog P2

Dreigingscontext	Inbraak via internet — via onbeveiligde toegangen, zwakke wachtwoorden of verouderde software — is de meest gebruikte aanvalsvector voor ransomware. Actieve exploits voor bekende kwetsbaarheden circuleren continu.
Potentiële impact	Ransomware-uitval van 3–7 dagen kost een organisatie van de omvang van Testbedrijf B.V. naar schatting €150.000–€400.000 aan omzetverlies, herstelkosten en operationele schade. AVG-meldplicht is van toepassing bij dataversleuteling.
Huidige situatie	Externe scan (Atlas Sentinel) toont open poorten en verouderde software. MFA is niet universeel uitgerold. Patching-proces is reactief, niet proactief.

T3 — Insider Risk (opzettelijk)

Hoog P2

Dreigingscontext	Opzettelijke handelingen door medewerkers of ex-medewerkers — zoals datadiefstal, fraude of sabotage — zijn moeilijk te detecteren en worden vaak pas laat ontdekt. Vertrokken medewerkers met actieve accounts vormen een structureel risico.
Potentiële impact	Datadiefstal van klantgegevens of prijsinformatie heeft directe reputatieschade en mogelijke juridische aansprakelijkheid tot gevolg. Herstel van verwijderde of gewijzigde productiedata kan meerdere dagen duren.
Huidige situatie	Het offboarding-proces (afsluiten accounts bij vertrek) is niet structureel geborgd. Geen monitoring op afwijkend gebruikersgedrag aanwezig. Scheiding van bevoegdheden in productiesystemen is beperkt.

T4 — Insider Risk (onopzettelijk)

Kritiek P1

Dreigingscontext	Menselijke fouten zijn de grootste oorzaak van beveiligingsincidenten. Verloren laptops, verkeerd verstuurde e-mails, hergebruik van wachtwoorden en onbedoeld delen van bestanden leiden regelmatig tot datalekken met AVG-meldplicht.
Potentiële impact	Bij Testbedrijf B.V. is in het afgelopen jaar minimaal één incident geweest waarbij bedrijfsinformatie onbedoeld extern is gedeeld. De kans op een meldplichtig datalek onder de AVG binnen 12 maanden wordt als hoog ingeschat. Boetes en herstelkosten kunnen oplopen tot €100.000.
Huidige situatie	Geen volledige schijfversleuteling op alle laptops. Wachtwoordbeleid is aanwezig maar naleving is niet afgedwongen. Geen automatische melding bij verdachte bestandsoverdrachten. Dit is de hoogste prioriteit in het actieplan.

T5 — DDoS & Uitvalbeheer

Laag P4

Dreigingscontext	DDoS-aanvallen op maakindustrie-bedrijven zijn minder frequent dan op financiële instellingen. Het risico is beperkt maar niet nul — zeker als uw klantportaal of orderverwerking online is.
Potentiële impact	Uitval van 4–24 uur heeft beperkte financiële impact maar kan klantvertrouwen schaden als leveringstijden worden gemist. Hersteltijd is primair afhankelijk van uw hostingprovider.
Huidige situatie	Geen DDoS-mitigatie actief. Back-up procedure is aanwezig. Business continuity plan is globaal beschreven maar niet getest. Relatief laag risico — niet prioritair.

T6 — Third Party Compromise

Gemiddeld P3

Dreigingscontext	Een inbreuk bij een van uw SaaS-leveranciers, IT-dienstverleners of logistieke partners kan uw bedrijfsdata blootstellen zonder dat u zelf iets fout doet. Supply chain-aanvallen nemen toe.
Potentiële impact	Afhankelijk van welke leverancier wordt getroffen. Bij een inbreuk bij uw ERP- of CRM-leverancier kan klant- en orderdata worden blootgesteld. AVG-meldplicht is van toepassing.
Huidige situatie	Geen leveranciersbeoordelingsproces (Vendorcheck) aanwezig. Verwerkersovereenkomsten zijn deels aanwezig. Geen overzicht van welke leveranciers toegang hebben tot persoonsgegevens.

IMPACT

Vierdimensionele impactanalyse

Per dreiging is de potentiële impact beoordeeld op vier dimensies die relevant zijn voor de bedrijfscontinuïteit van Testbedrijf B.V.: financieel, operationeel, reputatie en juridisch.

