

# IT-Infrastruktur-Audit

## Sicherheits- & Technologie-Analyse

muster-gmbh.de

Analysiert fuer: Muster GmbH (Beispiel)

Erstellungsdatum: 03.05.2026 10:56

### ZUSAMMENFASSUNG DER BEFUNDE



Mangelhaft

38

/ 100

SICHERHEITS-SCORE

Dieser Bericht basiert auf passiver Analyse oeffentlich zugaeuglicher Informationen. Alle Angaben ohne Gewaehr. Nicht weitergeben.

## Management-Zusammenfassung

	Bereich	Details
✓	SSL / TLS	Note B, gültig noch 82 Tage
✗	E-Mail-Sicherheit	SPF ✗ · DMARC ✗
✓	Security-Header	0 vorhanden, 0 fehlen
✓	DSGVO / Tracking	Keine Verstöße
✗	Datenschutz	Verbesserungsbedarf
✗	WAF-Schutz	Keine WAF erkannt
✗	Offene Ports	3 kritische Ports offen
✗	Performance	Nicht geprüft

### Kritische Handlungsempfehlungen:

#### 1. DMARC-Record nicht gesetzt

Es ist kein DMARC-Record für die Domain konfiguriert. Angreifer können E-Mails im Namen Ihrer Domain versenden (CEO-Fraud, Phishing).  
· DMARC-Record mit `p=quarantine` starten, nach 4 Wochen auf `p=reject` erhöhen.

#### 2. Port 3389 (RDP) öffentlich erreichbar

Remote Desktop Protocol auf Port 3389 ist von extern erreichbar — typisches Einfallstor für Ransomware-Gruppen. · RDP nur über VPN exponieren oder per Firewall auf bekannte IPs einschränken.

Kostenrisiko: Einfallstor für Cyberangriffe – Ø 200.000 € Schaden bei KMU

#### 3. CVE-2024-XXXX in eingesetzter Software (kritisch)

Erkannte Software-Version weist eine kritische, aktiv ausgenutzte Schwachstelle auf (CVSS 9.8). · Hersteller-Patch sofort einspielen, ggf. WAF-Rule als Übergangslösung.

#### 4. Content-Security-Policy fehlt

Keine CSP-Header gesetzt. XSS-Angriffe können browserseitig nicht blockiert werden. · Restriktive CSP mit `default-src 'self'` einführen.

#### 5. SPF-Record verwendet Soft-Fail (~all)

SPF endet mit `~all` statt `-all` — empfangende Mailserver behandeln gefälschte Mails nicht strikt. · SPF auf `-all` stellen, vorher alle legitimen Versand-Wege prüfen.

### Entwicklung seit letztem Audit:

	Vorheriger Scan	Aktueller Scan	Veränderung
Score	52/100	38/100	▼ -14
Datum			

## Inhaltsverzeichnis

1. Analyseumfang & Hinweise
2. Infrastruktur-Übersicht & Netzwerk-Topologie
3. Domain & Hosting
4. DNS-Konfiguration
5. E-Mail-Sicherheit
6. SSL/TLS-Analyse & Sicherheits-Header
7. Erweiterte Sicherheitsprüfungen
8. Technologie-Stack & DSGVO
9. Port-Scan & Angriffsfläche
10. Sicherheits-Radar
11. DSGVO & Compliance
12. Maßnahmenplan
13. Handlungsempfehlungen (Detail)
14. Nächste Schritte – Ihr Aktionsplan
15. Begriffe, Abkürzungen & Lösungshinweise

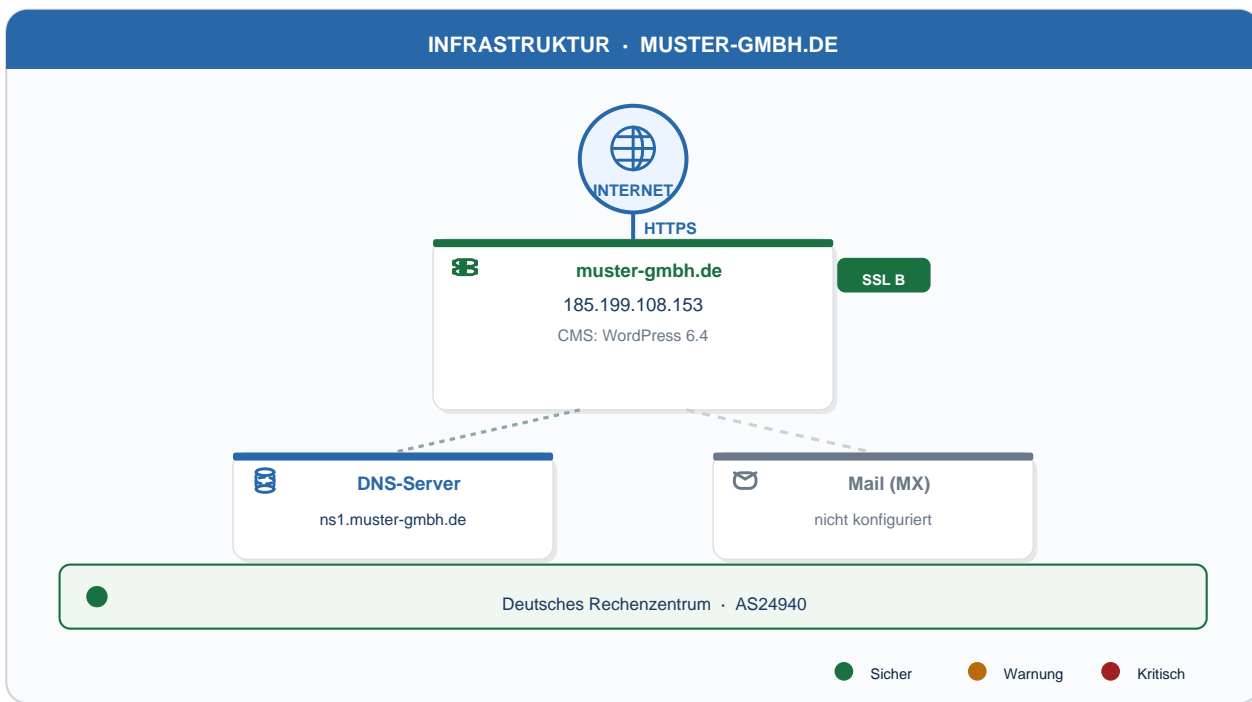
Hinweis: Die Seitenzahlen sind dynamisch und hängen vom Umfang der Analyseergebnisse ab.

## Analyseumfang & Hinweise

Analysierte Adresse	muster-gmbh.de
Analyse-Zeitpunkt	03.05.2026 10:56
Art der Analyse	Passive Analyse öffentlich zugänglicher Informationen (DNS, HTTPS, HTTP-Header, WHOIS, Zertifikat-Transparenz, Port-Scan der Haupt-IP)
Nicht erfasst	Interne Subnetze, weitere IP-Ranges oder Systeme in Kundenhoheit, VPN-Endpunkte, interne Anwendungen, Cloud-Instanzen, physische Infrastruktur, Endgeräte, Active Directory, sowie nicht öffentlich erreichbare Dienste.
Kein vollständiger Audit	<b>Wichtig:</b> Dieser Bericht ist eine erste automatische Analyse und ersetzt keinen vollständigen IT-Sicherheits-Audit oder ein Penetrationstesting. Für eine umfassende Bewertung ist ein qualifizierter Sicherheitsspezialist hinzuzuziehen. Alle Angaben sind unverbindlich und ohne Gewähr.

## Infrastruktur-Übersicht

Die folgende Skizze zeigt die öffentlich erkennbare IT-Infrastruktur von **muster-gmbh.de**. Sie basiert auf automatisierten DNS-, Port- und Web-Analysen der Haupt-Domain. Weitere Subnetze oder interne Systeme sind nicht Bestandteil dieser Darstellung.



■ 3 riskante Ports öffentlich erreichbar — Details siehe Abschnitt „Offene Ports“ weiter unten.

