Specter

Defensive Security Intelligence

Sicherheitsbericht · **Muster GmbH**
Erstellt: 2026-07-02 09:00 · Autorisiert durch: Geschäftsführung Muster GmbH · Referenz: BEISPIEL-2026-0001 (fiktiv)

Executive Summary

Im autorisierten Prüfumfang wurden **127 Finding(s)** und **5 Angriffspfad(e)** über **4 Asset(s)** identifiziert, davon **9 kritische** und **53 hohe** Risiken.

Wichtigste Risiken:

- Kritisch Root-Konto besitzt Access-Keys *(123456789012)*
- Kritisch Admin-Rolle von beliebigem Prinzipal annehmbar: ci-deploy *(ci-deploy)*
- Kritisch Root-Konto ohne MFA *(123456789012)*
- Kritisch Privilegiertes Konto ohne MFA: admin@mustermann.de *(admin@mustermann.de)*
- Kritisch Privilegierter Container: legacy-web *(legacy-web)*

Risiko-Einstufung

Schweregrad	Anzahl
Kritisch	9
Hoch	53
Mittel	39
Niedrig	26
Info	0

Angriffspfade (toxische Kombinationen)

AP-1: Domänenübernahme über exponierten Fernzugang Kritisch **· 4 Kombinationen**

1. Fernzugang identifizieren: fw-hq-fortigate/management (SSH-Fernzugang der Firewall öffentlich erreichbar)
2. Zugangsdaten verwenden: Standard-/Default-Zugangsdaten: mysql
3. Im internen Netz Fuß fassen und Rechte ausweiten (Domain Admin)
4. Netzwerkweite Kompromittierung / Ransomware-Ausbringung möglich

Offene RDP-/VPN-Zugänge sind der häufigste Ransomware-Einstieg im Mittelstand; zusammen mit schwachen oder geleakten Zugangsdaten führt das direkt ins interne Netz. Zusammengefasst aus 4 gleichartigen Kombinationen.

AP-2: DSGVO-meldepflichtiger Datenabfluss (Art. 33/34) Kritisch

1. Schwachstelle ausnutzen: Root-Konto besitzt Access-Keys (123456789012)
2. Zugriff auf personenbezogene Daten: mustermann.onmicrosoft.com
3. Datenabfluss -> Meldepflicht binnen 72 h an die Aufsichtsbehörde

Ein Abfluss personenbezogener Daten löst nach Art. 33/34 DSGVO eine Melde- und ggf. Benachrichtigungspflicht aus (Bußgeldrisiko bis 4 % des Jahresumsatzes).

AP-3: Ausnutzung bekannter Schwachstelle in veralteter Komponente Kritisch **· 6 Kombinationen**

1. Veraltete Komponente erkennen: Veraltete Exchange-Version (Build 15.1.2044.4) (mail.mustermann.de)
2. Öffentlich bekannte Schwachstelle (CVE/Exploit) recherchieren
3. Gegen erreichbaren Dienst ausnutzen: 00000000-1111-2222-3333-444444444444/nsg/nsg-db

Veraltete, von außen erreichbare Komponenten (z. B. altes Exchange, Log4j, alte VPN-Gateways) haben oft öffentlich verfügbare Exploits. Zusammengefasst aus 6 gleichartigen Kombinationen.

AP-4: Rechteausweitung über schwache Auth und Zugriffskontrolle Hoch

1. Schwache Authentifizierung überwinden: Root-Konto ohne MFA
2. Fehlerhafte Zugriffskontrolle ausnutzen: Root-Konto besitzt Access-Keys
3. Auf Ressourcen fremder Nutzer/Rollen zugreifen

Schwache Anmeldung senkt die Einstiegshürde; fehlende Objekt-Zugriffskontrolle erlaubt danach horizontale/vertikale Rechteausweitung.

