vallocor
SECURITY ENGINEERING

Guard the heart of your business.

External Security Check

Plain-language overview of your email security, certificates, subdomains, and open ports

CHECKED DOMAIN	TIME OF CHECK	REPORT ID	EUROPEAN CHECK NODE
vandijk-manufacturing.example	**2026-11-21 10:15 UTC**	**VAL-EXAMPLE**	**probe-nl-01.vallocor-edge.eu**

64 / 100
SECURITY SCORE

A Few Doors Left Ajar

Your website is reachable over HTTPS, but a few settings around email spoofing protection, old subdomains, or browser security headers can be tightened easily by your IT supplier.

ENISA BASELINE • NIS2 ART. 21(2) • ISO/IEC 27001:2022

Why These Basics Matter for Your Business (and Your Customers)

Automated scanners sweep the internet day and night looking for open login ports, forgotten test pages, and company domains that criminals can use to send fake invoices in your name. Larger customers, auditors, and cyber-insurers also increasingly ask for simple proof that these fundamentals are locked down.

What We See from the Outside

EMAIL & DOMAIN

Mail Platform (MX)	**Microsoft 365**
Approved Mail Servers (SPF)	**SoftFail (~all) (4/10)**
Fake Email Blocking (DMARC)	**None (Monitor)**
Encrypted Mail (MTA-STS)	**Missing**
Domain Signature (DNSSEC)	**In Place**
Certificate Lock (CAA)	**Missing**

WEBSITE & CERTIFICATES

Connection Encryption (TLS)	**TLS 1.3**
Certificate Valid For	**62 days**
Forced HTTPS (HSTS)	**Missing**
Browser Script Guard (CSP)	**Missing**
Security Contact (security.txt)	**Missing**
Visible Server Version	**Hidden**

HOSTING, SUBDOMAINS & PORTS

Hosting Provider (ASN)	**EU Hosting (NL)**
IPv6 Reachability	**In Place**
Subdomains (live / total)	**5 / 5**
Test, Admin or Orphan Hosts	**1**
Open Admin Ports	**1**
Known CVEs on IP	**0**

Concrete Fixes for You and Your IT Supplier

These items were checked safely from the outside without touching or disrupting your systems. You can hand this page straight to your internal IT manager or external IT partner.

1. Email protection (DMARC) is only watching, not blocking fake emails

IMPORTANT

Guideline: ENISA Anti-Phishing • NIS2 Art. 21(2) • ISO/IEC 27001:2022 A.8.23

```
What We Saw: _dmarc.vandijk-manufacturing.example -> v=DMARC1; p=none;
```

What Your IT Supplier Can Do: DMARC is present, but setting 'p=none' still lets fake emails sent in your name reach your customers. Ask your IT supplier to tighten the rule to 'p=quarantine' or 'p=reject'.

2. Admin login port (such as SSH or firewall management) is publicly reachable

IMPORTANT

Guideline: ENISA Secure Access • NIS2 Art. 21(2) • ISO/IEC 27001:2022 A.8.5

```
What We Saw: 198.51.100.42:8443/tcp (HTTPS admin portal reachable from internet)
```

What Your IT Supplier Can Do: Admin ports should not be open to the entire internet. Ask your IT supplier to restrict access to fixed office/VPN IP addresses and disable plain password logins.

3. Test, staging, or admin subdomains are publicly visible

ATTENTION

Guideline: ENISA Subdomain Hygiene • NIS2 Art. 21(2) • ISO/IEC 27001:2022 A.8.31

```
What We Saw: test-old.vandijk-manufacturing.example (active login page)
```

What Your IT Supplier Can Do: Forgotten test sites and admin portals are often left unpatched and give attackers an easy side door. Review these subdomains with your IT supplier: remove unused ones and put internal tools behind a VPN.

Want to Walk Through This Together or Fix It Hands-On?

Vallocor puts an independent European watchpost and an experienced specialist next to you and your IT supplier: from 24/7 outside monitoring (Outpost €149/mo) and internal server/firewall monitoring via the CollectorBox (Sentinel €490/mo) to monthly hands-on engineering hours (Bastion €1,490/mo). One-off baseline assessments and cleanup projects are also available at €175/hr.

Questions about this report? Email hello@vallocor.eu or visit https://vallocor.eu