

# TK-Infrastruktur-Audit

## Sicherheits- & Technologie-Analyse

tk.muster-gmbh.de

Analysiert fuer: Muster GmbH (TK-Audit - Beispiel)

Erstellungsdatum: 03.05.2026 10:56

### ZUSAMMENFASSUNG DER BEFUNDE



Mangelhaft



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

## Management-Zusammenfassung

	Bereich	Details
✓	SSL / TLS	Note A, gültig noch 62 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	1 kritische Ports offen
✗	Performance	Nicht geprüft

### Kritische Handlungsempfehlungen:

#### 1. Kein Toll-Fraud-Schutz aktiviert

Die TK-Anlage erlaubt internationale Sonderrufnummern ohne PIN-/Limit-Begrenzung. Bei Kompromittierung eines Endgeräts oder VoIP-Accounts können binnen Stunden Premium-Rate-Schäden im fünfstelligen Bereich entstehen (typischer Wochenend-Angriff: 8.000–35.000 €). · *Tarifsperren konfigurieren (00, 0900, 118, Auslandsregionen). PIN-Authentifizierung für Außerhaus-Telefonate. Tageslimit pro Nebenstelle.*

#### 2. SIP-Trunk unverschlüsselt (Klartext)

Die SIP-Verbindung zum SIP-Provider läuft über UDP/5060 ohne TLS-Verschlüsselung. Gespräche und Anmeldedaten werden im Klartext übertragen. Mitlesen / Mithören durch Dritte am Übertragungsweg möglich. · *SIP-TLS auf Port 5061 aktivieren, SRTP für Medien-Streams.*

#### 3. SIP-Registrierung mit schwachen Default-Credentials

Mehrere SIP-Endgeräte verwenden Standard-Passwörter (admin/1234, user/user). Dies ermöglicht SIP-Account-Übernahme und Anrufmissbrauch. · *Komplexe SIP-Passwörter (≥ 16 Zeichen), pro Endgerät individuell. Firewall-Regel: SIP-Registrierung nur aus internem Netz.*

#### 4. TK-Anlagen-Webgui ohne TLS / öffentlich erreichbar

Das Administrations-Webinterface der TK-Anlage ist über HTTP (nicht HTTPS) und aus dem Internet ohne VPN erreichbar. Brute-Force-Angriffe und Credentials-Abfangen möglich. · *HTTPS mit gültigem Zertifikat + Beschränkung auf VPN- oder Management-Netz.*

#### 5. DECT-Verschlüsselung deaktiviert oder schwach

Die DECT-Basisstationen senden ohne aktivierte Geräte-Authentisierung (DSAA2) und Medien-Verschlüsselung (DSC). Mit handelsüblicher Hardware können Gespräche mitgehört werden (gnu-radio + DECT-Sniffer). · *In der DECT-Basisstation: DSAA2 + DSC aktivieren, ggf. Firmware-Update einspielen.*

### Entwicklung seit letztem Audit:

	Vorheriger Scan	Aktueller Scan	Veränderung
Score	41/100	41/100	● 0
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

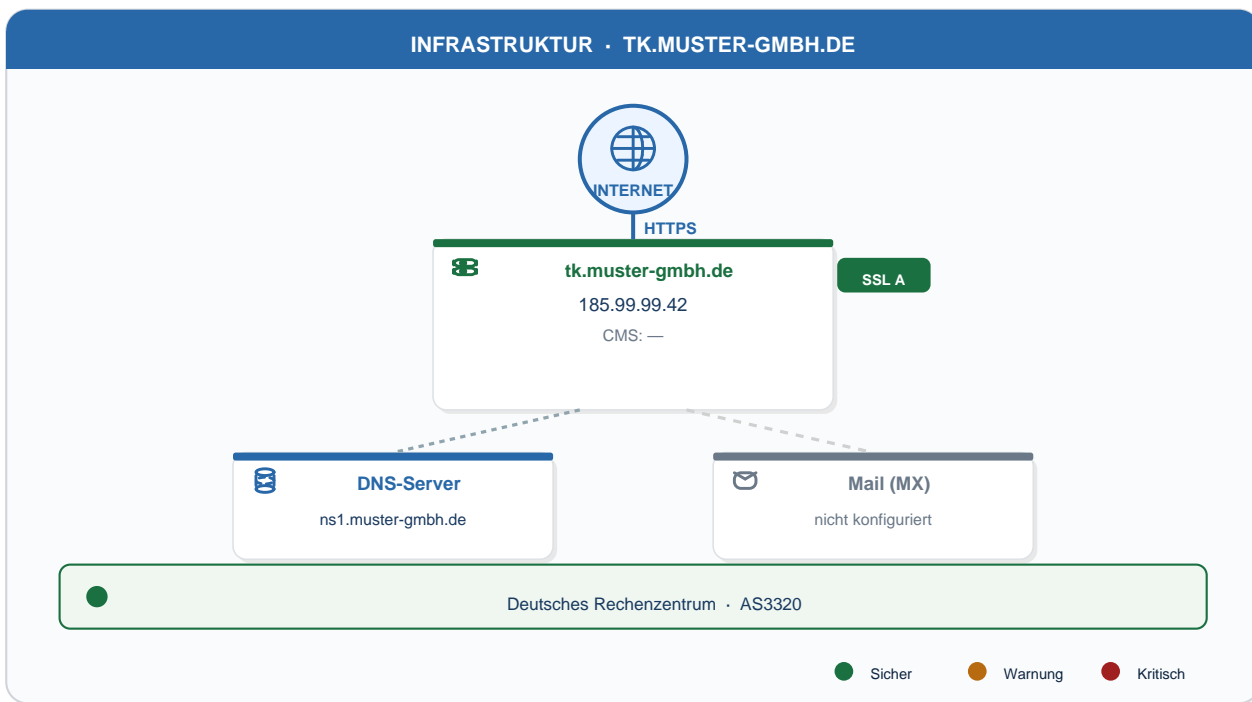
Hinweis: Die Seitenzahlen sind dynamisch und hängen vom Umfang der Analyseergebnisse ab.

