INSTANTSECURE

GEANONIMISEERDE PRAKTIJKCASE

Cybersecurity Bewijs- en Weerbaarheidscheck

B2B-softwareleverancier voorbereid op een klantassessment

Rapportnummer	**IS-CASE-2026-01**
Rapportdatum	**12 juli 2026**
Onderzoeksperiode	**10 werkdagen**
Classificatie	**Geanonimiseerd voorbeeldrapport**

Herkenbare kenmerken, aantallen en details zijn aangepast en gecombineerd om de werkwijze en rapportage realistisch te tonen.

KLANTVRAAG EN CONTEXT

1. Opdracht en organisatiecontext

De klantvraag

Een strategische klant vroeg de softwareleverancier om binnen zes weken een uitgebreide leveranciersbeoordeling te doorlopen. De directie wilde vooraf weten welke maatregelen daadwerkelijk waren ingericht, wat daarvan aantoonbaar was en welke verbeteringen eerst moesten worden uitgevoerd.

Organisatie	Nederlandse B2B-software- en managed-servicesleverancier
Omvang	34 medewerkers en vier vaste externen
Kernsystemen	Microsoft 365 Business Premium, Entra ID, Intune, Azure, GitHub, Jira, CRM en SaaS
IT-model	Externe MSP met interne IT-coordinator
Aanleiding	Strategische klant en procurementreview
Doorlooptijd	Tien werkdagen na complete aanlevering

Uitgevoerde werkzaamheden

- Managementinterview van 75 minuten.
- Interview met IT-coordinator en MSP.
- Review van 17 documenten en twee eerdere klantvragenlijsten.
- Beoordeling van acht geredigeerde exports en screenshots.

MANAGEMENTSAMENVATTING

2. Managementsamenvatting

De technische basis was bruikbaar, maar de organisatie kon zeven belangrijke klantclaims nog niet consequent en actueel onderbouwen. Het grootste risico zat in de afstand tussen wat management dacht dat geregeld was, wat de MSP daadwerkelijk beheerde en wat veilig richting een klant kon worden gedeeld.

Bestuurlijke conclusie

Een breed certificeringstraject was niet nodig voor de eerste klantdeadline. Toegang, herstelbaarheid, offboarding en incidentrespons moesten wel met voorrang worden aangescherpt en voorzien van actueel bewijs.

Status op hoofdlijnen

- 3 onderwerpen aanwezig en redelijk onderbouwd.
- 5 onderwerpen gedeeltelijk of technisch onbevestigd.
- 2 onderwerpen niet aantoonbaar geregeld.

Sterke punten

- Microsoft 365 Business Premium en centraal werkplekbeheer boden een bruikbare basis.
- De MSP kon relevante exports en beheerinformatie leveren.
- Management reserveerde eigenaarschap en budget voor opvolging.

BASELINE

3. Baseline- en bewijsmatrix

Domein	Status	Kernwaarneming	Vervolgroute
Context en processen	Aanwezig	Kritieke klantdienst en systemen benoemd; impacttoleranties aanvullen.	Management
Governance	Gedeeltelijk	Besluitvorming aanwezig; eigenaarschap en reviewcadans ontbraken.	Intern
Identiteit en toegang	Gedeeltelijk	MFA deels onderbouwd; uitzonderingen en externen bevestigen.	M365-review
Offboarding	Niet aangetoond	Geen uniforme checklist of sluitingsbewijs voor alle SaaS.	HR + IT + MSP
Werkplekken	Deels gevalideerd	29 van 31 apparaten compliant; twee uitzonderingen bevestigen.	Endpointreview
Back-ups en herstel	Gedeeltelijk	Back-upjobs aanwezig; geen recente hersteltest.	Restore-test
Logging	Gedeeltelijk	Alerts aanwezig; opvolging en escalatie niet aantoonbaar.	MSP-afspraken
Incidentmanagement	Niet aangetoond	Geen procedure, ernstindeling of klantmeldmatrix.	Procedure + oefening
Leveranciers	Gedeeltelijk	Lijst aanwezig zonder kritikaliteit en reviewdatum.	Leveranciersreview
Beleid en bewijs	Gedeeltelijk	Stukken verspreid en regelmatig zonder eigenaar of datum.	Evidence-index

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

HOOG

Waarneming	Een registratie-export liet zien dat 27 van 31 interne gebruikers een sterke authenticatiemethode hadden geregistreerd. Voor vier interne en twee externe accounts ontbrak voldoende bevestiging van afdwinging en uitzonderingen.
Onderbouwing	Entra-registratie-export, twee Conditional Access-samenvattingen, MSP-interview en actieve-accountlijst.
Impact	De eerdere klantclaim dat MFA voor alle gebruikers verplicht was, was te absoluut en niet volledig onderbouwd.
Actie	Gerichte Microsoft 365-review uitvoeren, toepassingsbereik en uitzonderingen bevestigen en een klantveilige samenvatting vastleggen.
Eigenaar	IT-coordinator met MSP
Deadline	15 werkdagen
Vervolgbewijs	Policy-export met datum en scope, uitzonderingenregister, break-glass-overzicht en herstelbewijs.