AP-5: Direkter Datenzugriff über offenen Cloud-Speicher Hoch **· 2 Kombinationen**

1. Öffentlich erreichbaren Speicher identifizieren: 00000000-1111-2222-3333-444444444444/storage/mustermannsa
2. Ohne Authentifizierung auf abgelegte Daten zugreifen

Fehlkonfigurierter Speicher gibt Daten ohne Zugangskontrolle preis. Zusammengefasst aus 2 gleichartigen Kombinationen.

Choke Points (engste Behebungsstellen)

Diese Findings zuerst beheben – jedes bricht mehrere Angriffspfade auf einmal:

- **Root-Konto besitzt Access-Keys** (123456789012) → bricht 2 Angriffspfad(e)
- **Verwundbare Abhängigkeit: django 2.2.0 (CVE-2022-28346)** (portal-backend/pypi/django) → bricht 1 Angriffspfad(e)
- **Öffentlicher Blob-Zugriff auf Storage-Account: mustermannsa** (00000000-1111-2222-3333-444444444444/storage/mustermannsa) → bricht 1 Angriffspfad(e)
- **SSH aus dem Internet erreichbar: ssh-admin** (fw-hq-fortigate/rule/ssh-admin) → bricht 1 Angriffspfad(e)

Quick Wins (kurzfristig, hohe Wirkung)

- **Standard-/Default-Zugangsdaten: mysql** (mysql:3306): Alle Standard-/Default-Zugangsdaten ändern, ungenutzte Konten deaktivieren, starke Passwort-Richtlinie und MFA durchsetzen.
- **Veraltete Exchange-Version (Build 15.1.2044.4)** (mail.mustermann.de): Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.
- **Verwundbare Abhängigkeit: log4j-core 2.14.1 (CVE-2021-44228)** (portal-backend/maven/log4j-core): Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.
- **Key Vault öffentlich erreichbar: kv-prod** (00000000-1111-2222-3333-444444444444/keyvault/kv-prod): Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.
- **Any-Any-Freigabe in der Firewall: permit-any-out** (fw-hq-fortigate/rule/permit-any-out): Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.
- **Exchange-ECP (Admin-Oberfläche) extern erreichbar** (mail.mustermann.de): Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

- **Weder Security Defaults noch Conditional Access aktiv** (mustermann.onmicrosoft.com): Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.
- **VM mit veraltetem Betriebssystem: vm-legacy-app** (00000000-1111-2222-3333-444444444444/vm/vm-legacy-app): Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.
- **Veraltetes/abgekündigtes VPN-Gateway: site-to-site-legacy** (fw-hq-fortigate/vpn/site-to-site-legacy): Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.
- **Verwundbare Abhängigkeit: django 2.2.0 (CVE-2022-28346)** (portal-backend/pypi/django): Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.
- **SSH-Fernzugang der Firewall öffentlich erreichbar** (fw-hq-fortigate/management): Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.
- **RDP aus dem Internet erreichbar: rdp-support** (fw-hq-fortigate/rule/rdp-support): Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.
- **SSH aus dem Internet erreichbar: ssh-admin** (fw-hq-fortigate/rule/ssh-admin): Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.
- **VPN-Zugang ohne MFA: site-to-site-legacy** (fw-hq-fortigate/vpn/site-to-site-legacy): Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.
- **Kein HSTS (Strict-Transport-Security): https://portal.musterversicherung.de** (https://portal.musterversicherung.de): TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.
- **Schwache TLS-Protokolle aktiv: tlsv1.0** (mail.mustermann.de): TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.
- **TLS-Zertifikat abgelaufen: portal.musterversicherung.de:443** (portal.musterversicherung.de:443/certificate): TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.
- **Veraltetes TLS-/SSL-Protokoll aktiv (SSLv3): portal.musterversicherung.de:443** (portal.musterversicherung.de:443/protocols): TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