## Analyseumfang & Hinweise

Analyseumfang & Hinweise	
Analysezeitpunkt	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 **tk.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.



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

## Domain & Hosting

Domain	tk.muster-gmbh.de
IP-Adresse	185.99.99.42
Reverse-DNS	sip-gw.muster-gmbh.de
Registrar	United Domains AG
Domain-Alter	2014-06-17
Ablauf in	2026-06-17
Aktualisiert	-
Name-Server	-
DNSSEC	Aktiv
IPv6 (AAAA)	Nicht konfiguriert
Hosting-Anbieter	-
Standort	DE
ASN	AS3320
DSGVO-Hosting	Ausserhalb EU: DE

## DNS-Konfiguration

A-Records (IPv4)	185.99.99.42
AAAA-Records (IPv6)	Nicht vorhanden
NS-Records	ns1.muster-gmbh.de

CAA-Record	Nicht vorhanden – jede CA kann Zertifikate ausstellen
DNSSEC	Aktiv – DNS kryptographisch signiert

---

## 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	Let's Encrypt
Zertifikat fuer	CN=tk.muster-gmbh.de
Gueltig ab	-
Gueltig bis	2026-07-04 (noch 62 Tage)
HSTS	Nicht konfiguriert
SSL-Grade	A
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	Auerswald PBX-Webgui
Betrieben mit	-
CMS	—
Generator	-
Programmiersprache	—
JavaScript-Frameworks	-
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.

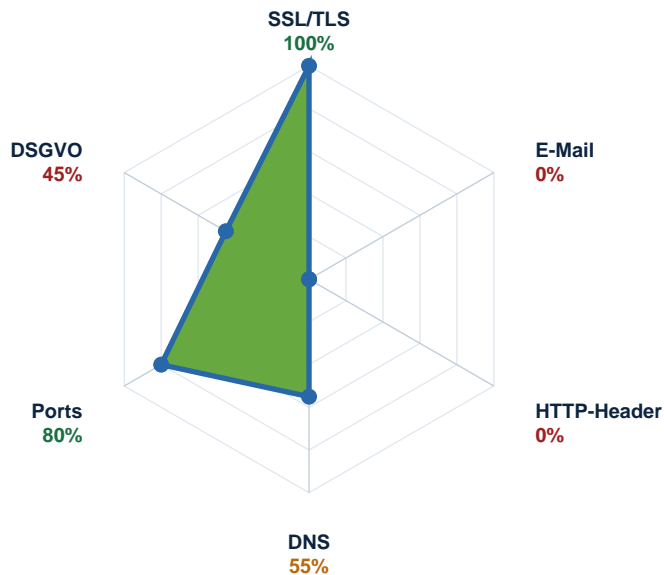
## Port-Scan & Angriffsfläche

Gescannte IP: **185.99.99.42** | 4 offene Port(s) gefunden von 22 geprüften

Port	Dienst	Risiko	Beschreibung	Banner
443	HTTPS	NIEDRIG	TK-Webgui (intern) — TLS aktiv	-
5060	SIP (UDP, Klartext)	HOCH	SIP-Trunk ohne Verschlüsselung — TLS nicht aktiv	-
5061	SIPS	NIEDRIG	SIP-TLS verfügbar — wird aber nicht genutzt	-
80	HTTP	MITTEL	Webgui-Portal ohne TLS — Login-Daten im Klartext	-

## 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	100%	Gut

E-Mail	0%	Kritisch
HTTP-Header	0%	Kritisch
DNS	55%	Verbesserungsbedarf
Ports	80%	Gut
DSGVO	45%	Kritisch

