SECURITY ASSESSMENT · CONFIDENTIAL

Havenzicht Logistics B.V.

REPORT NUMBER	VERSION	ASSESSMENT PERIOD	CLIENT
EBO-2026-014	1.0 — final	12–16 January 2026	Managing Director
LOCATIONS	**CLASSIFICATION**	**FINDINGS**	
NL · BE · DE	Confidential	2 (1 critical)	

Commissioned following: Supplier security questionnaire from a major customer

1 Executive summary

Havenzicht Logistics asked us to establish what the organisation looks like from the internet: which systems are reachable from outside, and what an attacker could do with them. The assessment follows the security questionnaire received from a major customer in November.

The headline is a single finding. A Windows server with Remote Desktop enabled is reachable directly from the internet with no second authentication factor. This is how most ransomware incidents at companies of this size begin: attackers scan continuously for exactly this port and try passwords automatically. While it remains open, the risk of an incident is not theoretical.

Three further findings carry a high rating, two of which can be resolved with existing licences at no additional cost — most importantly the absence of multi-factor authentication on the Microsoft 365 administrator accounts.

The overall picture is not unusual for an organisation of this size without a dedicated security function. These weaknesses accumulated through growth and deferred maintenance rather than negligence. The four most serious findings can be resolved within two weeks, largely by the current IT partner, and doing so removes the great majority of the risk.

2 Risk at a glance

1
CRITICAL

1
HIGH

ID	FINDING	SEVERITY	EFFORT	OWNER	PHASE
BEV-01	Remote Desktop reachable directly from the internet	CRITICAL	Low	IT partner	1
BEV-02	No multi-factor authentication on Microsoft 365 administrator accounts	HIGH	Low	IT partner	1

3 Scope and authorisation

IP RANGES	198.51.100.16/28, 203.0.113.40/29
DOMAINS	havenzicht-example.eu
CLOUD	Microsoft 365 tenant (configuration review only)
SOURCE ADDRESS	192.0.2.77
EXCLUDED	Internal networks · OT and warehouse systems · Social engineering · Denial of service · Active exploitation
AUTHORISATION	Engagement letter, 8 January 2026
SIGNED BY	Managing Director, 8 January 2026

The assessment was non-intrusive. Weaknesses were identified and verified by observation only; none was exploited, no data was accessed or altered, and no system was taken out of service. Everything described below was carried out from the source address named above, within the agreed scope and under the written authorisation referenced above.

4 Findings

BEV-01 Remote Desktop reachable directly from the internet

CRITICAL

WHAT WE FOUND

Port 3389 (Remote Desktop) on the terminal server is open to the entire internet. There is no VPN in front of it and no second authentication factor. The login screen discloses the Windows domain name.

EVIDENCE

```
198.51.100.24  3389/tcp  open  ms-wbt-server
 domain : HAVENZICHT
 NLA    : disabled
 MFA    : not detected
```

WHY IT MATTERS

Automated attacks scan for this type of port continuously. One working password — leaked from a breach elsewhere or guessed — grants direct access to a server inside the corporate network. This is the most common entry route for ransomware in mid-sized companies. A successful attack would be expected to halt order processing for several days.

RECOMMENDATION

Close port 3389 at the firewall today. Provide access exclusively through the VPN (see BEV-04) with multi-factor authentication. If external access must remain available in the short term, restrict it to known source addresses and enable Network Level Authentication.

CVSS V3.1

9.8 — AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EFFORT

Low — about 2 hours, IT partner

OWNER

IT partner

BEV-02

No multi-factor authentication on Microsoft 365 administrator accounts

HIGH

WHAT WE FOUND

Five accounts hold the Global Administrator role. None of them has multi-factor authentication enforced. Legacy authentication protocols remain enabled, which would allow MFA to be bypassed even once configured.

EVIDENCE

```
Global administrators : 5
MFA enforced          : 0 of 5
Legacy auth           : permitted
Conditional access    : no policy active
```

WHY IT MATTERS

An administrator account grants access to all company mail and documents, and can be used to intercept and alter invoices. It is also a question asked by virtually every supplier security questionnaire.

RECOMMENDATION

Enforce MFA on all administrator accounts, disable legacy authentication, and reduce the number of global administrators to two. Then roll MFA out to all staff in stages. This is covered by the existing licences.

CVSS V3.1

8.1 — AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

EFFORT

Low — about 4 hours, no additional cost

OWNER

IT partner

5 Three-phase plan

Phase 1 — immediately

Four actions that together remove the largest part of the risk. All four can be carried out by the current IT partner without investment in new tooling.

ID	ACTION	OWNER	EFFORT
BEV-01	Remote Desktop reachable directly from the internet	IT partner	Low
BEV-02	No multi-factor authentication on Microsoft 365 administrator accounts	IT partner	Low

6 Mapping to standards and regulation

Each finding below is tied to the control it bears on, so a supplier questionnaire or audit request can be answered directly from this table.

ID	FINDING	ISO 27001	NIS2
BEV-01	Remote Desktop reachable directly from the internet	A.8.20 Network security	(j) Multi-factor authentication and secure access
BEV-02	No multi-factor authentication on Microsoft 365 administrator accounts	A.8.5 Secure authentication	(j) Multi-factor authentication and secure access

7 Next steps

A report is a snapshot. Systems change, certificates expire and new weaknesses appear. We recommend a retest six weeks after delivery, confirming in writing that phases 1 and 2 are complete — which is precisely the evidence your customer is asking for. After that, a quarterly scan keeps the picture current.