## Domain & Hosting

Domain	muster-gmbh.de
IP-Adresse	185.199.108.153
Reverse-DNS	static.muster-gmbh.de
Registrar	United Domains AG
Domain-Alter	2014-06-17
Ablauf in	2026-06-17
Aktualisiert	-
Name-Server	-
DNSSEC	Nicht aktiv
IPv6 (AAAA)	Nicht konfiguriert
Hosting-Anbieter	-
Standort	DE
ASN	AS24940
DSGVO-Hosting	Ausserhalb EU: DE

## DNS-Konfiguration

A-Records (IPv4)	185.199.108.153
AAAA-Records (IPv6)	Nicht vorhanden
NS-Records	ns1.muster-gmbh.de, ns2.muster-gmbh.de

CAA-Record	Nicht vorhanden – jede CA kann Zertifikate ausstellen
DNSSEC	Nicht aktiv

---

## E-Mail-Sicherheit

**E-Mail-Spoofing ist moeglich!** E-Mails im Namen dieser Domain koennen ohne technische Einschraenkung gefaelscht werden.

MX-Server	Kein Mail-Server
Mail-Anbieter	-
SPF-Record	Nicht vorhanden
SPF-Policy	none (schwach)
DMARC-Record	Nicht vorhanden
DMARC-Policy	Nicht vorhanden
Gesamt-Note	? –

---

## SSL/TLS-Analyse

Status	Gueltig
Protokoll	-
Cipher Suite	- (0 Bit)
Aussteller	Sectigo RSA Domain Validation
Zertifikat fuer	CN=muster-gmbh.de
Gueltig ab	-
Gueltig bis	2026-07-24 (noch 82 Tage)
HSTS	Nicht konfiguriert
SSL-Grade	B
SANs	-

---

## Sicherheits-Header

Header-Score: 0% (Note: ?)

---

## Erweiterte Sicherheitspruefungen

Diese Seite dokumentiert ergaenzende Sicherheitsmechanismen, die ueber die Basis-Konfiguration hinausgehen und fuer einen umfassenden Schutz der Infrastruktur empfohlen werden.

### HTTP-zu-HTTPS-Weiterleitung

Status	<b>x Keine automatische Weiterleitung – Besucher können unverschlüsselt verbinden</b>
HTTP-Status	–
Ziel-URL	–

### HSTS-Preload-Register

Status	<b>x Nicht im Preload-Register – HSTS-Schutz nur nach erstem Besuch aktiv</b>
Register-Status	–
Empfehlung	Eintragung unter <a href="https://hstspreload.org/">https://hstspreload.org/</a> beantragen.

### MTA-STS (Mail Transport Agent Strict Transport Security)

Status	<b>x MTA-STS nicht konfiguriert – E-Mail-Transport kann abgehört werden</b>
DNS-Record	<b>x Fehlt</b>
Policy-Datei	<b>x Fehlt</b>
TLS-Reporting	<b>x Nicht konfiguriert</b>

### security.txt (RFC 9116)

Status	<b>x Nicht gefunden – Sicherheitsforscher können keinen Kontakt aufnehmen</b>
URL	–
Ablaufdatum	–
Zweck	Ermöglicht Sicherheitsforschern, Schwachstellen verantwortungsvoll zu melden (Responsible Disclosure).

### Cookie-Sicherheits-Analyse

Keine Set-Cookie-Header beim Seitenaufruf gefunden.

## Technologie-Stack

Web-Server	nginx 1.24
Betrieben mit	-
CMS	WordPress 6.4
Generator	-
Programmiersprache	PHP 8.1
JavaScript-Frameworks	jQuery 3.6.0
Analytics-Tools	Keine erkannt
CDN / WAF	-
HTTP-Version	-
Kompression	Nicht aktiv

Antwortzeit (TTFB)	-
--------------------	---

## DSGVO-Analyse

DSGVO-Risiko: **NIEDRIG** | Kein Cookie-Consent erkannt

Keine bekannten Tracker / kritischen Drittanbieter erkannt.

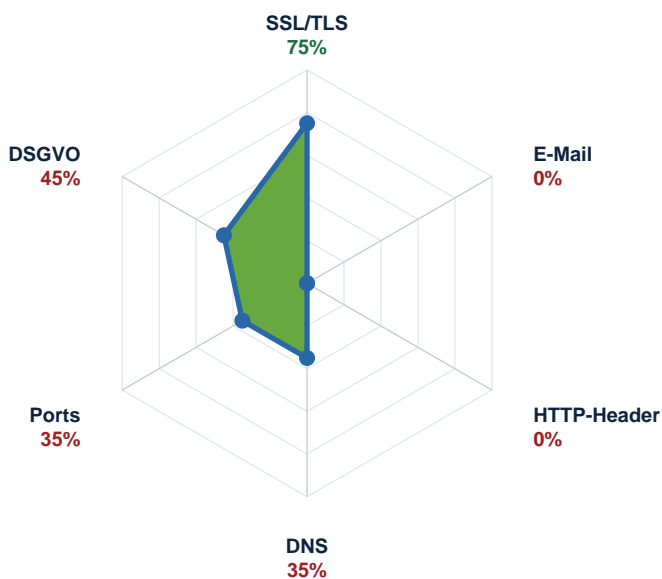
## Port-Scan & Angriffsfläche

Gescannte IP: **185.199.108.153** | 5 offene Port(s) gefunden von 22 geprueften

Port	Dienst	Risiko	Beschreibung	Banner
80	HTTP	NIEDRIG	Standard HTTP — leitet auf HTTPS um (akzeptabel)	-
443	HTTPS	NIEDRIG	Standard HTTPS — TLS 1.2/1.3 aktiv	-
3389	RDP	KRITISCH	Remote Desktop öffentlich erreichbar — Ransomware-	-
22	SSH	HOCH	SSH öffentlich — Brute-Force-Risiko	-
3306	MySQL	KRITISCH	Datenbank-Port direkt aus dem Internet erreichbar	-

## Sicherheits-Radar

Der Sicherheits-Radar zeigt die Bewertung der sechs zentralen Sicherheitskategorien auf einen Blick. Je weiter das blaue Polygon nach außen reicht, desto besser ist die Sicherheitslage in der jeweiligen Kategorie.



## Kategorie-Bewertungen

Kategorie	Score	Status
-----------	-------	--------

SSL/TLS	75%	Gut
E-Mail	0%	Kritisch
HTTP-Header	0%	Kritisch
DNS	35%	Kritisch
Ports	35%	Kritisch
DSGVO	45%	Kritisch

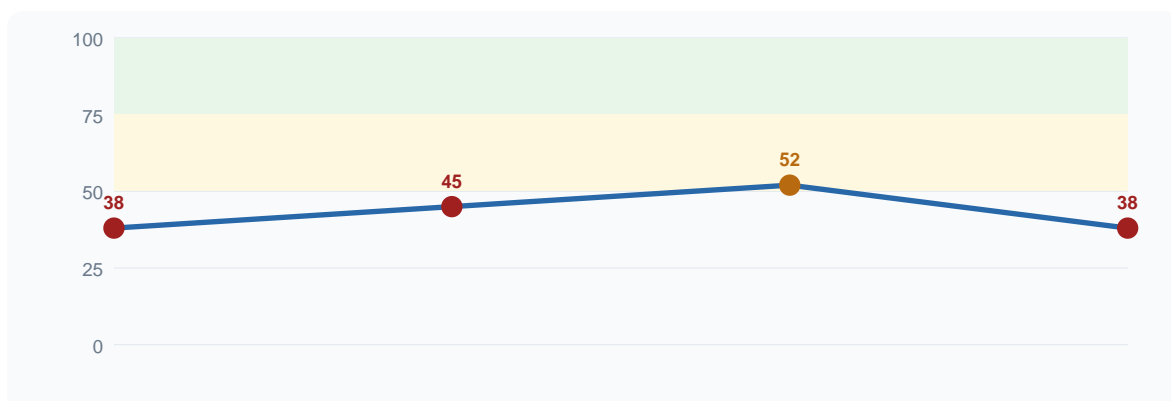
## DSGVO & Compliance

Detaillierte Analyse der Datenschutz-Grundverordnung (DSGVO) relevanten Aspekte und Compliance-Indikatoren.