Dreiging	Financieel	Operationeel	Reputatie	Juridisch
T1 Social Engineering	Gemiddeld	Laag	Gemiddeld	Laag
T2 External Intrusion	Hoog	Hoog	Gemiddeld	Gemiddeld
T3 Insider Risk (opzettelijk)	Hoog	Hoog	Hoog	Hoog
T4 Insider Risk (onopzettelijk)	Kritiek	Hoog	Gemiddeld	Hoog
T5 DDoS & Uitvalbeheer	Laag	Gemiddeld	Laag	Laag
T6 Third Party Compromise	Gemiddeld	Gemiddeld	Gemiddeld	Hoog

Hoogste gecombineerde impactscore: T4 — Insider Risk (onopzettelijk). De combinatie van een hoge kans (menselijke fouten komen dagelijks voor) en brede impact over alle vier dimensies maakt dit de meest urgente prioriteit voor Testbedrijf B.V..

ACTIEPLAN

Prioriteiten & Aanbevelingen

Onderstaand actieplan is direct afgeleid van de dreigingsanalyse. De acties zijn geprioriteerd op risicoscore en haalbaarheid. Quick wins zijn maatregelen die binnen drie maanden uitvoerbaar zijn met beperkte middelen.

Quick wins — uitvoeren binnen 3 maanden

#	Aanbeveling	Dreiging	Inspanning	Prioriteit
1	Schijfversleuteling (BitLocker/FileVault) activeren op alle laptops en mobiele apparaten	T4	Laag	P1
2	MFA verplicht stellen voor alle cloud-diensten en remote toegang	T2, T4	Laag	P1
3	Offboarding-procedure aanscherpen: checklist voor afsluiten accounts bij vertrek medewerkers	T3	Laag	P2
4	DMARC-record instellen op e-maildomein (p=quarantine als startpunt)	T1	Laag	P2
5	Wachtwoordmanager introduceren en wachtwoordbeleid afdwingen (minimaal 14 tekens, geen hergebruik)	T2, T4	Laag	P2
6	Leveranciersoverzicht opstellen: welke partijen hebben toegang tot persoonsgegevens? Verwerkersovereenkomsten completeren.	T6	Gemiddeld	P3

Middellange termijn — uitvoeren binnen 12 maanden

#	Aanbeveling	Dreiging	Prioriteit
7	Security awareness-training verplicht stellen voor alle medewerkers (minimaal 1x per jaar, inclusief phishing-simulatie)	T1, T3	P2
8	Patch-management proces formaliseren: maandelijkse patchcyclus voor alle systemen inclusief productiesoftware	T2	P2
9	Incidentresponsplan opstellen en testen: wat doet u de eerste 4 uur na een ransomware-aanval?	T2, T5	P3
10	Backup-procedure testen: hersteltest uitvoeren om te verifiëren dat back-ups ook daadwerkelijk werken	T2, T4	P3

1 1	Leveranciersbeoordeling uitvoeren voor Tier 1-leveranciers (Atlas Vendorcheck) op basis van BIO 2 v1.3	T6	**P3**

CONCLUSIE

Slotconclusie

Testbedrijf B.V. heeft een herkenbaar risicoprofiel voor een maakindustrie-organisatie van deze omvang. De grootste kwetsbaarheid ligt niet in technologie, maar in menselijk gedrag en ontbrekende procesborging — met name rondom onboarding, offboarding en het dagelijks omgaan met bedrijfsdata. De prioritaire acties (P1 en P2) zijn uitvoerbaar binnen drie maanden met beperkte investeringen en leveren directe risicoreductie op.

6	1	2	11
Dreigingen beoordeeld	Kritiek (P1)	Hoog (P2)	Aanbevelingen totaal

Herhaling & monitoring

Een risicoprofiel is geen statisch document. Dreigingen evolueren, uw organisatie groeit en wetgeving verandert. Atlas Insight 360 is ontworpen om jaarlijks herhaald te worden — als herhaling voor €1.000. Zo houdt u grip op de ontwikkeling van uw beveiligingsvolwassenheid over tijd.

Disclaimer

Dit rapport is gebaseerd op informatie verstrekt tijdens het assessment-interview en de externe Atlas Sentinel scan. Atlas Cybersecurity kan niet instaan voor de volledigheid van de verstrekte informatie. De bevindingen en aanbevelingen zijn indicatief en vormen geen formele audit of certificering. Dit rapport is vertrouwelijk en uitsluitend bestemd voor de directie van Testbedrijf B.V..

Klaar om uw risico's in kaart te brengen?

Dit rapport is een voorbeeld van wat Atlas Insight 360 oplevert voor een MKB-organisatie. Een volledig assessment wordt uitgevoerd op basis van een interview met uw directie of management — aangevuld met de Atlas Sentinel externe scan als nulmeting.

rtsb@atlas-cybersecurity.nl · atlas-cybersecurity.nl