Langfristige Maßnahmen

- Least-Privilege und regelmäßige Berechtigungs-Rezertifizierung (BSI ORP.4).
- Identitäts- und Berechtigungsmanagement härten, MFA flächendeckend (BSI ORP.4).
- Zentrales Passwort-/Secret-Management und MFA (BSI ORP.4).
- Patch- und Schwachstellenmanagement etablieren (BSI OPS.1.1.3), inkl. Software-Inventar (SBOM).
- Cloud-Sicherheitskonzept und sichere Grundkonfiguration (BSI OPS.2.2).
- Kryptokonzept nach BSI CON.1 umsetzen.
- Netzsegmentierung und striktes Firewall-Regelwerk (BSI NET.1.1).
- Zero-Trust-Fernzugang mit MFA statt offenem RDP/VPN (BSI OPS.1.2.5).
- TLS-Härtung und Kryptokonzept (BSI CON.1).
- Datenschutz-Managementsystem und Verschlüsselungskonzept (DSGVO, BSI CON.2).

Technische Findings

SPEC-9f347b98: Root-Konto besitzt Access-Keys

Kritisch

CVSS-Lite: 9.7 (Kritisch) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-250 · Asset: 123456789012 · Fundstelle: 123456789012 · Quelle: aws_analyzer

```
root_account.access_keys=1 (Root-Keys vermeiden)
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-f7da8fca: Admin-Rolle von beliebigem Prinzipal annehmbar: ci-deploy

Kritisch

CVSS-Lite: 9.7 (Kritisch) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-284 · Asset: ci-deploy · Fundstelle: 123456789012/role/ci-deploy · Quelle: aws_analyzer

```
trust='*' und administrative Policy
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-81ea1be3: Root-Konto ohne MFA

Kritisch

CVSS-Lite: 9.5 (Kritisch) · Kategorie: Schwache Authentifizierung · CWE-308 · Asset: 123456789012 · Fundstelle: 123456789012 · Quelle: aws_analyzer

```
root_account.mfa_enabled=false
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-11ba2f6f: Privilegiertes Konto ohne MFA: admin@mustermann.de

Kritisch

CVSS-Lite: 9.5 (Kritisch) · Kategorie: Schwache Authentifizierung · CWE-308 · Asset: admin@mustermann.de · Fundstelle: mustermann.onmicrosoft.com/admin@mustermann.de · Quelle: entra_analyzer

```
privileged=true, mfa_registered=false
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-1ebb5973: Privilegierter Container: legacy-web

Kritisch

CVSS-Lite: 9.6 (Kritisch) · Kategorie: Container-/Docker-Sicherheit · CWE-250 · Asset: legacy-web · Fundstelle: legacy-web · Quelle: container_analyzer

```
--privileged hebt nahezu alle Isolation auf - faktisch Root-Zugriff auf den Host
```

Gegenmaßnahme: Container härten: nicht privilegiert und als unprivilegierter Benutzer laufen (USER != root), das Docker-Socket niemals in Container mounten, Host-Networking vermeiden, nur die minimal nötigen Capabilities vergeben (--cap-drop=ALL, gezielt einzelne --cap-add), Images mit festem Tag/Digest pinnen (kein :latest) und regelmäßig aktualisieren, Ports nur auf benötigte Quell-IPs/127.0.0.1 veröffentlichen und den Docker-Daemon nicht ungeschützt exponieren.

SPEC-566a535b: Docker-Socket im Container gemountet: legacy-web

Kritisch

CVSS-Lite: 9.6 (Kritisch) · Kategorie: Container-/Docker-Sicherheit · CWE-250 · Asset: legacy-web · Fundstelle: legacy-web · Quelle: container_analyzer

```
/var/run/docker.sock im Container = vollständige Kontrolle über den Docker-Daemon und damit den Host
```

Gegenmaßnahme: Container härten: nicht privilegiert und als unprivilegierter Benutzer laufen (USER != root), das Docker-Socket niemals in Container mounten, Host-Networking vermeiden, nur die minimal nötigen Capabilities vergeben (--cap-drop=ALL, gezielt einzelne --cap-add), Images mit festem Tag/Digest pinnen (kein :latest) und regelmäßig aktualisieren, Ports nur auf benötigte Quell-IPs/127.0.0.1 veröffentlichen und den Docker-Daemon nicht ungeschützt exponieren.

