INSTANTSECURE

SAMENGESTELD VOORBEELD

Cybersecurity Bewijs- en Weerbaarheidscheck

Voor een Nederlandse B2B-softwareleverancier met 34 medewerkers

Rapportnummer	**IS-EXAMPLE-2026-01**
Rapportdatum	**12 juli 2026**
Onderzoeksperiode	**Illustratief: 10 werkdagen**
Classificatie	**Openbaar voorbeeld - geen klantgegevens**

BELANGRIJK

Dit rapport is volledig fictief en samengesteld uit veelvoorkomende MKB-situaties. Het is geen testimonial, echte klantcase, audit of complianceverklaring.

LEESWIJZER

Leeswijzer en belangrijke afbakening

Dit document laat zien hoe een rapport van de Cybersecurity Bewijs- en Weerbaarheidscheck eruit kan zien. De organisatie, aantallen, systemen, documenten, bevindingen, citaten en deadlines zijn verzonnen maar bewust realistisch samengesteld.

Geen echte klant en geen verborgen testimonial

De voorbeeldorganisatie bestaat niet. De beschreven resultaten mogen niet worden gelezen als ervaring, review, succesclaim of uitkomst van een werkelijk uitgevoerde opdracht.

Wat deze check wel doet

- Interviews, documenten en aangeleverd bewijs in samenhang beoordelen.
- Vastleggen wat aanwezig, gedeeltelijk, niet aangetoond, niet beoordeeld of buiten scope is.
- Managementbesluiten, technische verdiepingen en bewijsacties van elkaar scheiden.
- Een uitvoerbare 30/60/90-dagenroadmap opleveren.

Wat deze check niet doet

- Geen organisatie cyberveilig verklaren of incidentvrijheid garanderen.
- Geen pentest, vulnerability scan of onbeperkte configuratiereview.
- Geen audit, assurance, certificering of juridisch complianceoordeel.
- Geen automatische acceptatie door klanten, auditors of toezichthouders.

Momentopname

Een rapport beschrijft de stand binnen de afgesproken periode en scope. Nieuwe accounts, configuratiewijzigingen, incidenten of leveranciers kunnen de feitelijke situatie daarna wijzigen.

DE OPDRACHT

1. Opdracht en organisatiecontext

De vraag die morgen binnen zou kunnen komen

Praktische klantvraag

Wij zijn een softwareleverancier met 34 medewerkers. Onze MSP zegt dat Microsoft 365 en de laptops goed zijn ingericht. Over zes weken start procurement bij een grotere klant. We willen nu weten wat echt geregeld is, wat we kunnen aantonen en wat we eerst moeten oplossen.

Organisatie	Nederlandse B2B-software- en managed-servicesleverancier
Omvang	34 medewerkers, 4 vaste externen, geen intern securityteam
Kernsystemen	Microsoft 365 Business Premium, Entra ID, Intune, Azure, GitHub, Jira/Confluence, CRM en externe SaaS
IT-model	Dagelijks beheer via MSP; interne IT-coordinator als aanspreekpunt
Aanleiding	Voorbereiding op procurement- en leveranciersvragen binnen circa zes weken
Beschikbare tijd	Management wil binnen 90 dagen de belangrijkste gaten sluiten

Wat management vooraf dacht

- MFA staat aan, dus toegang is afgedekt.
- De MSP maakt back-ups, dus herstel is geregeld.
- Bij een incident bellen we de MSP en dan komt het goed.
- We hebben beleid in SharePoint, dus klantvragen zijn te beantwoorden.
- Onze leveranciers zijn bekende partijen, dus daar zit weinig risico.

SCOPE EN METHODE

2. Scope, methode en ontvangen informatie

Binnen scope

- Managementverantwoordelijkheid en besluitvorming.
- Identiteit, MFA, beheerdersrechten en in-/uitdiensttreding op proces- en bewijsniveau.
- Werkplekken, updates en technisch beheer op hoofdlijnen.
- Back-ups, hersteltesten, logging en incidentmanagement.
- Kritieke leveranciers, beleid, awareness en bewijsstatus.

Buiten scope

- Pentest, vulnerability scan, source-code review en aanvalssimulatie.
- Volledige Microsoft 365-, Azure- of endpointconfiguratiereview.
- Juridische beoordeling van contracten of wetstoepasselijkheid.
- Formele ISO 27001-gap assessment, audit, assurance of certificering.