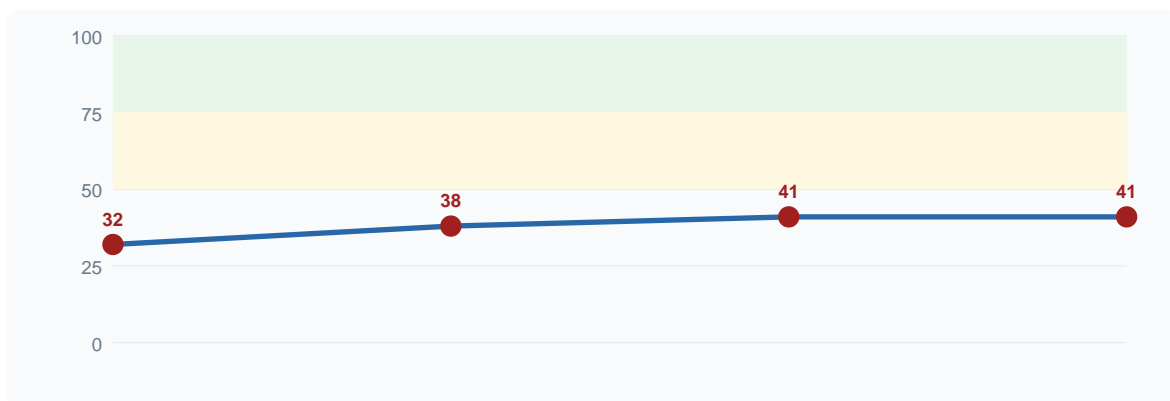
## DSGVO & Compliance

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: **↑ +9 Punkte Verbesserung** (von 32 auf 41 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	<b>Kein Backup der TK-Anlagen-Konfiguration</b> Wöchentliches Konfig-Backup auf separates System. Restore-Test halbjährlich.	1–2h	MITTEL
2	<b>Keine QoS-Priorisierung im Datennetz</b> DSCP-Marking auf SBC/Switch konfigurieren, QoS-Profil in Switches/Firewall akti	1–2h	MITTEL

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

P1	Maßnahme	Aufwand	Frist
<b>P1.1</b>	<b>Kein Toll-Fraud-Schutz aktiviert</b> Tarifsperrern konfigurieren (00, 0900, 118, Auslandsregionen). PIN-Authentifizierung für Außerhaus-Te	1–2h	Sofort
<b>P1.2</b>	<b>SIP-Trunk unverschlüsselt (Klartext)</b> SIP-TLS auf Port 5061 aktivieren, SRTP für Medien-Streams.	2–4h	< 1 Woche
<b>P1.3</b>	<b>SIP-Registrierung mit schwachen Default-Credentials</b> Komplexe SIP-Passwörter (≥16 Zeichen), pro Endgerät individuell. Firewall-Regel: SIP-Registrierung n	2–4h	< 1 Woche
<b>P1.4</b>	<b>TK-Anlagen-Webgui ohne TLS / öffentlich erreichbar</b> HTTPS mit gültigem Zertifikat + Beschränkung auf VPN- oder Management-Netz.	2–4h	< 1 Woche
<b>P1.5</b>	<b>DECT-Verschlüsselung deaktiviert oder schwach</b> In der DECT-Basisstation: DSAA2 + DSC aktivieren, ggf. Firmware-Update einspielen.	1–2h	< 1 Woche
<b>P1.6</b>	<b>Notruf-Standortdaten nicht hinterlegt</b> Pro Standort/Stockwerk eigene Routing-Regel mit ortsbezogener Notruf-Nummer. Test-Anruf bei 110/112	1–2h	Sofort
<b>P1.7</b>	<b>Telefon-Aufzeichnungen ohne Einwilligungs-Ansage</b> Begrüßungsansage erweitern: „Dieses Gespräch wird zu Qualitätzwecken aufgezeichnet. Wenn Sie damit	2–4h	< 1 Woche
<b>P1.8</b>	<b>TK-Anlagen-Firmware veraltet (CVE-relevant)</b> Firmware-Update einspielen. Pflege-Vertrag mit Hersteller prüfen — bei Auslauf Migrationspfad aufste	30 Min–2h	< 1 Woche

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

P2.1 23 % der Nebenstellen ungenutzt (kein Anruf seit 6 Monaten) – Nebenstellen prüfen: ehemalige Mitarbeiter, ausgemusterte RÄ

P2.2 Tarifmodell suboptimal (Provider-Vertrag älter als 4 Jahre) – Marktanfrage / Wettbewerbsanalyse. Bei öffentlichem Auftrag

## Handlungsempfehlungen (Detail)

### Sofortiger Handlungsbedarf (Kritisch / Hoch)

<b>KRITISCH</b>	<p><b>Kein Toll-Fraud-Schutz aktiviert</b></p> <p>Die TK-Anlage erlaubt internationale Sonderrufnummern ohne PIN-/Limit-Begrenzung. Bei Kompromittierung eines Endgeräts oder VoIP-Accounts können binnen Stunden Premium-Rate-Schäden im fünfstelligen Bereich entstehen (typischer Wochenend-Angriff: 8.000–35.000 €).</p> <p>&gt; <i>Tarifsperrern konfigurieren (00, 0900, 118, Auslandsregionen). PIN-Authentifizierung für Außerhaus-Telefonate. Tageslimit pro Nebenstelle.</i></p>
-----------------	--

