

InfoSafety CyberScan — NovaDesk BV (fictief)

Zakelijke dienstverlening · 4/8/2026

De CyberScan toetst 40 aandachtspunten uit CyFun® en het NIST Cybersecurity Framework. Het is geen formele CyFun-beoordeling, maar geeft in circa 15 minuten een grondig beeld van je cyberweerbaarheid.

De algemene cyberweerbaarheid van **NovaDesk BV (fictief)** is **Redelijk, maar met kritieke rode vlaggen (58%)**. De zekerheid van de antwoorden bedraagt **93%**. Er zijn **3 kritieke rode vlaggen** vastgesteld. De belangrijkste prioriteit ligt niet in extra complexiteit, maar in het wegwerken van deze rode vlaggen: Geteste back-up, Incidentresponsplan, MFA op kritieke accounts. De scan is een gestructureerde indicatie op basis van de antwoorden, geen formele audit of certificering.

Aanvullende context uit de intake

Uitbestede IT: De werkplek, Microsoft 365, back-up en eerstelijnsondersteuning worden door één externe IT-partner beheerd.

Persoonsgegevens: De organisatie verwerkt klanten-, medewerkers- en contactgegevens; er worden geen bijzondere categorieën op grote schaal verwerkt.

Cloud: De belangrijkste cloudtoepassingen zijn Microsoft 365, een CRM-platform en een online boekhoudpakket.

Extern bereikbare toepassingen: De publieke website en twee cloudportalen zijn extern bereikbaar; extern beheer gebeurt via beveiligde toegang.

58%

Algemene weerbaarheid

93%

Zekerheid van antwoorden

3

Kritieke rode vlaggen

22

Openstaande aandachtspunten

Kritieke maatregelen: **3 onvoldoende**, waarvan **2 ontbrekend/onzeker** en **1 gedeeltelijk**.

Je antwoordde 3× "Weet ik niet". Dat betekent niet automatisch dat maatregelen ontbreken, maar wel dat er onvoldoende zicht of eigenaarschap is. Voor een bestuurder of zaakvoerder is dat op zich een belangrijk governance-sigitaal.



1 Domeinscores

58% Governance	75% Identificeren
65% Beschermen	50% Detecteren
50% Reageren	50% Herstellen

2 Kritieke rode vlaggen

Een kritieke rode vlag is een ontbrekende of slechts gedeeltelijk aantoonbare basismaatregel die bij een cyberincident disproportioneel veel impact kan hebben.

1 Geteste back-up BESCHERMEN · PROCES

Een back-up die nooit getest is, blijkt vaak pas onbruikbaar wanneer je ze nodig hebt.

Controlevraag: "Worden back-ups regelmatig getest door effectief data of een systeem terug te zetten?"

Advies: Plan deze maand een testherstel van minstens één kritiek systeem.

2 Incidentresponsplan REAGEREN · PROCES

Zonder plan gaat de eerste, cruciale tijd verloren aan paniek en discussie.

Controlevraag: "Is er een eenvoudig incidentresponsplan dat beschrijft wie wat doet bij een cyberincident?"

Advies: Schrijf één A4 met: wie beslist, wie belt wie, welke systemen zet je offline en wie communiceert.

3 MFA op kritieke accounts BESCHERMEN · TECHNOLOGIE

Zonder MFA volstaat een gestolen wachtwoord vaak om binnen te geraken.

Controlevraag: "Is multi-factor authenticatie actief voor e-mail, cloudtoepassingen, VPN en administratoraccounts?"

Advies: Activeer MFA eerst op e-mail, cloudtoepassingen en administratoraccounts.

3 Top 5 bedrijfsrisico's

1 Geteste back-up **kernrisico**

Een back-up die nooit getest is, blijkt vaak pas onbruikbaar wanneer je ze nodig hebt.

Controlevraag: "Worden back-ups regelmatig getest door effectief data of een systeem terug te zetten?" —

BESCHERMEN · PROCES

2 Incidentresponsplan **kernrisico**

Zonder plan gaat de eerste, cruciale tijd verloren aan paniek en discussie.

Controlevraag: "Is er een eenvoudig incidentresponsplan dat beschrijft wie wat doet bij een cyberincident?" —

REAGEREN · PROCES

3 MFA op kritieke accounts **kernrisico**

Zonder MFA volstaat een gestolen wachtwoord vaak om binnen te geraken.