Prüfpunkt	Status	Details
DSGVO – Cookie-Consent	✗ Offen	Kein Cookie-Consent gefunden
DSGVO – Hosting EU	✗ Offen	Hosting in DE
DSGVO – Tracker	✓ Bestanden	Keine Tracker erkannt
BSI – HTTPS	✓ Bestanden	SSL/TLS aktiv und gültig
BSI – Sicherheits-Header	✗ Offen	Header-Score: 0%
BSI – E-Mail-Schutz	✗ Offen	E-Mail-Spoofing möglich

## Sicherheits-Score: Historischer Verlauf

Entwicklung des Sicherheits-Scores über die letzten Audits. Ein steigender Trend zeigt erfolgreiche Verbesserungsmaßnahmen.



Trend über 4 Audits: → **Unverändert** (von 38 auf 38 Punkte)

## Maßnahmenplan

Priorisierte Handlungsempfehlungen basierend auf der Analyse. Quick-Wins sind Maßnahmen mit geringem Aufwand und hoher Wirkung.

## Quick-Wins (geringer Aufwand, schnelle Umsetzung)

P	Maßnahme	Aufwand	Priorität
1	HSTS-Header fehlt Strict-Transport-Security: max-age=31536000; includeSubDomains; preload	30 Min–2h	MITTEL
2	DNSSEC nicht aktiviert DNSSEC beim Registrar / Provider aktivieren.	4–8h	MITTEL
3	CAA-Record nicht gesetzt CAA-Record mit zugelassener CA setzen (z. B. Let's Encrypt).	< 30 Min	NIEDRIG

## Sofortige Maßnahmen (Priorität 1 – Kritisch/Hoch)

P1	Maßnahme	Aufwand	Frist
P1.1	DMARC-Record nicht gesetzt DMARC-Record mit p=quarantine starten, nach 4 Wochen auf p=reject erhöhen.	30 Min–2h	Sofort
P1.2	Port 3389 (RDP) öffentlich erreichbar RDP nur über VPN exponieren oder per Firewall auf bekannte IPs einschränken.	1–2h	Sofort
P1.3	CVE-2024-XXXX in eingesetzter Software (kritisch) Hersteller-Patch sofort einspielen, ggf. WAF-Rule als Übergangslösung.	4–8h	Sofort
P1.4	Content-Security-Policy fehlt Restriktive CSP mit default-src 'self' einführen.	2–4h	< 1 Woche
P1.5	SPF-Record verwendet Soft-Fail (~all) SPF auf -all stellen, vorher alle legitimen Versand-Wege prüfen.	30 Min–2h	< 1 Woche
P1.6	Google Analytics ohne dokumentiertes Consent Consent-Manager implementieren oder GA durch Plausible/Matomo ersetzen.	2–4h	< 1 Woche
P1.7	Facebook-Pixel ohne Consent Pixel deaktivieren oder Consent-Mechanismus einbauen.	2–4h	< 1 Woche
P1.8	TLS 1.0/1.1 noch aktiviert Webserver-Konfig auf TLS 1.2 + 1.3 only setzen.	2–4h	< 1 Woche
P1.9	.git-Verzeichnis öffentlich erreichbar Über Webserver-Konfig sperren: location ~ /\.git { deny all; }	1–2h	Sofort

## Mittelfristige Maßnahmen (Priorität 2 – < 3 Monate)

P2.1 X-Frame-Options fehlt – X-Frame-Options: DENY oder Frame-Ancestors in CSP.

P2.2 Datenschutzerklärung enthält nicht alle Pflichtangaben – Datenschutzerklärung anwaltlich oder per BfDI-Vorlage aktual

## Handlungsempfehlungen (Detail)

### Sofortiger Handlungsbedarf (Kritisch / Hoch)

<b>KRITISCH</b>	<p><b>DMARC-Record nicht gesetzt</b></p> <p>Es ist kein DMARC-Record für die Domain konfiguriert. Angreifer können E-Mails im Namen Ihrer Domain versenden (CEO-Fraud, Phishing).</p> <p>&gt; DMARC-Record mit p=quarantine starten, nach 4 Wochen auf p=reject erhöhen.</p>
-----------------	--

<b>KRITISCH</b>	<p><b>Port 3389 (RDP) öffentlich erreichbar</b></p> <p>Remote Desktop Protocol auf Port 3389 ist von extern erreichbar — typisches Einfallstor für Ransomware-Gruppen.</p> <p><b>Kostenrisiko: Einfallstor für Cyberangriffe – Ø 200.000 € Schaden bei KMU</b></p> <p>&gt; RDP nur über VPN exponieren oder per Firewall auf bekannte IPs einschränken.</p>
<b>KRITISCH</b>	<p><b>CVE-2024-XXXX in eingesetzter Software (kritisch)</b></p> <p>Erkannte Software-Version weist eine kritische, aktiv ausgenutzte Schwachstelle auf (CVSS 9.8).</p> <p>&gt; Hersteller-Patch sofort einspielen, ggf. WAF-Rule als Übergangslösung.</p>
<b>HOCH</b>	<p><b>Content-Security-Policy fehlt</b></p> <p>Keine CSP-Header gesetzt. XSS-Angriffe können Browser-seitig nicht blockiert werden.</p> <p>&gt; Restriktive CSP mit default-src 'self' einführen.</p>
<b>HOCH</b>	<p><b>SPF-Record verwendet Soft-Fail (~all)</b></p> <p>SPF endet mit ~all statt -all — empfangende Mailserver behandeln gefälschte Mails nicht strikt.</p> <p>&gt; SPF auf -all stellen, vorher alle legitimen Versand-Wege prüfen.</p>
<b>HOCH</b>	<p><b>Google Analytics ohne dokumentiertes Consent</b></p> <p>Tracker setzt Cookies, bevor der Nutzer einwilligt — DSGVO-Verstoß (Art. 6 Abs. 1, EuGH-Urteil C-673/17).</p> <p>&gt; Consent-Manager implementieren oder GA durch Plausible/Matomo ersetzen.</p>
<b>HOCH</b>	<p><b>Facebook-Pixel ohne Consent</b></p> <p>Drittland-Übermittlung nach USA ohne Rechtsgrundlage.</p> <p>&gt; Pixel deaktivieren oder Consent-Mechanismus einbauen.</p>
<b>HOCH</b>	<p><b>TLS 1.0/1.1 noch aktiviert</b></p> <p>Veraltete Protokollversionen sind weiterhin verfügbar (BSI TR-02102 ausgeschlossen seit 2018).</p> <p>&gt; Webserver-Konfig auf TLS 1.2 + 1.3 only setzen.</p>
<b>KRITISCH</b>	<p><b>.git-Verzeichnis öffentlich erreichbar</b></p> <p>Quellcode-Repository unter /.git/config liegt frei — sensitive Daten (DB-Credentials, API-Keys) potenziell extrahierbar.</p> <p>&gt; Über Webserver-Konfig sperren: location ~ /\.git { deny all; }</p>

### Kurzfristig umzusetzen (< 3 Monate)

<b>MITTEL</b>	<p><b>HSTS-Header fehlt</b></p> <p>HTTP Strict Transport Security ist nicht aktiv — Downgrade-Angriffe möglich.</p> <p>&gt; Strict-Transport-Security: max-age=31536000; includeSubDomains; preload</p>
<b>MITTEL</b>	<p><b>X-Frame-Options fehlt</b></p> <p>Clickjacking-Schutz nicht aktiv.</p> <p>&gt; X-Frame-Options: DENY oder Frame-Ancestors in CSP.</p>
<b>MITTEL</b>	<p><b>DNSSEC nicht aktiviert</b></p> <p>DNS-Antworten sind nicht kryptografisch signiert — Cache-Poisoning-Risiko.</p> <p>&gt; DNSSEC beim Registrar / Provider aktivieren.</p>

## MITTEL

**Datenschutzerklärung enthält nicht alle Pflichtangaben**

Es fehlen Angaben zu Drittland-Übermittlungen und Aufbewahrungsfristen.  
> *Datenschutzerklärung anwaltlich oder per BfDI-Vorlage aktualisieren.*

**Mittelfristig / Best Practice**

## NIEDRIG

**CAA-Record nicht gesetzt**

Beliebige CAs könnten Zertifikate für die Domain ausstellen.  
> *CAA-Record mit zugelassener CA setzen (z. B. Let's Encrypt).*

**Nächste Schritte – Ihr Aktionsplan**

Basierend auf der Analyse empfehlen wir folgendes strukturiertes Vorgehen. Die Schritte sind nach Dringlichkeit und Aufwand priorisiert.