<b>HOCH</b>	<p><b>SIP-Trunk unverschlüsselt (Klartext)</b></p> <p>Die SIP-Verbindung zum SIP-Provider läuft über UDP/5060 ohne TLS-Verschlüsselung. Gespräche und Anmeldedaten werden im Klartext übertragen. Mitlesen / Mithören durch Dritte am Übertragungsweg möglich.</p> <p>&gt; <i>SIP-TLS auf Port 5061 aktivieren, SRTP für Medien-Streams.</i></p>
<b>HOCH</b>	<p><b>SIP-Registrierung mit schwachen Default-Credentials</b></p> <p>Mehrere SIP-Endgeräte verwenden Standard-Passwörter (admin/1234, user/user). Dies ermöglicht SIP-Account-Übernahme und Anrufmissbrauch.</p> <p>&gt; <i>Komplexe SIP-Passwörter (≥ 16 Zeichen), pro Endgerät individuell. Firewall-Regel: SIP-Registrierung nur aus internem Netz.</i></p>
<b>HOCH</b>	<p><b>TK-Anlagen-Webgui ohne TLS / öffentlich erreichbar</b></p> <p>Das Administrations-Webinterface der TK-Anlage ist über HTTP (nicht HTTPS) und aus dem Internet ohne VPN erreichbar. Brute-Force-Angriffe und Credentials-Abfangen möglich.</p> <p>&gt; <i>HTTPS mit gültigem Zertifikat + Beschränkung auf VPN- oder Management-Netz.</i></p>
<b>HOCH</b>	<p><b>DECT-Verschlüsselung deaktiviert oder schwach</b></p> <p>Die DECT-Basisstationen senden ohne aktivierte Geräte-Authentisierung (DSAA2) und Medien-Verschlüsselung (DSC). Mit handelsüblicher Hardware können Gespräche mitgehört werden (gnu-radio + DECT-Sniffer).</p> <p>&gt; <i>In der DECT-Basisstation: DSAA2 + DSC aktivieren, ggf. Firmware-Update einspielen.</i></p>
<b>KRITISCH</b>	<p><b>Notruf-Standortdaten nicht hinterlegt</b></p> <p>Bei einem Notruf (110, 112) aus dem internen Netz wird keine korrekte Standortinformation an die Leitstelle übermittelt. Verstoß gegen TKG § 108 / EU-Kodex 2018/1972. Im Notfall verzögert die Identifikation des Anrufers.</p> <p>&gt; <i>Pro Standort/Stockwerk eigene Routing-Regel mit ortsbezogener Notruf-Nummer. Test-Anruf bei 110/112 (vorher mit Leitstelle abstimmen).</i></p>
<b>HOCH</b>	<p><b>Telefon-Aufzeichnungen ohne Einwilligungs-Ansage</b></p> <p>Eingehende Gespräche werden mitgeschnitten, ohne dass der Anrufer auf die Aufzeichnung hingewiesen wird. DSGVO Art. 6/13 + § 201 StGB („Verletzung der Vertraulichkeit des Wortes“).</p> <p>&gt; <i>Begrüßungsansage erweitern: „Dieses Gespräch wird zu Qualitätszwecken aufgezeichnet. Wenn Sie damit nicht einverstanden sind, drücken Sie 9.“ Opt-Out-Pfad bereitstellen.</i></p>
<b>HOCH</b>	<p><b>TK-Anlagen-Firmware veraltet (CVE-relevant)</b></p> <p>Die eingesetzte Firmware-Version weist 3 öffentlich dokumentierte CVE-Lücken auf, davon eine kritisch (CVSS 9.1). Hersteller hat Patch verfügbar.</p> <p>&gt; <i>Firmware-Update einspielen. Pflege-Vertrag mit Hersteller prüfen — bei Auslauf Migrationspfad aufstellen.</i></p>

## Kurzfristig umzusetzen (< 3 Monate)

<b>MITTEL</b>	<p><b>23 % der Nebenstellen ungenutzt (kein Anruf seit 6 Monaten)</b></p> <p>Aus der CDR-Auswertung: 47 von 205 Nebenstellen haben in den letzten 6 Monaten weder ein- noch ausgehende Gespräche geführt. Gebundene Lizenz-/Hardware-Kosten ohne Gegenwert — Einsparpotenzial ca. 280 €/Monat.</p> <p>&gt; <i>Nebenstellen prüfen: ehemalige Mitarbeiter, ausgemusterte Räume. Lizenz-Inventar konsolidieren, ungenutzte Anschlüsse abkündigen.</i></p>
---------------	---

<b>MITTEL</b>	<p><b>Tarifmodell suboptimal (Provider-Vertrag älter als 4 Jahre)</b></p> <p>Aktueller TK-Tarif aus 2021. Marktanalyse zeigt: bei vergleichbarem Volumen sind heute 18 % günstigere Tarife verfügbar (alle vier großen Anbieter). Einsparpotenzial pro Jahr: ca. 4.800 €.</p> <p>&gt; <i>Marktanfrage / Wettbewerbsanalyse. Bei öffentlichem Auftraggeber: Ausschreibung gemäß UVgO/VOB.</i></p>
<b>MITTEL</b>	<p><b>Kein Backup der TK-Anlagen-Konfiguration</b></p> <p>Es existiert kein dokumentiertes, regelmäßiges Backup der Anlagen-Konfiguration (Rufnummern, Wahlpläne, Berechtigungen). Bei Hardware-Defekt droht Wiederherstellungs-Aufwand mehrerer Tage.</p> <p>&gt; <i>Wöchentliches Konfig-Backup auf separates System. Restore-Test halbjährlich.</i></p>
<b>MITTEL</b>	<p><b>Keine QoS-Priorisierung im Datennetz</b></p> <p>VoIP-Pakete laufen ohne DSCP-Markierung (EF / 46) im selben Queue wie Daten-Verkehr. Bei Lastspitzen kommt es zu Aussetzern und Echo. Messbar in CDR: 12 % der Gespräche mit MOS-Score &lt; 3.5.</p> <p>&gt; <i>DSCP-Marking auf SBC/Switch konfigurieren, QoS-Profil in Switches/Firewall aktivieren, Bandbreite-Reservierung für VoIP.</i></p>