Controlevraag: "Is multi-factor authenticatie actief voor e-mail, cloudtoepassingen, VPN en administratoraccounts?" —

BESCHERMEN · TECHNOLOGIE

4 Zicht op leveranciersactiviteit

Zonder zicht op leveranciersactiviteit merk je fouten of misbruik vaak pas veel later.

Controlevraag: "Kan je nagaan wat leveranciers met toegang tot jullie systemen doen, bijvoorbeeld via logging of periodieke rapportage?" —

DETECTEREN · LEVERANCIERS

5 Evaluatie na incident

Zonder evaluatie blijven dezelfde zwakke plekken bestaan.

Controlevraag: "Wordt na een incident of bijna-incident geëvalueerd wat beter kan?" —

HERSTELLEN · PROCES

4 Top 5 quick wins

1 Activeer MFA eerst op e-mail, cloudtoepassingen en administratoraccounts.

Waarom: Zonder MFA volstaat een gestolen wachtwoord vaak om binnen te geraken.

Typische eigenaar: IT-leverancier —

BESCHERMEN · TECHNOLOGIE

2 Plan deze maand een testherstel van minstens één kritiek systeem.

Waarom: Een back-up die nooit getest is, blijkt vaak pas onbruikbaar wanneer je ze nodig hebt.

Typische eigenaar: **IT-leverancier** — BESCHERMEN · PROCES

3

Schrijf één A4 met: wie beslist, wie belt wie, welke systemen zet je offline en wie communiceert.

Waarom: Zonder plan gaat de eerste, cruciale tijd verloren aan paniek en discussie.

Typische eigenaar: **directie** — REAGEREN · PROCES

4

Duid één aanspreekpunt aan voor informatieveiligheid.

Waarom: Zonder aanspreekpunt wordt veiligheid ieders taak, en dus vaak niemands prioriteit.

Typische eigenaar: **directie** — GOVERNANCE · MEDEWERKERS

5

Vraag je IT-leverancier een lijst van extern bereikbare systemen en wie ze beheert.

Waarom: Extern bereikbare systemen zijn vaak de eerste plek waar aanvallers zoeken naar zwakke plekken.

Typische eigenaar: **IT-leverancier** — IDENTIFICEREN · TECHNOLOGIE

5 30-dagenactieplan

Deze acties lossen rechtstreeks de kritieke rode vlaggen hierboven op — begin hier. Deze acties moet je minstens binnen 30 dagen opstarten. Sommige zijn snel klaar; andere (bv. een aanpassing bij je IT-leverancier) vragen verdere uitwerking, maar moeten wel nu al opgestart worden.

Geteste back-up

Een back-up die nooit getest is, blijkt vaak pas onbruikbaar wanneer je ze nodig hebt.

Plan deze maand een testherstel van minstens één kritiek systeem.

BESCHERMEN · PROCES

Afgesproken: Zaakvoerder · tegen 31/8/2026

Incidentresponsplan

Zonder plan gaat de eerste, cruciale tijd verloren aan paniek en discussie.

Schrijf één A4 met: wie beslist, wie belt wie, welke systemen zet je offline en wie communiceert.

REAGEREN · PROCES

Afgesproken: IT-partner · tegen 15/9/2026

MFA op kritieke accounts

Zonder MFA volstaat een gestolen wachtwoord vaak om binnen te geraken.

Activeer MFA eerst op e-mail, cloudtoepassingen en administratoraccounts.

BESCHERMEN · TECHNOLOGIE

Afgesproken: Zaakvoerder en IT-partner · tegen 30/9/2026

Cyberverzekering duidelijk

Zonder duidelijkheid over verzekering weet je pas tijdens een incident of en hoe je gedekt bent.

Vraag je verzekeraar welke cyberincidenten gedekt zijn en wie je eerst moet contacteren.

HERSTELLEN · LEVERANCIERS

Afgesproken: IT-partner · tegen 15/10/2026

Phishing-bewustmaking

Veel incidenten starten met een medewerker die op een link klikt of een frauduleuze instructie volgt.

Organiseer een korte sessie over phishing en factuur- of CEO-fraude.

BESCHERMEN · MEDEWERKERS

Afgesproken: Directie · tegen 30/11/2026

90-dagenactieplan

Zicht op leveranciersactiviteit

Zonder zicht op leveranciersactiviteit merk je fouten of misbruik vaak pas veel later.