F-02 Uitdiensttreding was niet uniform en een extern account bleef actief

HOOG

Waarneming	Er bestond geen centrale offboardingchecklist. Een extern GitHub-account stond elf dagen na de einddatum nog als actief geregistreerd.
Onderbouwing	HR-offboardingmail, actieve-accountlijst, GitHub-organisatielijst en interviews met HR en IT.
Impact	Verlate intrekking vergroot toegangsrisico en maakt klantantwoorden over tijdige offboarding moeilijk verdedigbaar.
Actie	Account sluiten, alle externe accounts reviewen en een uniform joiner/mover/leaver-proces invoeren.
Eigenaar	HR-manager en IT-coordinator
Deadline	Account direct; proces binnen 20 werkdagen
Vervolgbewijs	Afgesloten accountlijst, ondertekende checklist, sluitingsdatum en kwartaalreview.

F-03 Back-ups bestonden, maar herstel was niet aantoonbaar getest

HOOG

Waarneming	Dagelijkse jobrapportages waren beschikbaar, maar een restore-testverslag van de voorafgaande achttien maanden en een gemeten hersteltijd ontbraken.
Onderbouwing	Back-updashboard, MSP-maandrapport, contractpassage over bewaartermijnen en IT-interview.
Impact	Een geslaagde back-upjob bewijst niet dat gegevens volledig en binnen de benodigde tijd kunnen worden teruggezet.
Actie	Beperkte restore-test uitvoeren met gekozen dataset, succescriteria, gemeten hersteltijd en vastgelegde afwijkingen.
Eigenaar	IT-coordinator en MSP
Deadline	30 dagen
Vervolgbewijs	Restore-testplan, testverslag, logs, gemeten hersteltijd en datum volgende test.

F-04 Incidentrespons was persoonsafhankelijk en niet klantklaar

MIDDEN

Waarneming	Een eerder phishingincident werd via telefoon en WhatsApp afgehandeld. Rollen, ernstniveaus, eerste acties en klantmeldcriteria waren niet vooraf vastgesteld.
Onderbouwing	Incidentnotitie, managementinterview en MSP-interview.
Impact	Bij een nieuw incident zou tijd verloren gaan aan rolverdeling en communicatie.
Actie	Compacte incidentprocedure en contactkaart vaststellen en daarna een accountovername-scenario oefenen.
Eigenaar	COO, IT-coordinator en privacycontact
Deadline	Procedure 30 dagen; oefening 75 dagen
Vervolgbewijs	Vastgestelde procedure, contactlijst, oefenverslag en verbeteracties.

F-05 Logging en alertopvolging waren niet als proces aantoonbaar

MIDDEN

Waarneming	De MSP ontving beveiligingsalerts in een gedeelde mailbox. Classificatie, reactietijd, escalatiepad en periodieke rapportage waren niet overeengekomen.
Onderbouwing	MSP-dienstbeschrijving, screenshot alertmailbox en interviews.
Impact	Het bestaan van logs of alerts kon ten onrechte als actieve monitoring worden gepresenteerd.
Actie	Alertmatrix, reactietijden, escalatie en managementrapportage vastleggen.
Eigenaar	MSP service owner en IT-coordinator
Deadline	45 dagen
Vervolgbewijs	Alertmatrix, SLA, voorbeeldticket en maandrapport.

F-06 Kritieke leveranciers waren niet geclassificeerd

MIDDEN

Waarneming	Een lijst met twaalf leveranciers bestond, maar zonder kritikaliteit, proceseigenaar, toegangsvorm, exit-afhankelijkheid of laatste reviewdatum.
Onderbouwing	Leverancierslijst, contractmap en managementinterview.
Impact	De organisatie kon niet snel uitleggen welke leveranciers kritiek waren en welke continuiteitsmaatregelen bestonden.
Actie	Leveranciers classificeren op bedrijfsimpact, gegevens, toegang en vervangbaarheid; eerst de top vijf beoordelen.
Eigenaar	COO en contracteigenaren
Deadline	Top vijf 60 dagen; volledig 90 dagen
Vervolgbewijs	Geclassificeerd register, contractverwijzingen, reviewdatum, eigenaar en exitnotitie.

F-07 Securitybewijs was verspreid en miste datum, scope of eigenaar

MIDDEN

Waarneming	Beleid, exports en screenshots stonden verspreid over SharePoint, e-mail en het MSP-portaal. Meerdere stukken hadden geen eigenaar of reviewdatum.
Onderbouwing	Documentinventaris, twee klantvragenlijsten en interviews met management en IT.
Impact	Bestaande maatregelen waren daardoor traag en inconsistent aantoonbaar.
Actie	Evidence-index maken met bewijs-ID, onderwerp, eigenaar, datum, scope, deelbaarheidsniveau en volgende review.
Eigenaar	IT-coordinator als evidence-coordinator
Deadline	Eerste index 30 dagen; klantklare set 75 dagen
Vervolgbewijs	Evidence-index, versienummers, reviewdata, klantveilige exports en antwoordbibliotheek.