Uitgevoerde activiteiten in dit voorbeeld

Activiteit	Omvang	Doel
Managementinterview	75 minuten	Aanleiding, kritieke diensten, risicoacceptatie en besluitvorming
IT-coordinator	60 minuten	Accounts, apparaten, incidenten en bewijs
MSP-interview	60 minuten	MFA, monitoring, back-ups en open technische vragen
Documentreview	17 documenten	Beleid, procedures, contracten, registers en klantantwoorden
Bewijsreview	8 exports/screenshots	Status en beperkingen van MFA, apparaten, back-ups en logging

Beperking

Er is geen rechtstreekse systeemtoegang gebruikt. Technische conclusies zijn beperkt tot aangeleverde exports, screenshots, interviews en documenten.

MANAGEMENTSAMENVATTING

3. Managementsamenvatting

De voorbeeldorganisatie heeft meerdere zinvolle basismaatregelen, maar de huidige positie is nog niet consequent aantoonbaar richting een kritische klant. Het grootste probleem is niet dat er niets gebeurt; het probleem is dat uitvoering, eigenaarschap, technische bevestiging en bewijs niet als een beheerst geheel functioneren.

3 onderwerpen aanwezig en redelijk onderbouwd

5 onderwerpen zijn gedeeltelijk of technisch onbevestigd. 2 onderwerpen zijn niet aantoonbaar geregeld.

Niet onveilig verklaard, wel onvoldoende verdedigbaar

De organisatie kan nu niet zonder voorbehoud stellen dat MFA voor alle relevante accounts wordt afgedwongen, herstel aantoonbaar is getest, incidenten volgens een vooraf afgesproken proces worden afgehandeld en toegang tijdig wordt ingetrokken.

Sterke punten

- Microsoft 365 Business Premium en centraal werkplekbeheer bieden een bruikbare basis.
- De MSP kan relevante exports en beheerinformatie leveren.
- Dagelijkse back-upjobs en endpointbeheer zijn beschreven en deels onderbouwd.
- Management wil eigenaarschap en budget vrijmaken voor opvolging.

Belangrijkste onzekerheden

- MFA-registratie is niet hetzelfde als aantoonbare afdwinging.
- Een dagelijkse back-upjob bewijst niet dat herstel werkt.
- Uitdiensttreding en externe toegang zijn niet consequent aantoonbaar.
- Incidentrespons leunt op personen en mondelinge kennis.
- Bewijsstukken missen datum, scope, eigenaar of klantveilige versie.

BASELINE

4. Baseline- en bewijsmatrix

Domein	Status	Kernwaarneming	Technische verdieping?
Context en kritieke processen	Aanwezig	Kritieke klantdienst en kernsystemen zijn benoemd; impacttoleranties ontbreken.	Nee, eerst intern
Governance en eigenaarschap	Gedeeltelijk	COO neemt besluiten; formeel eigenaarschap en reviewcadans ontbreken.	Nee
Identiteit en toegang	Gedeeltelijk	MFA deels onderbouwd; afdwinging en externe accounts bevestigen.	Ja, M365-review
In-/uitdiensttreding	Niet aangetoond	Geen uniforme checklist of aantoonbare sluiting van alle SaaS-toegang.	Beperkt
Werkplekken en updates	Aanwezig, onbevestigd	29 van 31 apparaten zichtbaar als compliant; uitzonderingen bevestigen.	Ja, endpointreview
Back-ups en herstel	Gedeeltelijk	Back-upjobs bestaan; geen recent restore-testverslag.	Ja, restore-test
Logging en opvolging	Gedeeltelijk	Alerts gaan naar MSP; triage en escalatie niet aantoonbaar.	Ja, loggingreview
Incidentmanagement	Niet aangetoond	Geen vastgestelde procedure, ernstindeling of klantmeldmatrix.	Nee, daarna oefening
Leveranciers en cloud	Gedeeltelijk	Lijst bestaat zonder kritikaliteit, eigenaar en bewijs per leverancier.	Selectief
Beleid, awareness en bewijs	Gedeeltelijk	Beleid verouderd; awareness en evidence-index niet bijgehouden.	Nee