Vraag leveranciers met toegang tot systemen om logging of een periodiek activiteitenrapport.

DETECTEREN · LEVERANCIERS

Geschreven beleid

Zonder beleid hangen afspraken af van mondelinge gewoontes en individuele interpretatie.

Leg in één A4 de belangrijkste afspraken vast rond wachtwoorden, toegang, AI-gebruik, updates en meldingen.

GOVERNANCE · PROCES

Voldoende logretentie

Zonder voldoende loghistoriek is het moeilijk om te begrijpen wat er gebeurd is en welke data geraakt werd.

Vraag je IT-leverancier hoe lang logs van e-mail, cloud, firewall en endpoints bewaard blijven.

DETECTEREN · TECHNOLOGIE

Kritieke processen in kaart

Zonder zicht op kritieke processen weet je niet waar de grootste bedrijfsimpact zit.

Maak een korte lijst van de processen die maximaal één dag mogen stilliggen.

GOVERNANCE · PROCES

Communicatieverantwoordelijke

Ongecoördineerde communicatie kan vertrouwen schaden en juridische problemen vergroten.

Leg vast wie extern communiceert en wie berichten eerst goedkeurt.

REAGEREN · PROCES

7 Routekaart — komende 12 maanden

Evaluatie na incident

Zonder evaluatie blijven dezelfde zwakke plekken bestaan.

Plan na elk incident of bijna-incident een korte evaluatie: oorzaak, impact, verbeteractie, eigenaar.

HERSTELLEN · PROCES

Geoefende respons (tabletop)

Een plan dat nooit geoefend is, werkt vaak niet zoals verwacht.

Organiseer een korte tabletop-oefening van 45 minuten met directie en IT.

REAGEREN · PROCES

Jaarlijkse risicoanalyse

Zonder periodieke risicoanalyse investeer je mogelijk in de verkeerde maatregelen.

Plan jaarlijks één moment om de belangrijkste cyberrisico's opnieuw te beoordelen.

IDENTIFICEREN · PROCES

Managementopvolging

Zonder opvolging op managementniveau verdwijnt cybersecurity snel onderaan de prioriteitenlijst.

Zet cybersecurity jaarlijks op de agenda met een korte status: risico's, acties en openstaande beslissingen.

GOVERNANCE · PROCES

8 Vragen voor je IT-leverancier

Deze eerste vragenlijst helpt om belangrijke technische en organisatorische afspraken te verifiëren. Vraag bij antwoorden waar mogelijk om aantoonbare informatie, zoals een testdatum, rapport, overzicht of procedure.

Praktische tip: laat je leverancier per vraag aangeven wat volledig, gedeeltelijk of nog niet is afgedekt, wie eigenaar is van een verbeteractie en tegen wanneer die wordt uitgevoerd.

1. Welke diensten, systemen en gegevens beheren jullie voor ons, en wie is operationeel en contractueel verantwoordelijk?
2. Is MFA actief voor alle externe, beheer- en leverancierstoegang, en worden gedeelde accounts vermeden?
3. Hoe worden administratorrechten en de toegang van jullie medewerkers toegekend, periodiek nagekeken en ingetrokken bij functiewijziging of vertrek?
4. Hoe worden beveiligingsupdates en kritieke patches opgevolgd, getest en binnen welke termijnen toegepast?
5. Welke beveiliging en monitoring zijn actief op toestellen, servers, e-mail en cloudomgevingen, en wie volgt waarschuwingen op?
6. Hoe vaak worden back-ups gemaakt, hoelang worden ze bewaard en hoe zijn ze beschermd tegen wijziging, verwijdering en ransomware?
7. Wanneer werd voor het laatst een volledig herstel getest, wat was het resultaat en binnen welke termijn kunnen de belangrijkste systemen worden hersteld?
8. Welke relevante logs worden verzameld en bewaakt, hoelang worden ze bewaard en kunnen ze bij een incident ter beschikking worden gesteld?
9. Wat is jullie bereikbaarheid, responstijd en escalatieprocedure bij een vermoed cyberincident, en binnen welke termijn informeren jullie ons?
10. Welke systemen of diensten zijn vanaf het internet bereikbaar en hoe worden kwetsbaarheden daarop periodiek opgespoord en verholpen?
11. Welke onderdelen zijn vandaag volledig, gedeeltelijk of nog niet aantoonbaar afgedekt, en welk bewijs of rapport kan dit onderbouwen?
12. Welke drie concrete verbeteringen stellen jullie voor de komende 90 dagen voor, met eigenaar en streefdatum?

