Cybervagten

Ekstern sikkerhedsrapport

Virksomhed: Company
Domæne: company.example
Scandato: 27-09-2026 10:44 UTC

Sikkerhedsscore	72/100
Critical	0
High	0
Medium	0
Low	7

Rapporten viser, hvad udenforstående kan se om virksomhedens offentlige IT-infrastruktur. Den er baseret på konservative, ikke-destruktive kontroller.

Executive Summary

Den indledende scanning viser flere forhold, som bør forbedres for at reducere risikoen. Der er 0 prioriterede fund, som bør gennemgås af virksomhedens web-, DNS- eller email-leverandør.

Prioriteret handlingsplan

1. Content-Security-Policy mangler
Hvad betyder det: Headeren Content-Security-Policy blev ikke fundet
Anbefaling: Tilføj headeren i webserveren eller applikationen.

2. Strict-Transport-Security mangler
Hvad betyder det: Headeren Strict-Transport-Security blev ikke fundet
Anbefaling: Tilføj headeren i webserveren eller applikationen.

3. X-Content-Type-Options mangler
Hvad betyder det: Headeren X-Content-Type-Options blev ikke fundet
Anbefaling: Tilføj headeren i webserveren eller applikationen.

4. Referrer-Policy mangler
Hvad betyder det: Headeren Referrer-Policy blev ikke fundet
Anbefaling: Tilføj headeren i webserveren eller applikationen.

5. X-Frame-Options mangler
Hvad betyder det: Headeren X-Frame-Options blev ikke fundet
Anbefaling: Tilføj headeren i webserveren eller applikationen.

6. Frame-beskyttelse mangler i CSP
Hvad betyder det: CSP mangler frame-ancestors
Anbefaling: Tilføj frame-ancestors eller X-Frame-Options for at mindske clickjacking-risiko.

7. DNSSEC ser ikke ud til at være aktivt
Hvad betyder det: Ingen DNSKEY/DS fundet
Anbefaling: Aktiver DNSSEC hos DNS-udbyderen hvis det understøttes.

Website Security

Ingen særskilte fund i denne kategori.

Domain/DNS Security

DNSSEC ser ikke ud til at være aktivt
Alvorlighed: Low
Hvad blev fundet: Ingen DNSKEY/DS fundet
Hvorfor det betyder noget: Det ser ud til, at DNSSEC ikke er aktivt, hvilket kan gøre dit domæne mere sårbart over for angreb. Aktivér DNSSEC hos din DNS-udbyder, hvis det er muligt, for at forbedre sikkerheden.
Anbefaling: Aktiver DNSSEC hos DNS-udbyderen hvis det understøttes.

Email Security

Ingen særskilte fund i denne kategori.

External Attack Surface / OSINT

Ingen særskilte fund i denne kategori.

Detected Services

Offentligt synlige services fundet

Alvorlighed: Informational

Hvad blev fundet: 8080, 8443

Hvorfor det betyder noget: Der er fundet offentligt synlige services på porte 8080 og 8443. Bekræft, at disse services er nødvendige, opdaterede og begræns adgangen, hvor det er muligt, for at reducere angrebsfladen.

Anbefaling: Bekræft at alle synlige services er nødvendige, opdaterede og begrænset hvor muligt.

Positive Findings

Ingen særskilte fund i denne kategori.

Detekterede teknologier

Microsoft-HTTPAPI på autodiscover.company.example

Version: 2.0 (high sikkerhed i detektionen).

ASP.NET på company.example

Version: ukendt eller ikke bekræftet. Der knyttes derfor ingen kendt sårbarhed til dette fund.

Cloudflare på company.example

Version: ukendt eller ikke bekræftet. Der knyttes derfor ingen kendt sårbarhed til dette fund.

ASP.NET på www.company.example

Version: ukendt eller ikke bekræftet. Der knyttes derfor ingen kendt sårbarhed til dette fund.

Cloudflare på www.company.example

Version: ukendt eller ikke bekræftet. Der knyttes derfor ingen kendt sårbarhed til dette fund.

Kendte sårbarheder

Ingen kendte sårbarheder blev matchet til en bekræftet produktversion i de anvendte åbne sårbarhedsdata. Det er ikke en garanti for, at ingen sårbarheder findes.

Offentlig angrebsflade

Fundne offentlige IP-adresser: 10. Fundne subdomæner: 2. Synlige services: 9. Login-/admin-endpoints: 2.

Løbende overvågning

Cybervagten overvåger nu domænet hvert 15. minut og udfører en dybere kontrol én gang dagligt. Der sendes kun email, når der registreres en relevant ændring eller et nyt problem, så kendte uændrede forhold ikke gentages unødigt.

Tekniske noter

{'dns': {'a': ['192.0.2.184', '192.0.2.54'], 'aaaa': [], 'caa': [], 'dnssec': False, 'ns': ['ns.scannet2.dk.', 'ns2.scannet2.dk.'], 'txt': ['MS=ms77229151', 'atlassian-domain-verification=bqViFxVPcLhkTciRS5xxZT4bOcmUfs4imej34zdn4GOXJicAHHUD0HrXuiqct228', 'atlassian-sending-domain-verification=e0be1127-7a1a-42cc-9c7a-1b8f8493db79', 'google-site-verification=fW2N-UZfoTmL_xBE2VNnRiPHtMy6hZgIEzIJoWLUtbA', 'v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net include:spf.onlinemail.io include:spf.curanet.dk include:smtp1.newwweb.dk -all']}, 'email': {'dkim_note': 'DKIM selector cannot be reliably discovered without knowing the sender selector.', 'dmarc': ['v=DMARC1; p=none; rua=mailto:Company@company.example;'], 'mx': ['1 Company-com.mail.protection.outlook.com.'], 'spf': ['v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net include:spf.onlinemail.io include:spf.curanet.dk include:smtp1.newwweb.dk -all']}, 'tls': {'available': True, 'days_left': 44, 'expires_at': '2026-11-10T14:25:04+00:00', 'issuer': 'countryName=US, organizationName=Google Trust Services, commonName=WE1', 'version': 'TLSv1.3'}, 'open_ports':

[80, 443, 8080, 8443], 'subdomains': {'autodiscover.company.example': ['192.0.2.105', '192.0.2.121', '192.0.2.137'], 'www.company.example': ['192.0.2.184', '192.0.2.54']}}