F-01 MFA is niet aantoonbaar voor alle relevante accounts afgedwongen

PRIORITEIT HOOG

Waarneming	Een geredigeerde registratie-export laat zien dat 27 van 31 interne gebruikers een sterke authenticatiemethode hebben geregistreerd. Registratie bewijst niet dat MFA bij iedere relevante aanmelding wordt afgedwongen. Voor vier interne accounts en twee externe accounts ontbreekt voldoende onderbouwing.
Onderbouwing bekeken	Entra-registratie-export, twee Conditional Access-screenshots, MSP-interview en lijst van actieve interne en externe accounts.
Waarom dit ertoe doet	De organisatie kan richting klant te stellig antwoorden dat MFA voor iedereen verplicht is, terwijl uitzonderingen en externe accounts nog niet zijn bevestigd.
Aanbevolen actie	Voer een gerichte read-only Microsoft 365-review uit. Bevestig toepassingsbereik, uitzonderingen, break-glass accounts en legacy authenticatie. Leg daarna een geredigeerde klantversie vast.
Voorgestelde eigenaar	IT-coordinator met MSP of InstantIT
Streefdatum	Binnen 15 werkdagen
Gewenst vervolgbewijs	Policy-export met datum en scope, uitzonderingenregister, break-glass-overzicht en herstelbewijs.

F-02 Uitdiensttreding is niet uniform en een extern account bleef te lang actief

PRIORITEIT HOOG

Waarneming	Er bestaat geen centrale joiner/mover/leaver-checklist voor Microsoft 365, GitHub, Jira, CRM en overige SaaS. In de aangeleverde lijst stond een extern GitHub-account elf dagen na de einddatum nog als actief geregistreerd.
Onderbouwing bekeken	HR-offboardingmail, overzicht actieve externe accounts, GitHub-organisatielijst en interviews.
Waarom dit ertoe doet	Verlate intrekking kan leiden tot ongewenste toegang en maakt klantantwoorden over tijdige offboarding moeilijk verdedigbaar.
Aanbevolen actie	Blokkeer het account na validatie. Maak een checklist met trigger, systemenlijst, uitvoerder, controleur, sluitingsbevestiging en bewijs. Review alle externe en voormalige accounts.
Voorgestelde eigenaar	HR-manager en IT-coordinator
Streefdatum	Account direct; proces binnen 20 werkdagen
Gewenst vervolgbewijs	Afgesloten accountlijst, ondertekende checklist, export met sluitingsdatum en kwartaalreview.

F-03 Back-ups bestaan, maar herstel is niet aantoonbaar getest

PRIORITEIT HOOG

Waarneming	De MSP levert dagelijkse jobrapportages voor Microsoft 365 en de kernapplicatie. Er is geen restore-testverslag van de afgelopen achttien maanden en geen aantoonbare hersteltijd.
Onderbouwing bekeken	Back-updashboard, maandrapport MSP, contractpassage over bewaartermijnen en interview.
Waarom dit ertoe doet	Een geslaagde back-upjob bewijst niet dat gegevens volledig, bruikbaar en binnen de benodigde tijd teruggezet kunnen worden.
Aanbevolen actie	Plan een beperkte restore-test met gekozen dataset, succescriteria, hersteltijd, verantwoordelijke en terugvalscenario. Leg beperkingen en vervolgacties vast.
Voorgestelde eigenaar	IT-coordinator en MSP
Streefdatum	Binnen 30 dagen
Gewenst vervolgbewijs	Restore-testplan, testverslag, screenshots of logs, gemeten hersteltijd en datum volgende test.

F-04 Incidentrespons is persoonsafhankelijk en niet klantklaar

PRIORITEIT MIDDEN

Waarneming	Bij een phishingincident in 2025 verliep afstemming via telefoon en WhatsApp. Er is geen vastgestelde procedure met ernstniveaus, eerste acties, beslissers, bewijsbewaring of klantmeldcriteria.
Onderbouwing bekeken	Korte incidentnotitie uit 2025 en interviews met management en MSP.
Waarom dit ertoe doet	Tijdens een incident gaat tijd verloren aan rollen en communicatie. De organisatie kan niet aantonen dat klant- en contractmeldingen vooraf zijn voorbereid.
Aanbevolen actie	Maak een compacte incidentprocedure plus een eenpagina-contactkaart. Voeg ernstindeling, eerste 60 minuten, communicatie, bewijsbewaring en klant-/contractcheck toe. Oefen daarna een scenario.
Voorgestelde eigenaar	COO, IT-coordinator en privacy/juridisch contact
Streefdatum	Procedure binnen 30 dagen; oefening binnen 75 dagen
Gewenst vervolgbewijs	Vastgestelde procedure, contactlijst, oefenverslag, aanwezigen en verbeteracties.