SPEC-7875a860: Standard-/Default-Zugangsdaten: mysql

Kritisch

CVSS-Lite: 9.8 (Kritisch) · Kategorie: Standard-/Default-Zugangsdaten · CWE-798 · Asset: mysql:3306 · Fundstelle: mysql:3306 · Quelle: database_analyzer

```
Aktive Default-Zugangsdaten - sofort ändern; öffentlich bekannt und erstes Angriffsziel
```

Gegenmaßnahme: Alle Standard-/Default-Zugangsdaten ändern, ungenutzte Konten deaktivieren, starke Passwort-Richtlinie und MFA durchsetzen.

SPEC-6ed63e86: Veraltete Exchange-Version (Build 15.1.2044.4)

Kritisch

CVSS-Lite: 9.7 (Kritisch) · Kategorie: Veraltete Komponente/Abhängigkeit (bekannte CVE) · CWE-1104 · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de · Quelle: exchange_analyzer

```
Exchange 2016 Build 15.1.2044.4 < Richtwert 15.1.2507 - möglicherweise anfällig für ProxyLogon (CVE-2021-26855) / ProxyShell (CVE-2021-34473)
```

Gegenmaßnahme: Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.

SPEC-2fc81ec0: Verwundbare Abhängigkeit: log4j-core 2.14.1 (CVE-2021-44228)

Kritisch

CVSS-Lite: 9.7 (Kritisch) · Kategorie: Veraltete Komponente/Abhängigkeit (bekannte CVE) · CWE-1395 · Asset: portal-backend/maven/log4j-core · Fundstelle: portal-backend/maven/log4j-core · Quelle: dependency_analyzer

```
Version 2.14.1 erfüllt Advisory CVE-2021-44228 (verwundbar: <2.15.0; behoben in 2.17.1) - Log4Shell Remote Code Execution
```

Gegenmaßnahme: Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.

SPEC-0f4408c1: Zu viele Subscription-Owner (4)

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-269 · Asset: 00000000-1111-2222-3333-444444444444 · Fundstelle: 00000000-1111-2222-3333-444444444444/rbac · Quelle: azure_analyzer

```
4 Owner auf Subscription-Ebene (Empfehlung <= 3)
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-39fe66f1: Überprivilegierter IAM-User (Admin): deploy-bot

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-269 · Asset: deploy-bot · Fundstelle: 123456789012/user/deploy-bot · Quelle: aws_analyzer

```
attached_policies=['AdministratorAccess']
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-60bc5404: Zu viele privilegierte Konten in 'Domain Admins' (9)

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-269 · Asset: mustermann.local · Fundstelle: mustermann.local/Domain Admins · Quelle: ad_analyzer

```
Domain Admins: 9 Mitglieder (Richtwert <= 8)
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-00cc0dfd: Zu viele Konten in 'Global Administrator' (7)

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-269 · Asset: mustermann.onmicrosoft.com · Fundstelle: mustermann.onmicrosoft.com/Global Administrator · Quelle: entra_analyzer

```
Global Administrator: 7 Mitglieder (Empfehlung <= 5)
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-14595b9d: Überprivilegierte App-Registrierung: Alt-Sync-Tool

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-250 · Asset: mustermann.onmicrosoft.com · Fundstelle: mustermann.onmicrosoft.com/app/Alt-Sync-Tool · Quelle: entra_analyzer

```
admin_consent=true, Berechtigungen=['Directory.ReadWrite.All', 'Mail.Read']
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-abea65ca: IAM-Konsolenzugriff ohne MFA: deploy-bot

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-308 · Asset: deploy-bot · Fundstelle: 123456789012/user/deploy-bot · Quelle: aws_analyzer

```
console_access=true, mfa_enabled=false
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-8e58f5be: Kerberos-Pre-Auth deaktiviert (AS-REP-Roasting): m.weber