ROADMAP

5. 30/60/90-dagenroadmap

Termijn	Actie	Eigenaar	Bewijs
0-5 dagen	Extern GitHub-account sluiten en externe toegang reviewen.	IT + MSP	Sluitingsbewijs
0-15 dagen	M365-review op MFA, uitzonderingen en break-glass.	MSP	Policy-export
0-30 dagen	Restore-test met gemeten hersteltijd uitvoeren.	IT + MSP	Testverslag
0-30 dagen	Incidentprocedure en klantmeldcheck vaststellen.	COO	Procedure v1.0
0-30 dagen	Evidence-index opbouwen en klantantwoorden herzien.	IT + InstantSecure	Index en antwoordset
31-60 dagen	Offboarding, alertopvolging en top-vijf leveranciers formaliseren.	HR, IT, COO, MSP	Checklist en registers
61-90 dagen	Incidentoefening uitvoeren en managementreview inplannen.	COO + IT	Oefenverslag

RESULTAAT

6. Resultaat na opvolging

31 van 31 interne accounts beoordeeld

Vier accounts zijn hersteld. Uitzonderingen en noodaccounts zijn afzonderlijk vastgelegd.

Hersteltijd gemeten op 2 uur en 18 minuten

De restore-test leverde twee concrete verbeteracties op met eigenaar en deadline.

24 bewijsstukken geregistreerd

Negen bewijsstukken waren direct klantklaar; zes waren gekoppeld aan een open verbeteractie.

Incidentprocedure vastgesteld en geoefend

Rollen, eerste acties, escalatie en klantcommunicatie zijn getest in een accountovername-scenario.

Uitkomst voor het klantassessment

De leverancier beantwoorde de vragenlijst met actuele, begrensde formuleringen en bewijs per onderwerp. Voor resterende open punten waren eigenaar, deadline en vervolgbewijs opgenomen. De klant stelde nog twee inhoudelijke verduidelijkingsvragen, maar vroeg geen volledige herbeoordeling.

EVIDENCE-INDEX

7. Voorbeeld van de evidence-index

ID	Bewijsstuk	Status	Scope of beperking
E-001	MFA-registratie-export	Aanwezig	Registratie; afdwinging later bevestigd
E-002	Conditional Access-samenvatting	Opgeleverd	Scope en uitzonderingen vastgelegd
E-003	Externe-accountlijst	Opgeleverd	M365, GitHub, Jira en CRM
E-004	Back-up jobrapport	Aanwezig	Toont jobs, niet herstelbaarheid
E-005	Restore-testverslag	Opgeleverd	2 uur 18 minuten; twee afwijkingen
E-006	Incidentprocedure	Opgeleverd	Versie 1.0 vastgesteld en geoefend
E-007	Endpoint-export	Gedeeltelijk	29 van 31 apparaten bevestigd
E-008	Leveranciersregister	Opgeleverd	Top vijf geclassificeerd

Klantveilige deelregel

Alleen informatie die nodig was om de maatregel aannemelijk te maken, werd gedeeld. Gebruikersnamen, tenant-ID’s, interne adressen, herstelcodes en volledige policylogica bleven buiten de klantversie.

MANAGEMENTBESLUITEN

8. Vastgelegde besluiten

D-01

De COO is bestuurlijk eigenaar van cybersecuritybesluiten; de IT-coordinator beheert de evidence-index.

D-02

De MSP levert ieder kwartaal geredigeerde exports voor MFA, endpoints, back-ups en alertopvolging.

D-03

Minimaal ieder halfjaar wordt een hersteltest uitgevoerd voor een kritieke dataset of dienst.

D-04

Open risico’s worden alleen met eigenaar, deadline en expliciete risicoacceptatie doorgeschoven.

D-05

Klantantwoorden worden uitsluitend gebruikt met actueel bewijs of een expliciet open punt.

Voorbeeld van klantklare MFA-formulering

Feitelijk en begrensd

MFA wordt afgedwongen voor beheerders en reguliere gebruikers binnen de vastgestelde toegangspolicies. Uitzonderingen en noodaccounts zijn afzonderlijk geregistreerd en worden periodiek beoordeeld. Een geredigeerde samenvatting van de actuele scope en laatste review is beschikbaar.

EINDCONCLUSIE

9. Eindconclusie

De organisatie beschikte over een bruikbare technische basis, maar kon belangrijke klantclaims aanvankelijk niet consequent onderbouwen. Door toegang, herstel, offboarding, incidentrespons en bewijsbeheer gericht te verbeteren, ontstond binnen negentig dagen een werkbare en verdedigbare basis voor het klantassessment.

Wat het rapport veranderde

De directie kreeg geen generieke lijst van tientallen controles, maar een beperkte set beslissingen, concrete opdrachten voor de MSP en een bewijsstructuur die direct bruikbaar was in het klantproces.

Logische vervolgroutes

- Technische quick wins via MSP, InstantIT of specialist.
- Cybersecurity Bewijsmap voor structureel hergebruik van bewijs en antwoorden.
- Pentest of vulnerability scan wanneer technische kwetsbaarheden moeten worden getest.
- Audit, certificering of juridisch advies wanneer formele zekerheid nodig is.

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