**Phase 1: Sofortige Absicherung****Woche 1**

*Kritische und hohe Sicherheitslücken schließen. Diese Punkte stellen ein unmittelbares Risiko dar.*

#	Maßnahme	Aufwand	Verantwortlich
1	<b>DMARC-Record nicht gesetzt</b> DMARC-Record mit p=quarantine starten, nach 4 Wochen auf p=reject erhöhen.	30 Min–2h	IT-Dienstleister
2	<b>Port 3389 (RDP) öffentlich erreichbar</b> RDP nur über VPN exponieren oder per Firewall auf bekannte IPs einschränken.	1–2h	IT-Dienstleister
3	<b>CVE-2024-XXXX in eingesetzter Software (kritisch)</b> Hersteller-Patch sofort einspielen, ggf. WAF-Rule als Übergangslösung.	4–8h	IT-Dienstleister
4	<b>Content-Security-Policy fehlt</b> Restriktive CSP mit default-src 'self' einführen.	2–4h	IT-Dienstleister
5	<b>SPF-Record verwendet Soft-Fail (~all)</b> SPF auf -all stellen, vorher alle legitimen Versand-Wege prüfen.	30 Min–2h	IT-Dienstleister
6	<b>Google Analytics ohne dokumentiertes Consent</b> Consent-Manager implementieren oder GA durch Plausible/Matomo ersetzen.	2–4h	IT-Dienstleister

**Phase 2: Kurzfristige Optimierung****Monat 1–2**

*Mittlere Befunde beheben und Basis-Sicherheitsstandards herstellen.*

#	Maßnahme	Aufwand	Verantwortlich
1	<b>HSTS-Header fehlt</b> Strict-Transport-Security: max-age=31536000; includeSubDomains; preload	30 Min–2h	IT-Dienstleister
2	<b>X-Frame-Options fehlt</b> X-Frame-Options: DENY oder Frame-Ancestors in CSP.	< 30 Min	IT-Dienstleister
3	<b>DNSSEC nicht aktiviert</b> DNSSEC beim Registrar / Provider aktivieren.	4–8h	IT-Dienstleister
4	<b>Datenschutzerklärung enthält nicht alle Pflichtangaben</b> Datenschutzerklärung anwaltlich oder per BfDI-Vorlage aktualisieren.	2–4h	IT-Dienstleister

## Phase 3: Langfristige Härtung

Quartal 1–2

Best Practices umsetzen, Monitoring einrichten und kontinuierliche Verbesserung sicherstellen.

#	Maßnahme	Aufwand	Verantwortlich
1	CAA-Record nicht gesetzt CAA-Record mit zugelassener CA setzen (z. B. Let's Encrypt).	< 30 Min	IT-Dienstleister

## Empfohlener Prüfrhythmus

Maßnahme	Intervall	Hinweis
Sicherheits-Scan	Monatlich	Automatisiert über TWS Pilot
SSL-Zertifikat prüfen	Quartal	Ablaufdatum überwachen, auto-renewal einrichten
DNS-Konfiguration	Halbjährlich	SPF, DMARC, DNSSEC validieren
Penetrationstest	Jährlich	Durch ext. Dienstleister, inkl. Social Engineering

## Begriffe, Abkürzungen &amp; Lösungshinweise

Hinweis: Die folgenden Erklärungen und Handlungsempfehlungen sind unverbindliche, nicht geprüfte Vorschläge auf Basis allgemein anerkannter Best Practices. Für verbindliche Maßnahmen ist ein qualifizierter IT-Sicherheitsspezialist hinzuzuziehen.

## DNS (Domain Name System)

Das DNS übersetzt menschenlesbare Domainnamen (z. B. firma.de) in IP-Adressen. Fehlkonfigurierte DNS-Einträge können Angriffe wie DNS-Spoofing oder Cache-Poisoning ermöglichen.

Massnahme: Regelmäßige Überprüfung der DNS-Einträge, Aktivierung von DNSSEC, Verwendung redundanter Nameserver.

## DNSSEC (DNS Security Extensions)

Kryptografische Signatur der DNS-Einträge. Verhindert, dass Angreifer gefälschte DNS-Antworten einschleusen (DNS-Spoofing).

Massnahme: Aktivierung im Registrar-Panel und beim DNS-Provider. Erfordert Unterstützung durch Nameserver und Registrar.

## A-Record / AAAA-Record

DNS-Einträge, die eine Domain auf eine IPv4- (A) bzw. IPv6-Adresse (AAAA) zeigen lassen. Fehlende AAAA-Records bedeuten, dass die Website nicht über IPv6 erreichbar ist.

Massnahme: IPv6 beim Hoster aktivieren und AAAA-Record im DNS eintragen.

## CAA-Record (Certification Authority Authorization)

Gibt an, welche Zertifizierungsstellen (CAs) SSL-Zertifikate für die Domain ausstellen dürfen. Ohne CAA kann jede CA ein Zertifikat ausstellen – Risiko für unberechtigte Zertifikate.

Massnahme: CAA-Record im DNS hinzufügen, z. B.: 0 issue "letsencrypt.org"

## SSL/TLS (Secure Sockets Layer / Transport Layer Security)

Protokoll zur Verschlüsselung der Datenübertragung zwischen Browser und Server (erkennbar an HTTPS). Veraltete Versionen (SSL, TLS 1.0/1.1) gelten als unsicher.

Massnahme: Nur TLS 1.2 oder TLS 1.3 aktivieren. Veraltete Protokolle im Webserver deaktivieren.

## SSL-Grade (A+, A, B, C, F)

Bewertung der SSL/TLS-Konfiguration nach dem SSL Labs-Standard. A+ ist das Optimum, F bedeutet kritische Sicherheitslücken.

Massnahme: Webserver-Konfiguration anpassen: starke Cipher Suites, HSTS aktivieren, Forward Secrecy sicherstellen.