F-05 Logging en alertopvolging zijn niet als proces aantoonbaar

PRIORITEIT MIDDEN

Waarneming	De MSP ontvangt beveiligingsalerts in een gedeelde mailbox. Een overeengekomen classificatie, reactietijd, escalatiepad en maandelijkse rapportage ontbreken.
Onderbouwing bekeken	MSP-dienstbeschrijving, screenshot van alertmailbox en interviews.
Waarom dit ertoe doet	Het bestaan van logs of alerts kan ten onrechte als actieve monitoring worden gepresenteerd. Zonder opvolgproces kunnen relevante signalen blijven liggen.
Aanbevolen actie	Definieer welke alerts worden opgevolgd, binnen welke termijn, door wie en wanneer management wordt geinformeerd. Bevestig daarna bronnen en retentie technisch.
Voorgestelde eigenaar	MSP service owner en IT-coordinator
Streefdatum	Binnen 45 dagen
Gewenst vervolgbewijs	Alertmatrix, SLA, escalatiepad, voorbeeldticket en maandrapport.

F-06 Kritieke leveranciers zijn niet geclassificeerd

PRIORITEIT MIDDEN

Waarneming	Er is een spreadsheet met twaalf leveranciers, maar zonder kritikaliteit, proceseigenaar, gegevenscategorie, toegangsvorm, exit-afhankelijkheid of datum van laatste beoordeling.
Onderbouwing bekeken	Leverancierslijst, contractmap en managementinterview.
Waarom dit ertoe doet	De organisatie kan niet snel uitleggen welke leveranciers kritiek zijn, welke toegang zij hebben en welke contractuele of continuiteitsmaatregelen bestaan.
Aanbevolen actie	Classificeer leveranciers op bedrijfsimpact, gegevens, toegang en vervangbaarheid. Controleer eerst de vijf kritieke leveranciers en leg ontbrekende contractstukken of risicoacceptaties vast.
Voorgestelde eigenaar	COO en contracteigenaren
Streefdatum	Top vijf binnen 60 dagen; volledige lijst binnen 90 dagen
Gewenst vervolgbewijs	Geclassificeerd register, contractverwijzingen, reviewdatum, open punt, eigenaar en exitnotitie.

F-07 Bewijs is verspreid en mist datum, scope of eigenaar

PRIORITEIT MIDDEN

Waarneming	Beleid, exports, screenshots en klantantwoorden staan verspreid over SharePoint, e-mail en het MSP-portaal. Twee eerdere klantantwoorden stellen dat MFA voor alle gebruikers verplicht is zonder gekoppelde onderbouwing.
Onderbouwing bekeken	Documentinventaris, twee eerdere klantvragenlijsten en interviews.
Waarom dit ertoe doet	Ook bestaande maatregelen zijn daardoor traag en inconsistent aantoonbaar. Verouderde of te stellige antwoorden vergroten commercieel en contractueel risico.
Aanbevolen actie	Maak een evidence-index met bewijs-ID, onderwerp, eigenaar, datum, scope, deelbaarheidsniveau en volgende review. Koppel standaardantwoorden alleen aan actuele onderbouwing.
Voorgestelde eigenaar	IT-coordinator als evidence-coordinator
Streefdatum	Eerste index binnen 30 dagen; klantklare set binnen 75 dagen
Gewenst vervolgbewijs	Evidence-index, versienummers, reviewdata, klantveilige exports en goedgekeurde antwoordbibliotheek.

ROADMAP

6. 30/60/90-dagenroadmap

De roadmap is geprioriteerd op directe toegangs- en herstelrisico's, klantverdedigbaarheid en afhankelijkheden tussen acties. Technische uitvoering en juridisch advies zijn afzonderlijke opdrachten waar nodig.

Termijn	Actie	Eigenaar	Gewenst resultaat of bewijs
0-5 dagen	Sluit resterend extern GitHub-account en review alle externe accounts.	IT-coordinator + MSP	Sluitingsbewijs en uitzonderingenlijst.
0-15 dagen	Gerichte M365-review op MFA, uitzonderingen, break-glass en legacy routes.	MSP / InstantIT	Geredigeerde policy-export en herstelacties.
0-30 dagen	Voer beperkte restore-test uit met succescriteria en gemeten hersteltijd.	IT-coordinator + MSP	Ondertekend testverslag.
0-30 dagen	Stel incidentprocedure, contactkaart en klantmeldcheck vast.	COO	Goedgekeurde versie en distributielijst.
0-30 dagen	Maak evidence-index en stop ongefundeerde standaardantwoorden.	IT-coordinator + InstantSecure	Evidence-index en herziene antwoordbibliotheek.
31-60 dagen	Formaliseer offboarding, alertopvolging en top-vijf leveranciersclassificatie.	HR, IT, COO en MSP	Checklist, alertmatrix en register.
61-90 dagen	Oefen incident, bouw klantklare bewijsset en managementreview.	COO + IT + InstantSecure	Oefenverslag, Bewijsmap en reviewagenda.