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-522 · Asset: m.weber · Fundstelle: mustermann.local/m.weber · Quelle: ad_analyzer

```
kerberos_preauth=false
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-073d540b: Passwort-Mindestlänge zu gering (8 < 12)

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-521 · Asset: mustermann.local · Fundstelle: mustermann.local · Quelle: ad_analyzer

```
password_policy.min_length = 8
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-595866cd: Passwort-Komplexität nicht erzwungen

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-521 · Asset: mustermann.local · Fundstelle: mustermann.local · Quelle: ad_analyzer

```
password_policy.complexity = false
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-beab5cf1: Keine Account-Lockout-Policy (Brute-Force ungebremst)

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-307 · Asset: mustermann.local · Fundstelle: mustermann.local · Quelle: ad_analyzer

```
password_policy.lockout_threshold = 0
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-00ea6f87: krbtgt-Passwort veraltet (1450 Tage) - Golden-Ticket-Risiko

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-324 · Asset: mustermann.local · Fundstelle: mustermann.local · Quelle: ad_analyzer

```
krbtgt_password_age_days = 1450 (> 180)
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-6da533f5: Keine MFA-Erzwingung (Security Defaults/CA)

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-308 · Asset: mustermann.onmicrosoft.com · Fundstelle: mustermann.onmicrosoft.com · Quelle: entra_analyzer

```
Keine aktive Richtlinie erzwingt MFA
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-59ddef66: Legacy-Authentifizierung nicht blockiert (Password-Spraying)

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-287 · Asset: mustermann.onmicrosoft.com · Fundstelle: mustermann.onmicrosoft.com · Quelle: entra_analyzer

```
legacy_auth_allowed=true, keine CA blockiert Legacy-Auth
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-21b52553: Datenbank ohne Authentifizierung: redis

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-306 · Asset: redis:6379 · Fundstelle: redis:6379 · Quelle: database_analyzer

```
Der Dienst verlangt keine Anmeldung - jeder mit Netzzugang kann lesen/schreiben (typisch bei Redis/MongoDB-Standardinstallationen)
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-6bdbf551: Privilegiertes Konto mit nie ablaufendem Passwort: svc-mssql

Hoch

CVSS-Lite: 7.9 (Hoch) · Kategorie: Schwache Authentifizierung · CWE-262 · Asset: svc-mssql · Fundstelle: mustermann.local/svc-mssql · Quelle: ad_analyzer

```
privileged=true, password_never_expires=true
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-d272723a: Restore-Test überfällig (400 Tage): erp-datenbank

Hoch

CVSS-Lite: 8.0 (Hoch) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-754 · Asset: Muster Versicherung AG/backup/erp-datenbank · Fundstelle: Muster Versicherung AG/backup/erp-datenbank · Quelle: backup_analyzer

```
last_restore_test_days=400 - mindestens jährlich testen
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-bcaae6c6: Höchstens eine Backup-Kopie (Single Point of Failure): fileserver-daily

Hoch

CVSS-Lite: 8.0 (Hoch) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-693 · Asset: Muster Versicherung AG/backup/fileserver-daily · Fundstelle: Muster Versicherung AG/backup/fileserver-daily · Quelle: backup_analyzer

```
copies=1 - 3-2-1-Regel verlangt mindestens 3 Kopien
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-5c31f48c: Kein offline-/unveränderbares (Immutable) Backup: fileserver-daily

Hoch

CVSS-Lite: 8.0 (Hoch) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-693 · Asset: Muster Versicherung AG/backup/fileserver-daily · Fundstelle: Muster Versicherung AG/backup/fileserver-daily · Quelle: backup_analyzer

```
offline_or_immutable=false - Ransomware kann erreichbare Backups mitverschlüsseln/löschen
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-6fee4a14: Keine Offsite-Kopie des Backups: fileserver-daily