<b>HSTS (HTTP Strict Transport Security)</b>	
HTTP-Sicherheits-Header, der Browser zwingt, die Website ausschließlich über HTTPS aufzurufen. Schützt vor Downgrade-Angriffen und Protokoll-Stripping.	<i>Massnahme: Im Webserver konfigurieren: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload</i>
<b>SPF (Sender Policy Framework)</b>	
DNS-Eintrag, der festlegt, welche Mailserver E-Mails im Namen der Domain versenden dürfen. Ohne SPF kann jeder Server Mails mit gefälschtem Absender verschicken.	<i>Massnahme: SPF-Record im DNS anlegen, z. B.: v=spf1 mx ~all (Softfail) oder v=spf1 mx -all (Hardfail/reject).</i>
<b>DMARC (Domain-based Message Authentication, Reporting &amp; Conformance)</b>	
Ergänzt SPF und DKIM. Legt fest, was passiert, wenn eine E-Mail die Prüfung nicht besteht (none = nichts, quarantine = Spam, reject = ablehnen). Ohne DMARC ist Phishing im Namen der Domain möglich.	<i>Massnahme: DMARC-Record anlegen: v=DMARC1; p=quarantine; rua=mailto:dmarc@firma.de Langfristig auf p=reject wechseln.</i>
<b>MX-Record (Mail Exchange)</b>	
DNS-Eintrag, der angibt, welcher Mailserver für die Domain zuständig ist. Fehlende oder falsche MX-Records führen zu Mailzustellungsproblemen.	<i>Massnahme: MX-Record beim DNS-Provider korrekt eintragen und auf den Mailserver zeigen lassen.</i>
<b>Content-Security-Policy (CSP)</b>	
HTTP-Header, der steuert, welche externen Ressourcen (Scripts, Bilder, Frames) geladen werden dürfen. Verhindert Cross-Site-Scripting (XSS) und Clickjacking.	<i>Massnahme: Im Webserver oder CMS konfigurieren. Start: Content-Security-Policy: default-src 'self'</i>
<b>X-Frame-Options</b>	
Verhindert, dass die Website in einem iFrame einer fremden Seite eingebettet wird (Clickjacking-Schutz).	<i>Massnahme: Header setzen: X-Frame-Options: DENY oder SAMEORIGIN</i>
<b>X-Content-Type-Options</b>	
Verhindert, dass Browser Dateitypen erraten (MIME-Sniffing), was zu Angriffen führen kann.	<i>Massnahme: Header setzen: X-Content-Type-Options: nosniff</i>
<b>Referrer-Policy</b>	
Steuert, welche Referrer-Informationen beim Navigieren weitergegeben werden. Ohne Policy werden vollständige URLs an Drittsiten übermittelt.	<i>Massnahme: Header setzen: Referrer-Policy: strict-origin-when-cross-origin</i>
<b>DSGVO (Datenschutz-Grundverordnung)</b>	
EU-Verordnung zum Schutz personenbezogener Daten. Betreiber müssen u. a. Einwilligung für Tracking einholen, Datentransfers in Drittländer dokumentieren und eine Datenschutzerklärung vorhalten.	<i>Massnahme: Cookie-Consent-Tool implementieren, Datenschutzerklärung aktualisieren, Auftragsverarbeitungsverträge (AVV) mit Dienstleistern abschließen.</i>
<b>Google Analytics / Tag Manager</b>	
Web-Analyse-Tools von Google. Ohne Einwilligung (Opt-in) ist der Einsatz in der EU unzulässig (EuGH-Urteil, Schrems II, DSK-Beschlüsse).	<i>Massnahme: Cookie-Consent mit Opt-in implementieren. Alternativ datenschutzfreundliche Tools nutzen (z. B. Matomo selbst gehostet, Plausible Analytics).</i>
<b>Google Fonts (extern)</b>	
Werden Fonts direkt von Google-Servern geladen, wird die IP des Besuchers übermittelt – ohne Einwilligung unzulässig (LG München, Az. 3 O 17493/20).	<i>Massnahme: Fonts lokal einbinden: Schriften herunterladen und auf dem eigenen Server bereitstellen.</i>

<b>Offene Ports</b>	
TCP/UDP-Ports, die von außen erreichbar sind. Unnötig offene Ports vergrößern die Angriffsfläche. Kritische Ports: 21 (FTP), 22 (SSH), 23 (Telnet), 3389 (RDP), 1433 (MSSQL), 3306 (MySQL).	<i>Massnahme: Firewall-Regeln prüfen: Nur zwingend benötigte Ports öffentlich zugänglich lassen. Verwaltungszugänge (SSH, RDP) auf Whitelist-IPs beschränken oder VPN vorschalten.</i>
<b>FTP (Port 21)</b>	
Veraltetes, unverschlüsseltes Dateiübertragungsprotokoll. Zugangsdaten werden im Klartext übertragen.	<i>Massnahme: FTP deaktivieren und durch SFTP (SSH File Transfer Protocol, Port 22) ersetzen.</i>
<b>Telnet (Port 23)</b>	
Veraltetes, unverschlüsseltes Remote-Login-Protokoll. Vollständig obsolet.	<i>Massnahme: Telnet-Dienst deaktivieren. SSH als sicheren Ersatz verwenden.</i>
<b>RDP (Port 3389)</b>	
Remote Desktop Protocol für Windows-Fernzugriff. Häufig Ziel automatisierter Brute-Force-Angriffe.	<i>Massnahme: RDP nicht direkt ins Internet exponieren. VPN vorschalten, NLA (Network Level Authentication) aktivieren, IP-Whitelist konfigurieren.</i>
<b>Hosting außerhalb der EU</b>	
Server in Drittländern (z. B. USA) unterliegen anderen Datenschutzgesetzen. US-Cloud Act ermöglicht US-Behörden Zugriff ohne EU-Rechtsweg.	<i>Massnahme: Auf EU-Rechenzentrum wechseln, bevorzugt in Deutschland (BSI C5-zertifizierte Anbieter). Auftragsverarbeitungsvertrag (AVV) mit Hostler abschließen.</i>
<b>ASN (Autonomous System Number)</b>	
Eindeutige Nummer eines Netzwerks im Internet (z. B. eines Hosting-Providers). Gibt Auskunft über den tatsächlichen Infrastrukturanbieter, unabhängig von der Domain.	<i>Massnahme: Keine direkte Maßnahme nötig – Informationswert für Herkunft und Anbieter des Hostings.</i>
<b>Subdomains (Zertifikat-Transparenz-Logs)</b>	
CT-Logs (Certificate Transparency) protokollieren alle ausgestellten SSL-Zertifikate öffentlich. Darüber können Subdomains eines Unternehmens aufgedeckt werden – auch interne oder vergessene.	<i>Massnahme: Alle aufgelisteten Subdomains prüfen: Nicht mehr benötigte abschalten, veraltete Systeme patchen, Sicherheitsniveau angleichen.</i>

## Risikobilanz in Euro — Vorstands-Übersicht

Erwarteter Gesamtschaden bei Realisierung aller Befunde	<b>788.800 €</b>
Risikoerwartungswert (gewichtet × Eintrittswahrscheinlichkeit)	<b>323.120 €</b>
Bandbreite (Best-/Worst-Case)	<b>186.880 € ... 3.944.000 €</b>
Branchen-Faktor angewendet	<b>MITTELSTAND (×1.6)</b>
Aufwand zur Behebung (alle Befunde)	<b>53.0 h · 7.685 € netto</b>
Risiko-Hebel (ROI-Faktor)	<b>42.0 ×</b> 1 € Investition wendet ca. 42.0 € Risiko ab

### Wie kommen diese Beträge zustande?

Die Werte sind **keine erfundenen Zahlen**, sondern fußen auf den unten zitierten öffentlichen Studien deutscher und internationaler Branchenverbände. Drei Größen fließen pro Befund ein:

- ① **Schadenshöhe** bei Eintritt — abgeleitet aus den Mittelwerten der aktuellen Branchenstudien (siehe Quellenliste unten), differenziert nach Severity-Stufe.
- ② **Eintrittswahrscheinlichkeit** — Erfahrungswert aus BSI-Lagebericht 2024: kritisch ≈ 45 %, hoch ≈ 30 %, mittel ≈ 15 %, niedrig ≈ 5 % p. a.
- ③ **Branchenfaktor** — Multiplikator aus dem Pre-Audit-Fragebogen (KMU = 1,0; Mittelstand = 1,6; Konzern = 4,5; Behörde = 2,1; Gesundheit = 2,8; Finanzdienstleister = 3,5; KRITIS = 3,2). Branche dieses Audits: **MITTELSTAND (×1.6)**.

