dijkzeker

Maandrapport beveiliging

Hendriks Installatietechniek B.V.

Oktober 2026

Pakket Compleet

Er is actie nodig

Per onderdeel zie je eerst de cijfers en daarna wat er moet gebeuren. Wij nemen contact met jullie op om het samen op te lossen.

Wachtwoorden

Actie nodig

Beveiligingsscore 76%

Browser

Let op

1180 keer tegengehouden, 2 keer toch doorgegaan

Bewaking

Actie nodig

92% van de Microsoft 365-controles in orde, 1 kritiek

Bewustzijn

In orde

8,3% klikte op een oefenmail

Compliance

Actie nodig

64% van de controlepunten aangetoond

E-mail

Let op

Domeinscore 10/10, risico laag

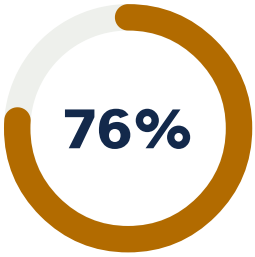
WACHTWOORDEN

Hoe veilig zijn jullie wachtwoorden?

Jullie bewaren wachtwoorden in een versleutelde wachtwoordkluis. Wij zien niet wat erin staat, alleen hoe sterk de wachtwoorden zijn en of ze in een datalek voorkomen.

Wachtwoordkluis

Actie nodig



Beveiligingsscore

Sterke en unieke wachtwoorden en tweestapsverificatie

11 van 12
collega's gebruiken de kluis

2
in een datalek

17
op meer plekken gebruikt

1
zonder tweestapsverificatie

Sterkte van 486 wachtwoorden

87% sterk



421 sterk · 43 redelijk · 22 zwak

Zo maken we het beter

1. 2 wachtwoorden komen voor in bekende datalekken. Wijzig ze zo snel mogelijk.
2. De beveiligingsscore van de wachtwoordkluis is 76 van de 100. Die score kijkt naar sterke en unieke wachtwoorden en of tweestapsverificatie aanstaat. Met de punten hieronder gaat hij omhoog.
3. 1 collega heeft de uitnodiging voor de wachtwoordkluis nog niet geaccepteerd.
4. 22 wachtwoorden zijn zwak. Laat de kluis een sterk wachtwoord maken en vervang ze.
5. 17 wachtwoorden worden op meer plekken gebruikt. Als één site lekt, zijn de andere dan ook open.

6 1 gebruiker heeft geen tweestapsverificatie op de kluis. Zet die aan met een app op de telefoon.

7 1 gebruiker heeft de afgelopen 30 dagen niet ingelogd in de kluis.

Stand van 26-10-2026

BROWSERBESCHERMING

Wat hield de browserbeveiliging tegen?

Op de werkplekken draait een beveiliging in de browser. Die houdt nepsites, gevaarlijke downloads, advertenties met verborgen code en het delen van gevoelige gegevens (bijvoorbeeld in een AI-chat) tegen, of waarschuwt eerst.

Browserbeveiliging

Let op



Risico weggenomen
van alles wat is gesignaleerd

1180 keer tegengehouden

21 keer gewaarschuwd

2 keer toch doorgegaan na een waarschuwing

1240 meldingen in totaal

12 beschermde browsers

148 websites gecontroleerd

Waar ging het over?

Onderwerp	Meldingen
Advertenties en volgscripts	1012
Phishing en nep-inlogpagina's	96
Niet-goedgekeurde clouddiensten	71
Gevoelige gegevens in AI-chats	9
Wachtwoordregels	6

Hoe veilig wordt er ingelogd op websites?

84 score veilig inloggen (van 100)	**412** keer ingelogd op een website	**381** met tweestapsverificatie of Microsoft-inlog
31 zonder tweestapsverificatie	**9** met een zwak wachtwoord	**0** met een uitgelekt wachtwoord

Zo maken we het beter

1. 2 keer ging iemand toch door na een waarschuwing van de browserbeveiliging. We kijken samen welke sites dat waren en of ze op de blokkeerlijst moeten.
2. Bij 31 van de 412 keer inloggen op een website werd geen tweestapsverificatie gebruikt. Zet die aan bij de diensten waar dat kan, te beginnen met boekhouding, bank en webshop.
3. 9 keer werd ingelogd met een zwak wachtwoord. Laat de wachtwoordkluis voor die websites een sterk wachtwoord maken.

Periode 01-10 tot en met 26-10-2026

BEWAKING

Staan Microsoft 365 en de apparaten veilig ingesteld?

We controleren elke dag de beveiligingsinstellingen van Microsoft 365, de updates op de apparaten en wat er van buitenaf zichtbaar is. Verdachte activiteit, zoals een inlogpoging vanuit het buitenland, krijgen we direct te zien.

Bewaking

Actie nodig



Microsoft 365

166 van 180 controles in orde

1 kritieke punten

5 punten met hoge prioriteit

4 meldingen van verdachte activiteit deze maand

1 accounts in een datalek

3 ontbrekende updates op apparaten

2 zwakke plekken vanaf internet

Per onderdeel

Onderdeel	Open	Kritiek	Hoog
Microsoft 365-instellingen	14	1	4
Updates op Windows-apparaten	3	0	1
E-mailinstellingen	2	0	0
Bereikbaar vanaf internet	2	0	0

Belangrijkste open punten in Microsoft 365

- Zorg dat alle beheerders phishing-bestendige MFA gebruiken
- Blokkeer verouderde aanmeldmethoden (legacy authenticatie)
- Schakel het automatisch doorsturen van e-mail naar externe adressen uit
- Beperk het delen van bestanden met externe gebruikers tot bekende domeinen

Meest gemelde activiteit: Inlogpoging vanuit het buitenland (2), Verdachte doorstuurregel (1), Phishingmail gemeld door medewerker (1)

Zo maken we het beter

1. 1 account van jullie komt voor in een recent datalek. Wijzig het wachtwoord direct en controleer of tweestapsverificatie aanstaat.
2. Er staat 1 kritiek punt open. Die pakken we als eerste op.
3. Er staan 5 punten met hoge prioriteit open.
4. Op de apparaten ontbreken 3 beveiligingsupdates. Zorg dat computers automatisch bijwerken en af en toe opnieuw opstarten.
5. Vanaf internet zijn 2 zwakke plekken gevonden, bijvoorbeeld een verouderd certificaat of een open poort.