## Mittelfristig / Best Practice

<b>NIEDRIG</b>	<p><b>Wahlplan / Berechtigungs-Konzept nicht dokumentiert</b></p> <p>Die internen Wahlpläne (welche Nebenstelle darf wohin telefonieren?) sind nur im Kopf des damaligen Administrators. Bei Personalwechsel oder Hardware-Tausch fehlt die Grundlage für korrekte Wieder-Inbetriebnahme.</p> <p>&gt; <i>Wahlplan + Berechtigungs-Matrix dokumentieren (z. B. Ramses-Standard oder Excel-Vorlage). Halbjährliche Review.</i></p>
----------------	--

## 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>Kein Toll-Fraud-Schutz aktiviert</b> Tarifsperrern konfigurieren (00, 0900, 118, Auslandsregionen). PIN-Authentifizierung für Au	1–2h	IT-Dienstleister
2	<b>SIP-Trunk unverschlüsselt (Klartext)</b> SIP-TLS auf Port 5061 aktivieren, SRTP für Medien-Streams.	2–4h	IT-Dienstleister
3	<b>SIP-Registrierung mit schwachen Default-Credentials</b> Komplexe SIP-Passwörter (≥16 Zeichen), pro Endgerät individuell. Firewall-Regel: SIP-Regis	2–4h	IT-Dienstleister
4	<b>TK-Anlagen-Webgui ohne TLS / öffentlich erreichbar</b> HTTPS mit gültigem Zertifikat + Beschränkung auf VPN- oder Management-Netz.	2–4h	IT-Dienstleister
5	<b>DECT-Verschlüsselung deaktiviert oder schwach</b> In der DECT-Basisstation: DSAA2 + DSC aktivieren, ggf. Firmware-Update einspielen.	1–2h	IT-Dienstleister

6	<b>Notruf-Standortdaten nicht hinterlegt</b> Pro Standort/Stockwerk eigene Routing-Regel mit ortsbezogener Notruf-Nummer. Test-Anruf be	1–2h	IT-Dienstleister
---	--	------	------------------

### Phase 2: Kurzfristige Optimierung

Monat 1–2

Mittlere Befunde beheben und Basis-Sicherheitsstandards herstellen.

#	Maßnahme	Aufwand	Verantwortlich
1	<b>23 % der Nebenstellen ungenutzt (kein Anruf seit 6 Monaten)</b> Nebenstellen prüfen: ehemalige Mitarbeiter, ausgemusterte Räume. Lizenz-Inventar konsolidi	1–2h	IT-Dienstleister
2	<b>Tarifmodell suboptimal (Provider-Vertrag älter als 4 Jahre)</b> Marktanfrage / Wettbewerbsanalyse. Bei öffentlichem Auftraggeber: Ausschreibung gemäß UVgO	1–2h	IT-Dienstleister
3	<b>Kein Backup der TK-Anlagen-Konfiguration</b> Wöchentliches Konfig-Backup auf separates System. Restore-Test halbjährlich.	1–2h	IT-Dienstleister
4	<b>Keine QoS-Priorisierung im Datennetz</b> DSCP-Marking auf SBC/Switch konfigurieren, QoS-Profile in Switches/Firewall aktivieren, Ba	1–2h	IT-Dienstleister

### Phase 3: Langfristige Härtung

Quartal 1–2

Best Practices umsetzen, Monitoring einrichten und kontinuierliche Verbesserung sicherstellen.

#	Maßnahme	Aufwand	Verantwortlich
1	<b>Wahlplan / Berechtigungs-Konzept nicht dokumentiert</b> Wahlplan + Berechtigungs-Matrix dokumentieren (z. B. Ramses-Standard oder Excel-Vorlage).	1–2h	IT-Dienstleister