### Risikoerwartungswert = Schadenshöhe × Eintrittswahrscheinlichkeit × Branchenfaktor

Quelle	Verwendete Zahl	Beispiel-Anwendung im Bericht
<b>Bitkom „Wirtschaftsschutz 2024“</b> Studie unter 1.003 deutschen Unternehmen, veröffentl. 28.08.2024	Ø Schaden KMU pro Cybervorfall: <b>206.000 €</b> Gesamtschaden D 2024: 178,6 Mrd. €	Basiswert für „mittel“/„hoch“-Befunde, skaliert nach Branchengröße. Z. B. CSP-Lücke „hoch“: 12.000 € erwartet.
<b>IBM „Cost of a Data Breach Report 2024“</b> 600 Unternehmen weltweit, IBM Security/Ponemon	Ø Datenschutzvorfall global: <b>4,88 Mio. USD</b> Deutschland: 4,10 Mio. €	Anker für „kritisch“-Befunde mit Datenleck-Potenzial (z. B. .git-Verzeichnis exponiert, RDP offen).
<b>BSI Lagebericht IT-Sicherheit 2024</b> Bundesamt für Sicherheit in der Informationstechnik	Ø Ransomware-Schaden Mittelstand: <b>1,2 Mio. €</b> Eintrittswkt. bei offenem RDP: ca. 45 % p. a.	Quelle für Eintrittswahrscheinlichkeiten und Bewertung von Port-/CVE-Befunden.
<b>Allianz Cyber Risk Trends 2024</b> AGCS Schadensauswertung > 1.700 Cyberschäden	Ø Betriebsunterbrechung: <b>23 Tage</b> Ø Kosten/Stunde Stillstand KMU: 4.300 €	Ausfallkosten-Komponente bei kritischen Verfügbarkeits-Befunden.
<b>BfDI Tätigkeitsberichte 2023/24</b> Bundesbeauftragter für den Datenschutz	DSGVO-Bußgelder DE 2024: <b>Median 5.000 € · Ø 285.000 €</b> Maximum: 4 % Jahresumsatz	Bußgeld-Erwartungswert für DSGVO-Befunde (Tracker, Cookie-Consent, unvollständige Datenschutzerklärung).

<b>BSI IT-Grundschutz-Kompodium 2023</b> Risikobewertungs-Tabelle, Kap. „Schadensauswirkungen“	Schadens-Klassen 1–5: <b>Klasse 3 = bis 50.000 €</b> <b>Klasse 4 = bis 200.000 €</b>	Mappingbasis Severity → Schadensklasse für die Risiko-Matrix.
---	--	---

**Konkretes Beispiel — wie ein Befund umgerechnet wird:**

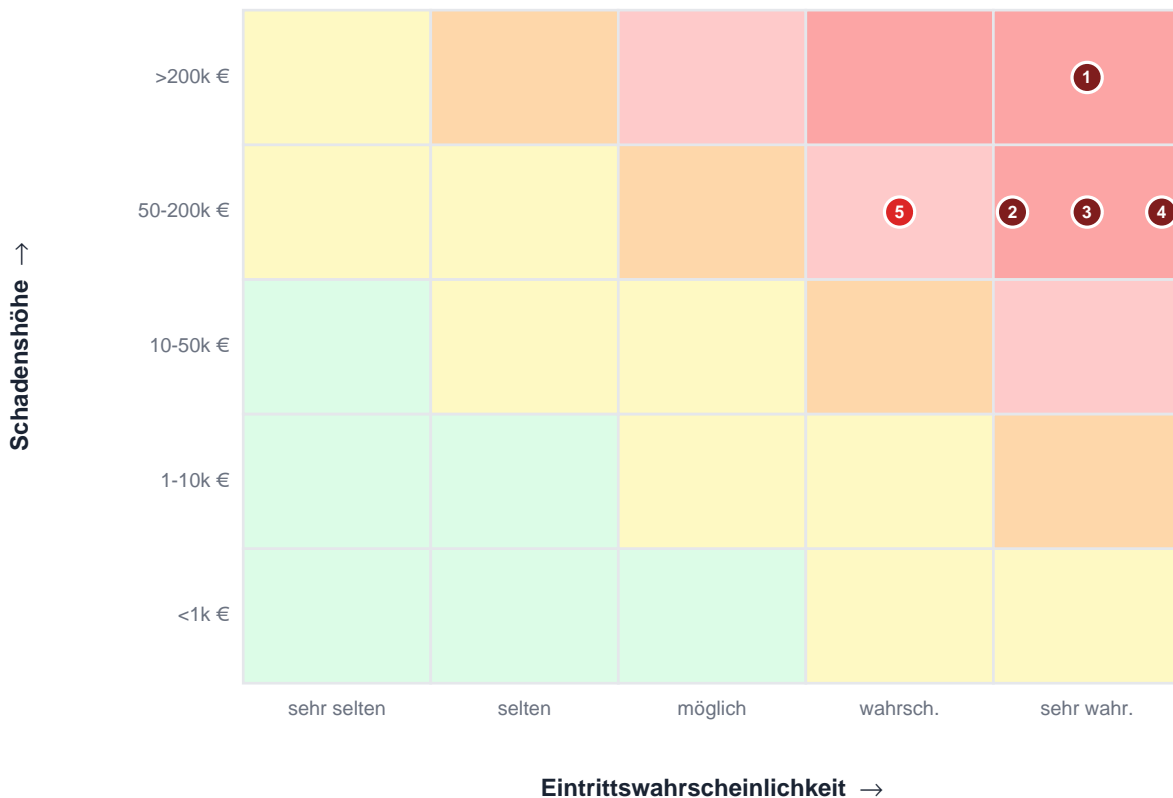
Befund „DMARC-Record nicht gesetzt“ (Severity „kritisch“):

- Schadenshöhe (typisch CEO-Fraud-Fall. IBM/Bitkom): 65.000 € erwartet. Bandbreite 15.000–320.000 €
- Eintrittswahrscheinlichkeit (BSI Lagebericht): 45 % p. a. bei fehlender Mail-Authentisierung
- Branchenfaktor (Audit-Branche MITTELSTAND): x1.6
- **Risikoerwartungswert:** 65.000 € x 0.45 x 1.6 = **46.800 €** p. a.

*Hinweis:* Die Werte sind **plausibilisierte Schätzungen** für die Geschäftsleitung — keine versicherungsmathematische Garantie. Sie eignen sich für den Risikodialog und für Investitionsentscheidungen, nicht für die Berechnung von Versicherungsprämien oder Schadensersatzforderungen.

## Risiko-Matrix

Visualisierung der Top-Befunde nach Eintrittswahrscheinlichkeit (X-Achse) und Schadenshöhe (Y-Achse). Die nummerierten Punkte beziehen sich auf die Liste der Top-5-Risiken unten.



Nr.	Befund	Severity	Erwarteter Schaden	Risiko (× WK)
1	CVE-2024-XXXX in eingesetzter Software	KRITISCH	232.000 €	104.400 €
2	Port 3389 (RDP) öffentlich erreichbar	KRITISCH	152.000 €	68.400 €
3	Sensitive .git Verzeichnis exposed	KRITISCH	124.800 €	56.160 €
4	DMARC-Record nicht gesetzt	KRITISCH	104.000 €	46.800 €
5	SPF-Record verwendet Soft-Fail	HOCH	56.000 €	16.800 €

## § 1 NIS-2-Konformitäts-Bewertung

NIS-2-Status	<b>WICHTIGE Einrichtung</b>
Sektor-Klassifikation	Anhang II — Verarbeitendes Gewerbe
NIS-2-Reifegrad	46 %
Bereiche mit Befund	7 kritische / 10 gesamt

Art. 21 Abs. 2	Maßnahmenbereich	Reife	Befunde
lit. a	Risikomanagement-Konzept	0 %	3 x
lit. b	Vorfallbewältigung	60 %	1 x
lit. c	Geschäftskontinuität / Backup	100 %	✓
lit. d	Sicherheit der Lieferkette	100 %	✓
lit. e	Sicherheit bei Beschaffung, Entwicklung, Wartung	29 %	3 x
lit. f	Wirksamkeitsbewertung	60 %	1 x
lit. g	Cyberhygiene & Schulungen	0 %	6 x
lit. h	Kryptografie & Verschlüsselung	70 %	2 x
lit. i	Personalsicherheit & Zugriffskontrolle	9 %	3 x
lit. j	Multi-Faktor-Authentisierung & sichere Kommunikation	29 %	3 x

**Bewertung:** ■ Hoher Handlungsbedarf: Im NIS-2-Geltungsbereich (Anhang II — Verarbeitendes Gewerbe) mit Reifegrad nur 46 %. Geschäftsleitung haftet persönlich nach § 38 NIS2UmsuCG. Sofortmaßnahmen erforderlich.