Een diepgaandere leveranciersbeoordeling nodig?

InfoSafety kan op aanvraag en tegen betaling een uitgebreidere leveranciersvragenlijst bezorgen en de antwoorden verwerken in een gestructureerd rapport. Dat rapport kan als bijlage of onderbouwing worden opgenomen in het informatieveiligheidsbeleid en als basis dienen voor verdere afstemming, verbeterafspraken en opvolging met de leverancier. Aanvragen kan via info@infosafety.be.

9 Praktische incidentfiche

Vul de contactgegevens vooraf in, bewaar een afgedrukte kopie en noteer tijdens een incident alle belangrijke acties en beslissingen.

A. Eerste vaststellingen

Datum en tijd ontdekking:

Melder en contactgegevens:

Vermoed type incident:

Eerste signaal of melding:

Getroffen systemen/toestellen:

Mogelijk getroffen gegevens:

Bedrijfsimpact/stilstand:

Huidige status: [] actief [] ingedamd [] hersteld

B. Contactlijst

Interne incidentleider/beslisser:

IT-/securityleverancier:

DPO/privacycontact:

Verzekeraar + polisnummer:

Juridisch adviseur:

Communicatieverantwoordelijke:

Directie/bestuur:

Alternatief noodnummer:

C. Eerste acties

1. Noteer tijdstip, melder, symptomen en reeds uitgevoerde handelingen.
2. Contacteer de IT-/securityleverancier en wijs één interne incidentleider aan.
3. Herstart, wis of herstel systemen niet zonder afstemming; voorkom verlies van bewijs.
4. Isoleer getroffen toestellen of accounts gecontroleerd wanneer verdere verspreiding dreigt.
5. Bewaar relevante e-mails, screenshots, logs, meldingen en tijdstippen.
6. Bepaal welke systemen, processen, gegevens en externe partijen mogelijk geraakt zijn.
7. Leg elke belangrijke actie, beslissing, verantwoordelijke en het resultaat vast.
8. Beoordeel samen met privacy/juridisch of meldplichten en termijnen van toepassing zijn.
9. Controleer de voorwaarden van de cyberverzekering vóór externe expertise wordt besteld.
10. Stem interne en externe communicatie centraal af en vermijd ongecoördineerde boodschappen.

D. Mogelijke meldingen en communicatie

- ☐ Persoonsgegevens mogelijk geraakt: ja / nee / onbekend
- ☐ Datalekbeoordeling gestart
- ☐ NIS2/CCB-meldplicht beoordeeld indien van toepassing
- ☐ Verzekeraar geïnformeerd volgens polisvoorwaarden
- ☐ Klanten/partners informeren: beslissing vastgelegd
- ☐ Medewerkersinstructie of waarschuwing verspreid

E. Beslis- en actielog

Tijdstip	Actie of beslissing	Door wie

10 Type aandachtspunten

De meeste aandachtspunten zitten bij leveranciers en externe partijen.

Proces
10/20

Technologie
5/10

Medewerkers
3/5

Leveranciers
4/5

Wil je hulp bij de uitvoering?

Dit rapport is bedoeld om zelf mee aan de slag te kunnen. Wil je begeleiding bij het uitwerken, prioriteren of opvolgen van de acties, dan kan InfoSafety helpen op drie niveaus.

Op basis van deze scan lijkt vooral **InfoSafety Bestuur** relevant, maar dit blijft optioneel.

InfoSafety Start

2.950 €

eenmalig

De basis op orde — beleid, rollen en een concrete roadmap.

InfoSafety Groei

595 €

per maand

Begeleiding bij de uitvoering, het hele jaar door.

AANBEVOLEN

InfoSafety Bestuur

1.250 €

per maand

Virtuele CISO — voor bedrijven die het structureel willen aanpakken.

Richtprijzen, excl. btw. Het definitieve voorstel hangt af van bedrijfsgrootte en scope.

De scan geeft richting en is geen formele audit, CyFun-verificatie of certificering.

[Privacy](#) · [Disclaimer](#) · [Contact](#)