## Empfohlener Prüfrhythmus

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

## Begriffe, Abkürzungen & 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.*

<b>DNSSEC (DNS Security Extensions)</b>	
Kryptografische Signatur der DNS-Einträge. Verhindert, dass Angreifer gefälschte DNS-Antworten einschleusen (DNS-Spoofing).	<i>Massnahme: Aktivierung im Registrar-Panel und beim DNS-Provider. Erfordert Unterstützung durch Nameserver und Registrar.</i>
<b>A-Record / AAAA-Record</b>	
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.	<i>Massnahme: IPv6 beim Hoster aktivieren und AAAA-Record im DNS eintragen.</i>
<b>CAA-Record (Certification Authority Authorization)</b>	
Gibt an, welche Zertifizierungsstellen (CAs) SSL-Zertifikate für die Domain ausstellen dürfen. Ohne CAA kann jede CA ein Zertifikat ausstellen – Risiko für unberechtigte Zertifikate.	<i>Massnahme: CAA-Record im DNS hinzufügen, z. B.: 0 issue "letsencrypt.org"</i>
<b>SSL/TLS (Secure Sockets Layer / Transport Layer Security)</b>	
Protokoll zur Verschlüsselung der Datenübertragung zwischen Browser und Server (erkennbar an HTTPS). Veraltete Versionen (SSL, TLS 1.0/1.1) gelten als unsicher.	<i>Massnahme: Nur TLS 1.2 oder TLS 1.3 aktivieren. Veraltete Protokolle im Webserver deaktivieren.</i>
<b>SSL-Grade (A+, A, B, C, F)</b>	
Bewertung der SSL/TLS-Konfiguration nach dem SSL Labs-Standard. A+ ist das Optimum, F bedeutet kritische Sicherheitslücken.	<i>Massnahme: Webserver-Konfiguration anpassen: starke Cipher Suites, HSTS aktivieren, Forward Secrecy sicherstellen.</i>
<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 Drittseiten 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>

**Subdomains (Zertifikat-Transparenz-Logs)**

CT-Logs (Certificate Transparency) protokollieren alle ausgestellten SSL-Zertifikate öffentlich. Darüber können Subdomains eines Unternehmens aufgedeckt werden – auch interne oder vergessene.

*Massnahme: Alle aufgelisteten Subdomains prüfen: Nicht mehr benötigte abschalten, veraltete Systeme patchen, Sicherheitsniveau angleichen.*

## Risikobilanz in Euro — Vorstands-Übersicht

Erwarteter Gesamtschaden bei Realisierung aller Befunde	<b>417.600 €</b>
Risikoerwartungswert (gewichtet × Eintrittswahrscheinlichkeit)	<b>146.480 €</b>
Bandbreite (Best-/Worst-Case)	<b>92.320 € ... 2.064.000 €</b>
Branchen-Faktor angewendet	<b>MITTELSTAND (×1.6)</b>
Aufwand zur Behebung (alle Befunde)	<b>40.0 h · 5.800 € netto</b>
Risiko-Hebel (ROI-Faktor)	<b>25.3 ×</b> 1 € Investition wendet ca. 25.3 € 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-Kompendium 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:**

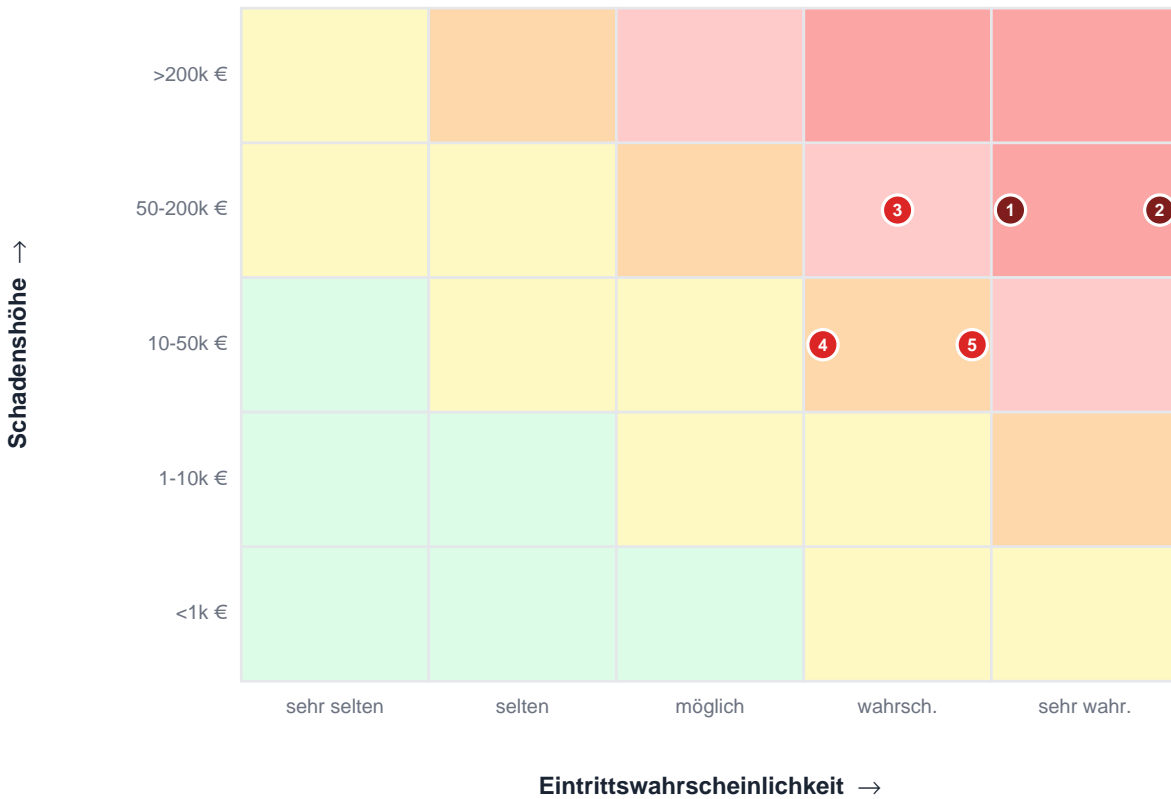
Befund „DMARC-Record nicht gesetzt“ (Severity „kritisch“):