## § 2 ISO/IEC 27001:2022 — Annex-A-Coverage

Im Rahmen dieses externen Audits wurden **20 der 93 Annex-A-Controls** automatisiert geprüft. Coverage: **30 %** der prüfbaren Controls erfüllt (6 ohne Befund, 14 mit Befund).

Control	Inhalt	Befunde	Severity
A.5.14	Informationsübertragung (DKIM, SPF, DMARC für Mail)	2	KRITISCH
A.5.31	Rechtliche, statutarische, vertragliche Anforderungen (DSGVO/Impressum)	3	HOCH
A.5.7	Threat Intelligence (CVE-Tracking, Schwachstellen-Monitoring)	1	KRITISCH
A.8.10	Informationslöschung (sensitive_files exposure)	1	KRITISCH
A.8.20	Netzwerksicherheit (Firewall, geschlossene Ports)	2	KRITISCH
A.8.21	Sicherheit von Netzwerkdiensten (TLS, sichere Protokolle)	3	HOCH
A.8.22	Trennung von Netzwerken (Segmentierung)	1	KRITISCH
A.8.23	Web-Filter / Browser-Sicherheit (CSP, X-Frame-Options)	2	HOCH
A.8.24	Verwendung von Kryptographie (TLS 1.2+, sichere Cipher, DNSSEC)	2	HOCH

<b>A.8.26</b>	Sicherheitsanforderungen an Anwendungen (CSP, Input-Validation)	2	<b>HOCH</b>
<b>A.8.28</b>	Sicherer Code (Output-Escaping, sichere Header)	2	<b>HOCH</b>
<b>A.8.5</b>	Sichere Authentisierung (MFA, sichere Mail-Authentisierung)	2	<b>KRITISCH</b>
<b>A.8.8</b>	Verwaltung technischer Schwachstellen (CVE-Patching)	1	<b>KRITISCH</b>
<b>A.8.9</b>	Konfigurationsmanagement (Security-Header, gehärtete Defaults)	1	<b>KRITISCH</b>

**Empfehlung:** ISO/IEC 27001:2022-Reifegrad ist niedrig (30 %). 14 Controls mit Befunden. Eine Zertifizierung wäre derzeit nicht realistisch. Empfehlung: Grundabsicherung über die Roadmap, danach erneutes Audit.

### § 3 DSGVO Art. 32 — Technische und Organisatorische Maßnahmen

Art. 32 DSGVO verpflichtet Verantwortliche, geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Aus dem externen Audit ergeben sich folgende TOM-relevante Befunde:

Schutzziel (Art. 32 DSGVO)	Stand	Befunde aus diesem Audit
Verschlüsselung der Übertragung (lit. a)	<b>x Mangelhaft</b>	TLS-Konfiguration siehe Abschnitt SSL/TLS
Vertraulichkeit personenbezogener Daten (lit. b)	<b>x 7 Tracker ohne Consent</b>	Drittanbieter-Tracker siehe DSGVO-Abschnitt
Verfügbarkeit / Belastbarkeit (lit. b)	<b>x 3 riskante Ports</b>	Port-Scan-Ergebnis siehe entsprechender Abschnitt
Regelmäßige Überprüfung der Wirksamkeit (lit. d)	Empfohlen jährlich	Dieses Audit dient als Nachweis. Wiederholungs-Audit jährlich.

### § 4 Maßnahmen-Roadmap

Die Roadmap ist nach Dringlichkeit strukturiert. Die geschätzten Stundenwerte gehen von einem qualifizierten IT-Dienstleister mit Standard-Stundensatz aus (145 € netto). Sofort-Maßnahmen sollten innerhalb von 7 Tagen begonnen werden.

Sofort (≤ 7 Tage)		4 Maßnahmen	
#	Maßnahme	Severity	Risiko-Hebel
1	DMARC-Record nicht gesetzt	KRITISCH	46.800 €
2	Port 3389 (RDP) öffentlich erreichbar	KRITISCH	68.400 €
3	CVE-2024-XXXX in eingesetzter Software	KRITISCH	104.400 €
4	Sensitive .git Verzeichnis exposed	KRITISCH	56.160 €

Kurzfristig (≤ 30 Tage)		5 Maßnahmen	
#	Maßnahme	Severity	Risiko-Hebel
1	Content-Security-Policy fehlt	HOCH	8.640 €

2	SPF-Record verwendet Soft-Fail	HOCH	16.800 €
3	Google Analytics ohne Cookie-Consent (Tracker)	HOCH	4.800 €
4	Facebook-Pixel Tracker ohne Einwilligung	HOCH	4.800 €
5	TLS-Cipher TLS_RSA_WITH_AES_128_CBC_SHA schwach	HOCH	7.200 €

Mittelfristig (≤ 90 Tage)		5 Maßnahmen	
#	Maßnahme	Severity	Risiko-Hebel
1	SSL kein HSTS	MITTEL	1.680 €
2	X-Frame-Options fehlt	MITTEL	1.440 €
3	DNSSEC fehlt	MITTEL	1.200 €
4	CAA fehlt	NIEDRIG	80 €
5	Datenschutzerklärung unvollständig	MITTEL	720 €

## § 4b Konkrete Umsetzung — copy-paste-fertige Konfigurationen

Für die Top-5-Befunde liefern wir hier direkt einsetzbare Konfigurations-Schnipsel. Diese sind als Vorlage gedacht — bitte vor der produktiven Umsetzung im Wartungsfenster prüfen und auf Ihre spezifische Umgebung anpassen.

### [KRITISCH] 1. Kritisches CVE umgehend patchen

*Befund:* CVE-2024-XXXX in eingesetzter Software

CVSS ≥ 9.0 = aktiv ausgenutzt. Zeitfenster bis Massen-Exploitation liegt typisch bei 24–72 h.

#### ► Sofort-Maßnahmen

1. CVE-Nummer notieren → CVE.org / NVD nachschlagen für Details.
2. Hersteller-Patch finden (Release-Notes).
3. Backup VOR Update (DB-Dump + Datei-Snapshot).
4. Patch einspielen – falls nicht möglich: WAF-Rule oder Service abschalten.
5. Nach Update: Verify mit nmap/Vulnerability-Scanner, dass die Lücke geschlossen ist.

### [KRITISCH] 2. Riskanten Port via Firewall einschränken

*Befund:* Port 3389 (RDP) öffentlich erreichbar

RDP (3389), SMB (445), Datenbanken (3306, 5432, 1433, 27017, 6379) gehören NIEMALS direkt ins Internet. Lösung: VPN (WireGuard / OpenVPN), Bastion-Host oder IP-Whitelist. Statistisch werden öffentliche RDP-Ports binnen 24 h angegriffen.

#### ► iptables (Linux)

```
# RDP nur aus VPN-Subnetz erlauben:
iptables -A INPUT -p tcp --dport 3389 -s 10.0.0.0/24 -j ACCEPT
iptables -A INPUT -p tcp --dport 3389 -j DROP
```

#### ► ufw (Ubuntu / Debian)

```
sudo ufw deny 3389/tcp
sudo ufw allow from 10.0.0.0/24 to any port 3389
sudo ufw reload
```

#### ► Windows Defender Firewall (PowerShell)

```
New-NetFirewallRule -DisplayName "Block RDP from Internet" -Direction Inbound -LocalPort 3389
-Protocol TCP -Action Block
New-NetFirewallRule -DisplayName "Allow RDP from VPN" -Direction Inbound -LocalPort 3389
-Protocol TCP -RemoteAddress 10.0.0.0/24 -Action Allow
```

■ *Vor der Umsetzung beachten: Vor dem Setzen der DROP-Regel sicherstellen, dass eigener Admin-Zugang NICHT abgeschnitten wird (z. B. via VPN bereits erreichbar).*

### [KRITISCH] 3. Sensitive Dateien per Webserver-Konfig sperren

*Befund:* Sensitive .git Verzeichnis exposed

.git, .env, .htaccess.bak und ähnliches niemals öffentlich erreichbar.