EVIDENCE-INDEX

7. Voorbeeld evidence-index

Een evidence-index voorkomt dat screenshots, beleidsdocumenten en exports zonder context worden gedeeld. Ieder bewijsstuk krijgt een ID, eigenaar, datum, scope, deelbaarheidsniveau en volgende review.

ID	Bewijsstuk	Status	Scope of beperking
E-001	MFA-registratie-export	Aanwezig	Registratie; geen volledige afdwingingsbevestiging
E-002	Conditional Access-samenvatting	Gedeeltelijk	Twee policies; uitzonderingen niet volledig
E-003	Actieve externe accounts	Aanwezig	M365 en GitHub; overige SaaS aanvullen
E-004	Back-up jobrapport	Aanwezig	Toont jobs; geen herstelbaarheid
E-005	Restore-testverslag	Ontbreekt	Nog uit te voeren
E-006	Incidentprocedure	Ontbreekt	Concept nog niet vastgesteld
E-007	Endpoint compliance-export	Gedeeltelijk	29/31 zichtbaar; uitzonderingen bevestigen
E-008	Leveranciersregister	Gedeeltelijk	Twaalf leveranciers; geen kritikaliteit

Deelbaarheidsregel

Een klantveilige versie bevat alleen informatie die nodig is om de maatregel aannemelijk te maken. Gebruikersnamen, tenant-ID's, interne IP-adressen, herstelcodes en volledige policylogica worden verwijderd of samengevat.

MANAGEMENTBESLUITEN

8. Besluiten die bij oplevering nodig zijn

D-01

Benoem de COO formeel als bestuurlijk eigenaar en de IT-coordinator als evidence-coordinator.

D-02

Geef opdracht voor een gerichte Microsoft 365-review en autoriseer geredigeerde exports.

D-03

Plan ieder halfjaar een hersteltest voor ten minste een kritieke dataset of dienst.

D-04

Stel de incidentprocedure vast en wijs een juridisch/privacy-escalatiecontact aan.

D-05

Classificeer eerst de vijf kritieke leveranciers en accepteer open risico’s alleen schriftelijk.

D-06

Gebruik richting klanten geen absolute formuleringen zonder actuele onderbouwing.

Voorbeeld van een verdedigbare klantformulering

MFA - na de eerste review

MFA wordt afgedwongen voor beheerders en voor reguliere gebruikers die binnen de vastgestelde toegangspolicies vallen. Een gerichte review van uitzonderingen en externe accounts is gestart. Tot afronding beschrijven wij de maatregel als gedeeltelijk bevestigd.

EINDCONCLUSIE

9. Eindconclusie

In dit samengestelde voorbeeld is de organisatie niet afgekeurd en ook niet veilig verklaard. Meerdere maatregelen bestaan waarschijnlijk, maar cruciale claims over MFA, herstel, offboarding, logging en incidentrespons zijn nog niet voldoende bevestigd of aantoonbaar gemaakt.

Realistische eindboodschap aan de klant

De organisatie heeft een bruikbare technische en organisatorische basis. De hoogste prioriteit ligt bij toegang, herstelbaarheid en incidentvoorbereiding. Wanneer de acties voor de eerste 30 dagen worden uitgevoerd en onderbouwd, kan de organisatie aanzienlijk feitelijker antwoorden op een eerste klantassessment. Dat blijft een momentopname en geen audit- of complianceverklaring.

Logische vervolgroutes

Route	Wanneer	Uitvoerder
Technische quick wins	MFA, accounts, restore-test, endpoint- of loggingvalidatie	MSP, InstantIT of specialist
Cybersecurity Bewijsmap	Bewijs en klantantwoorden structureel hergebruiken	InstantSecure
Pentest / vulnerability scan	Technische kwetsbaarheden of aanvalspaden testen	Gespecialiseerde partner
Audit / certificering	Formele zekerheid of certificaat vereist	Onafhankelijke auditor
Juridisch advies	Wetstoepasselijkheid of contractrisico beoordelen	Gespecialiseerde jurist

Over InstantSecure

InstantSecure helpt MKB-leveranciers basismaatregelen, uitvoering, bewijs, open punten en roadmap met elkaar verbinden. De dienstverlening is geen audit, certificering, pentest, assurance of juridisch complianceoordeel. Technische uitvoering loopt via de eigen IT-partij, MSP, InstantIT of een specialist.

Website: instantsecure.nl E-mail: contact@instantsecure.nl