- 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	Notruf-Standort fehlt	KRITISCH	128.000 €	57.600 €
2	Toll-Fraud-Schutz fehlt	KRITISCH	56.000 €	25.200 €
3	TK-Firmware veraltet, CVE	HOCH	60.800 €	18.240 €
4	SIP-Trunk unverschlüsselt	HOCH	35.200 €	10.560 €
5	SIP-Default-Passwörter	HOCH	28.800 €	8.640 €

## § 1 NIS-2-Konformitäts-Bewertung

NIS-2-Status	<b>WICHTIGE Einrichtung</b>
Sektor-Klassifikation	Anhang II — Verarbeitendes Gewerbe
NIS-2-Reifegrad	88 %
Bereiche mit Befund	0 kritische / 10 gesamt

Art. 21 Abs. 2	Maßnahmenbereich	Reife	Befunde
lit. a	Risikomanagement-Konzept	80 %	1 x
lit. b	Vorfallbewältigung	100 %	✓
lit. c	Geschäftskontinuität / Backup	100 %	✓
lit. d	Sicherheit der Lieferkette	100 %	✓
lit. e	Sicherheit bei Beschaffung, Entwicklung, Wartung	80 %	1 x
lit. f	Wirksamkeitsbewertung	80 %	1 x
lit. g	Cyberhygiene & Schulungen	80 %	1 x
lit. h	Kryptografie & Verschlüsselung	100 %	✓
lit. i	Personalsicherheit & Zugriffskontrolle	80 %	1 x
lit. j	Multi-Faktor-Authentisierung & sichere Kommunikation	80 %	1 x

**Bewertung:** Im NIS-2-Geltungsbereich (Anhang II — Verarbeitendes Gewerbe). NIS-2-Reife ist hoch (88 %).  
Empfohlen: jährliches externes Audit + Geschäftsleitungs-Schulung nach § 38 NIS2UmsuCG.

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

Im Rahmen dieses externen Audits wurden **20 der 93 Annex-A-Controls** automatisiert geprüft. Coverage: **80 %** der prüfbaren Controls erfüllt (16 ohne Befund, 4 mit Befund).

Control	Inhalt	Befunde	Severity
A.5.7	Threat Intelligence (CVE-Tracking, Schwachstellen-Monitoring)	1	HOCH
A.8.20	Netzwerksicherheit (Firewall, geschlossene Ports)	1	HOCH
A.8.21	Sicherheit von Netzwerkdiensten (TLS, sichere Protokolle)	1	HOCH
A.8.8	Verwaltung technischer Schwachstellen (CVE-Patching)	1	HOCH

**Empfehlung:** ISO/IEC 27001:2022-Reifegrad: 80 % der prüfbaren Controls erfüllt. 4 Controls weisen Befunde auf. Maßnahmen aus der Roadmap umsetzen, dann erneut prüfen — Zertifizierungs-Reife in 6–12 Monaten realistisch.

## § 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)	✓ Erfüllt	TLS-Konfiguration siehe Abschnitt SSL/TLS
Vertraulichkeit personenbezogener Daten (lit. b)	✓ Erfüllt	Drittanbieter-Tracker siehe DSGVO-Abschnitt
Verfügbarkeit / Belastbarkeit (lit. b)	x 1 riskante Ports	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)		2 Maßnahmen	
#	Maßnahme	Severity	Risiko-Hebel
1	Toll-Fraud-Schutz fehlt	KRITISCH	25.200 €
2	Notruf-Standort fehlt	KRITISCH	57.600 €

Kurzfristig (≤ 30 Tage)		6 Maßnahmen	
#	Maßnahme	Severity	Risiko-Hebel
1	SIP-Trunk unverschlüsselt	HOCH	10.560 €
2	SIP-Default-Passwörter	HOCH	8.640 €
3	TK-Webgui ohne TLS / public	HOCH	5.760 €
4	DECT-Verschlüsselung schwach	HOCH	7.680 €
5	Aufzeichnung ohne Einwilligung	HOCH	6.720 €
6	TK-Firmware veraltet, CVE	HOCH	18.240 €

Mittelfristig (≤ 90 Tage)		5 Maßnahmen	
#	Maßnahme	Severity	Risiko-Hebel
1	Ungenutzte Nebenstellen 23%	MITTEL	1.200 €
2	Tarif veraltet, Einsparpotenzial	MITTEL	1.920 €
3	Kein TK-Konfig-Backup	MITTEL	1.920 €
4	Keine VoIP-QoS	MITTEL	960 €
5	Wahlplan undokumentiert	NIEDRIG	80 €

## § 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. Notruf-Standortdaten korrekt routen (TKG § 108)

*Befund:* Notruf-Standort fehlt

Bei Notrufen aus VoIP-Anlagen wird ohne explizite Konfiguration meist die Hauptstandort-Adresse übermittelt. Bei mehreren Standorten / Stockwerken verzögert das die Identifikation. EU-Kodex 2018/1972 + TKG § 108 Pflicht — in Deutschland seit 21.12.2020 verbindlich.