#### ► nginx

```
location ~ /\.(git|env|svn|hg|bzip) {
    deny all;
    access_log off;
    log_not_found off;
}
location ~ /\.(bak|sql|log|backup|old)$ {
    deny all;
}
```

#### ► Apache .htaccess

```
RedirectMatch 404 /\.(git|env|svn|hg|bzip)

Require all denied
```

### [KRITISCH] 4. DMARC-Record stufenweise einführen

*Befund:* DMARC-Record nicht gesetzt

DMARC schützt vor CEO-Fraud + Phishing. Empfohlene Stufen: (1) p=none + rua für 4 Wochen Monitoring → (2) p=quarantine + pct=25 → (3) p=reject pct=100. Die Reports an rua-Mailbox liefern den Nachweis, welche Versand-Wege noch nicht SPF/DKIM-konform sind.

#### ► DNS TXT-Record (Stufe 1: nur Monitoring)

```
_dmarc IN TXT "v=DMARC1; p=none; rua=mailto:dmarc@ihre-firma.de;
ruf=mailto:dmarc@ihre-firma.de; fo=1"
```

#### ► DNS TXT-Record (Stufe 2: 25 % Quarantäne)

```
_dmarc IN TXT "v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc@ihre-firma.de"
```

#### ► DNS TXT-Record (Stufe 3: produktiv strikt)

```
_dmarc IN TXT "v=DMARC1; p=reject; pct=100; rua=mailto:dmarc@ihre-firma.de; sp=reject;
aspf=s; adkim=s"
```

■ *Vor der Umsetzung beachten: Vor Aktivierung von p=reject: mind. 4 Wochen lang die rua-Reports auswerten (Tools: Postmark DMARC-Monitor, dmarcian, Easyworld dmarc-XML).*

### [HOCH] 5. SPF-Record auf strict-fail (-all) härten

*Befund:* SPF-Record verwendet Soft-Fail

SPF mit "-all" weist empfangende Mailserver an, gefälschte E-Mails strikt abzulehnen. Vorher unbedingt alle legitimen Versand-Wege ergänzen (Newsletter-Provider, ERP, Druckerei, ...) — sonst werden eigene Mails geblockt.

#### ► DNS TXT-Record (Beispiel: Microsoft 365 + SendGrid)

```
@ IN TXT "v=spf1 include:spf.protection.outlook.com include:sendgrid.net -all"
```

#### ► DNS TXT-Record (Beispiel: Google Workspace)

```
@ IN TXT "v=spf1 include:_spf.google.com -all"
```

■ *Vor der Umsetzung beachten: SPF erlaubt max. 10 DNS-Lookups (RFC 7208). Bei mehr Versand-Diensten "include:" konsolidieren oder Subdomain-SPF einsetzen.*

## § 5 E-Mail-Sicherheit (Deep-Scan)

SPF — All-Modus	~all	✓ gut
SPF — DNS-Lookups	5 / 10 erlaubt	✓
DMARC — Policy	p=None (pct=0)	unzureichend
DMARC — RUA-Reports	— nicht konfiguriert	■
DKIM — Selektoren gefunden	1 / 18 geprüft	✓
DKIM — Schlüsselstärke	2048 bit	✓
BIMI (Logo-Sichtbarkeit)	nicht konfiguriert	Bonus für Markensichtbarkeit
DNS-Blacklist-Status	✓ sauber in allen geprüften Listen	Spamhaus ZEN, SpamCop, SORBS, Barracuda

## § 6 IP-Reputation & Threat-Intelligence

IP-Adresse	185.199.108.153	
ISP	Hetzner Online GmbH	DE
Nutzungstyp	Data Center/Web Hosting/Transit	
AbuseIPDB Confidence	0 / 100	SAUBER
Total Reports (90 Tage)	0	
Tor-Exit-Node	✓ Nein	
Gesamtbewertung	SAUBER	

## § 7 Methoden, Quellen & Limitierungen

### Datenquellen:

- Cloudflare DNS-over-HTTPS (DNS-Auflösung A, AAAA, MX, NS, TXT, CAA, DNSKEY)
- RDAP-Server der zuständigen Registry (DENIC für .de, IANA-Hub für .com/.org)
- NIST National Vulnerability Database (CVE-Matching)
- crt.sh (Certificate-Transparency-Logs für Subdomain-Enumeration)
- OffeneRegister.de (Geschäftsführer-/Handelsregister-Lookup für deutsche Firmen)
- AbuseIPDB Public API (IP-Reputation, optional)
- Tor-Project-Exit-List (Tor-Node-Detection)
- Spamhaus / SpamCop / SORBS / Barracuda DNSBL-Zonen
- BSI IT-Grundschutz Kompendium 2023 (BSI-Mapping)
- Bitkom-Studie „Wirtschaftsschutz 2024“ + IBM Cost of a Data Breach Report 2024 (Schadenshöhen-Schätzung)

### Score-Berechnung:

Der Gesamtscore (0–100) ist eine gewichtete Linearkombination aller Befunde. Ein kritischer Befund senkt den Score um 20 Punkte, ein hoher um 10, ein mittlerer um 5, ein niedriger um 2. Der NIS-2-Reifegrad und die ISO-Coverage werden separat als Prozent-Werte berechnet — sie sind keine Einzelnoten, sondern messen die Erfüllung formaler Compliance-Anforderungen.

### Limitierungen dieses Audits:

- **Externe Sicht:** Geprüft wird ausschließlich, was öffentlich von außen sichtbar ist. Interne Schwachstellen (Active Directory, Endpunkt-Konfigurationen, Backup-Strategie, physische Zutrittskontrolle) sind nicht Gegenstand.
- **Momentaufnahme:** Der Befund spiegelt den Zustand zum Zeitpunkt des Scans. Konfigurationsänderungen können den Status verschieben.
- **Keine Penetration:** Es wurden ausschließlich passive bzw. RFC-konforme Banner-Grabs ausgeführt. Es wurden keine Exploits eingesetzt — d. h. eine Schwachstelle kann gemeldet sein, ohne dass sie aktiv ausnutzbar war.
- **Schadenshöhen sind Schätzungen** auf Basis öffentlich publizierter Studien — keine versicherungsmathematische Bewertung.
- **Subdomain-Liste** aus Certificate-Transparency-Logs ist nicht vollständig: Subdomains ohne öffentliches TLS-Zertifikat werden nicht gefunden.

### Sachverständiger:

Dieser Bericht wurde durch **Thomas Svilar**, Inhaber TWS Unternehmensberatung, Fachplaner für ITK-Systeme, erstellt und freigegeben. Mehr als 20 Jahre praktische Erfahrung im Bereich Informations- und Telekommunikationstechnik, mit Schwerpunkt auf Vergabeverfahren für deutsche Kommunen, Behörden und Schulträger. Bei Fragen zum Befund: thomas.svilar@twsconsult.de

---

#### Über diesen Bericht

Dieser Bericht wurde automatisch durch TWS Pilot erstellt und basiert auf passiver Analyse öffentlich zugänglicher Informationen (DNS, HTTP-Header, Zertifikat-Transparenz-Logs, offene Ports). Es handelt sich um eine Momentaufnahme – Änderungen der Infrastruktur können jederzeit eintreten. Für eine vollständige Sicherheitsprüfung empfehlen wir ein professionelles Penetrationstesting.

© TWS Pilot – Thomas Svilar | IT-Fachplanung & Beratung | Alle Angaben ohne Gewähr | Vertraulich