Stand van 26-10-2026

BEWUSTZIJN

Herkennen collega's een nepmail?

Medewerkers krijgen korte lessen en af en toe een onschuldige oefenmail die op phishing lijkt. Zo leren ze nepmail herkennen en melden.

Training en oefenmails

In orde

12 medewerkers in training	**78** gemiddelde score op de lessen	**12** oefenmails verstuurd
1 keer op de link geklikt	**0** keer gegevens ingevuld	**7** keer netjes gemeld

Stand van 26-10-2026

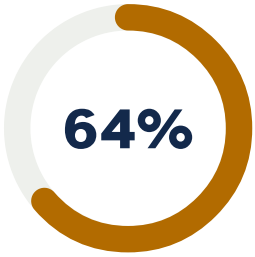
COMPLIANCE

Hoe ver zijn jullie met de normen?

Per norm staan controlepunten. Bij elk punt leggen we vast hoe het geregeld is, met bewijs. Zo kunnen jullie het laten zien aan een klant, verzekeraar of auditor.

Voortgang

Actie nodig



Aangetoond

61 van 96 controlepunten

24 normen	**9** open taken
0 taken over de deadline	**1** hoge risico's (van 14)

Zo maken we het beter

1. Bij 61 van de 96 controlepunten is aangetoond dat het geregeld is (63,5%). We werken de rest stap voor stap samen af.
2. 1 risico is na maatregelen nog hoog. Kies per risico: extra maatregel of bewust accepteren.

Stand van 26-10-2026

E-MAILBEVEILIGING

Kan iemand mailen uit jullie naam?

We controleren elke dag of mail die namens jullie domein wordt verstuurd echt van jullie komt, en of vervalste mail wordt tegengehouden.

Domeinbewaking voor: **hendriks-voorbeeld.nl** Let op



Domeinscore

Risico laag

DMARC — In orde
Beleid voor vervalste mail: weigeren

SPF — In orde
Wie mag namens jullie mailen

DKIM — In orde
Digitale handtekening onder jullie mail

Goed herkend — 97%
742 mails in 7 dagen

MTA-STS — Testmodus
Versleuteling tussen mailservers staat nog in testmodus

Zwarte lijsten — In orde
Mailservers staan niet op een blokkadelijst

Wat betekent dit?

Kan iemand mailen uit jullie naam?
Nee. Mail die zich voordoet als jullie (bijvoorbeeld een nepfactuur) wordt door de ontvanger geweigerd.

Komt jullie eigen mail goed aan?
Bijna altijd. Alleen mail via Exact Online werd niet herkend en kan bij de ontvanger worden geweigerd.

Probeerde iemand jullie na te doen?
Ja, 38 keer kwam er mail van onbekende afzenders die zich als jullie voordeden. Die is door de ontvangers geweigerd.

01-10 Goed herkende mail per dag (0 tot 100%) 26-10

Mailverkeer oktober 2026 (01-10 t/m 26-10)

2.582
mails verstuurd namens jullie

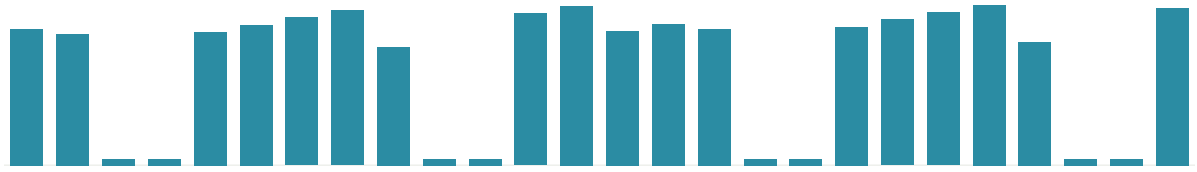
2.407
goed herkend

96
doorgestuurd door ontvangers

41
afgekeurd (niet herkend)

38
vervalsingspogingen

52
geweigerd door ontvangers, 9 in spam



01-10 Mails per dag (hoogste dag: 158) 26-10

Wie mailt namens jullie?

Dienst	Goed	Doorgestuurd	Afgekeurd	Status
Microsoft 365	2.239	96	0	In orde
Exact Online	168	0	41	Let op
Onbekende afzenders (mogelijk vervalsing)	0	0	38	Tegengehouden

Ontvangen door: Microsoft 365 (1.498), Google (Gmail) (439), Outlook.com (284), KPN (129), Ziggo (77)

Afgekeurde mail kwam uit: Nederland (34), Verenigde Staten (19), Duitsland (11), China (8), Rusland (7)

Zo maken we het beter

1. Exact Online verstuurde 41 mails namens jullie die niet goed werden herkend. Het gaat om een klein aantal, maar zijn het bijvoorbeeld facturen of meldingen, dan komen die niet aan. Wij zoeken uit wat het is en melden de dienst zo nodig aan.

2. Versleuteling tussen mailservers (MTA-STS) staat nog in testmodus. Als de rapporten schoon zijn, zetten we hem op afdwingen.