#### ► 3CX: Standort-basiertes Notruf-Routing

1. Settings → Outbound Rules → "Emergency".
2. Pro Standort eine Regel: Pattern "110|112" → SIP-Trunk dieses Standorts.
3. Settings → Phones → pro Mobilteil "Office Location" zuordnen.
4. Test-Anruf vorher mit der Leitstelle abstimmen!

#### ► Auerswald: Standort-Kennung pro Nebenstelle

1. Konfigurator → "Anschlüsse" → SIP-Provider → "Notruf"-Tab.
2. Pro Provider die Standort-Adresse hinterlegen (Straße, Stadt, Stockwerk).
3. Pro Nebenstelle: Provider zuordnen → Notrufe gehen über den jeweils richtigen.

■ *Vor der Umsetzung beachten: TEST-NOTRUFE NIEMALS OHNE VORANMELDUNG bei der Leitstelle (110/112) durchführen — sonst rückt eine Streife aus. Stattdessen: Provider-Test-Notrufnummer (variiert).*

### [KRITISCH] 2. Toll-Fraud-Schutz: Tarifsperren + PIN

*Befund:* Toll-Fraud-Schutz fehlt

Premium-Rate-Anrufe (00-Auslandsgespräche, 0900-Mehrwert) sind das lukrativste Ziel kompromittierter VoIP-Anlagen. Standard: Wochenend-Angriff mit 5-stelligem Schaden. Schutz: Tagessperre + PIN für Auslandsgespräche + Tageslimit pro Nebenstelle.

#### ► Auerswald (COMfortel-/COMpact-Serie)

1. Konfigurations-Manager → "Berechtigungen" → "Externe Rufnummern".
2. Verbotene Vorwahlen: 00, 0900, 0137, 0181, 0190.
3. PIN-Sperre: "Externe Sonderwahl" → PIN aktivieren (mind. 6 Stellen).
4. Tageslimits pro Nebenstelle: "Verbindungslimit/Tag" auf z. B. 50 Min Ausland.

#### ► 3CX

1. Settings → Outbound Rules → New rule.
2. Pattern: "00.\*" oder "0900.\*" → Block.
3. Settings → Phones → "Outbound calls allowed: Office hours only".
4. Settings → Security → Anti-Hacking-Profil aktivieren.

#### ► STARFACE

1. Admin → Routing → Wahlregeln.
2. Neue Regel: "Sperrliste" - Vorwahlen 00, 0900, 0137 zuordnen.
3. Admin → Benutzer → Berechtigungs-Profile → "Externe Rufnummern: nur Festnetz inland".

■ *Vor der Umsetzung beachten: Bei Cloud-PBX (Sipgate, easybell, Telekom Cloud-PBX): Tarifsperren werden oft beim Provider gesetzt, nicht in der Anlage selbst.*

### [HOCH] 3. CVE „hoch“ zeitnah patchen (≤ 14 Tage)

*Befund:* TK-Firmware veraltet, CVE

Standard-Patching-Window für High-Severity-CVEs.

### ► Standard-Vorgehen

Wie bei "cve\_kritisch", aber Patching-Fenster: 14 Tage statt 24 h.  
Wenn das interne IT-Team das nicht im SLA hat: externer IT-Dienstleister.

## [HOCH] 4. SSH/Telnet/FTP härten

*Befund:* SIP-Trunk unverschlüsselt

SSH ist oft notwendig, aber Brute-Force-Versuche kommen täglich. Telnet/FTP haben keine Existenzberechtigung mehr.

### ► OpenSSH /etc/ssh/sshd\_config

```
# Schlüssel-only, kein Passwort, fail2ban:
PermitRootLogin no
PasswordAuthentication no
KbdInteractiveAuthentication no
PubkeyAuthentication yes
MaxAuthTries 3
LoginGraceTime 30
```

### ► fail2ban-Konfiguration

```
[sshd]
enabled = true
bantime = 86400
findtime = 600
maxretry = 3
```

## § 5 E-Mail-Sicherheit (Deep-Scan)

<b>SPF — All-Modus</b>	-all	✓ optimal
<b>SPF — DNS-Lookups</b>	3 / 10 erlaubt	✓
<b>DMARC — Policy</b>	p=quarantine (pct=100)	gut
<b>DMARC — RUA-Reports</b>	mailto:dmarc@muster-gmbh.de	✓
<b>DKIM — Selektoren gefunden</b>	1 / 18 geprüft	✓
<b>DKIM — Schlüsselstärke</b>	2048 bit	✓
<b>BIMI (Logo-Sichtbarkeit)</b>	nicht konfiguriert	Bonus für Markensichtbarkeit
<b>DNS-Blacklist-Status</b>	✓ sauber in allen geprüften Listen	Spamhaus ZEN, SpamCop, SORBS, Barracuda

## § 6 IP-Reputation & Threat-Intelligence

<b>IP-Adresse</b>	185.99.99.42	
<b>ISP</b>	Deutsche Telekom AG	DE
<b>Nutzungstyp</b>	Business	
<b>AbuseIPDB Confidence</b>	0 / 100	SAUBER
<b>Total Reports (90 Tage)</b>	0	

<b>Tor-Exit-Node</b>	✓ Nein	
<b>Gesamtbewertung</b>	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@twiconsult.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