Hoch

CVSS-Lite: 8.0 (Hoch) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-693 · Asset: Muster Versicherung AG/backup/fileserver-daily · Fundstelle: Muster Versicherung AG/backup/fileserver-daily · Quelle: backup_analyzer

```
offsite=false - kein Schutz gegen Standort-Totalverlust (Brand/Ransomware im LAN)
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-d3238e8e: Wiederherstellung nie getestet: fileserver-daily

Hoch

CVSS-Lite: 8.0 (Hoch) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-754 · Asset: Muster Versicherung AG/backup/fileserver-daily · Fundstelle: Muster Versicherung AG/backup/fileserver-daily · Quelle: backup_analyzer

```
restore_tested=false - ungetestete Backups sind im Ernstfall oft nicht wiederherstellbar
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-2e2444fa: Öffentlicher Blob-Zugriff auf Storage-Account: mustermannsa

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Offener/fehlkonfigurierter Cloud-Speicher · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Fundstelle: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Quelle: azure_analyzer

```
public_blob_access=true - Daten ohne Zugangskontrolle erreichbar
```

Gegenmaßnahme: Öffentlichen Zugriff auf Speicher/Buckets sperren, Least-Privilege-Policies setzen und Verschlüsselung im Ruhezustand aktivieren.

SPEC-7beab70b: Öffentlicher S3-Bucket: mustermann-kunden-backups

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Offener/fehlkonfigurierter Cloud-Speicher · CWE-284 · Asset: s3://mustermann-kunden-backups · Fundstelle: s3://mustermann-kunden-backups · Quelle: aws_analyzer

```
public=true - ohne Zugangskontrolle erreichbar
```

Gegenmaßnahme: Öffentlichen Zugriff auf Speicher/Buckets sperren, Least-Privilege-Policies setzen und Verschlüsselung im Ruhezustand aktivieren.

SPEC-f77359e5: Gefährliche Capabilities: legacy-web (NET_ADMIN, SYS_ADMIN)

Hoch

CVSS-Lite: 8.0 (Hoch) · Kategorie: Container-/Docker-Sicherheit · CWE-250 · Asset: legacy-web · Fundstelle: legacy-web · Quelle: container_analyzer

```
cap_add=['NET_ADMIN', 'SYS_ADMIN'] - ermöglicht Ausbruch/Host-Zugriff
```

Gegenmaßnahme: Container härten: nicht privilegiert und als unprivilegierter Benutzer laufen (USER != root), das Docker-Socket niemals in Container mounten, Host-Networking vermeiden, nur die minimal nötigen Capabilities vergeben (--cap-drop=ALL, gezielt einzelne --cap-add), Images mit festem Tag/Digest pinnen (kein :latest) und regelmäßig aktualisieren, Ports nur auf benötigte Quell-IPs/127.0.0.1 veröffentlichen und den Docker-Daemon nicht ungeschützt exponieren.

SPEC-d9e7a031: VPN mit schwacher Kryptographie: site-to-site-legacy

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Schwache Kryptographie · CWE-327 · Asset: fw-hq-fortigate/vpn/site-to-site-legacy · Fundstelle: fw-hq-fortigate/vpn/site-to-site-legacy · Quelle: firewall_analyzer

```
encryption=3des - veraltet, durch AES-256/SHA-256+ ersetzen
```

Gegenmaßnahme: Schwache Algorithmen (MD5/SHA1) durch SHA-256+ bzw. für Passwörter durch bcrypt/scrypt/Argon2 ersetzen. Keine Eigenbau-Kryptographie.

SPEC-cfe88ad8: TLS-Zertifikat mit schwacher Signatur: portal.musterversicherung.de:443

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Schwache Kryptographie · CWE-327 · Asset: portal.musterversicherung.de:443/certificate · Fundstelle: portal.musterversicherung.de:443/certificate · Quelle: tls_analyzer

```
signature_algorithm=sha1WithRSAEncryption - SHA-1/MD5 gelten als gebrochen
```

Gegenmaßnahme: Schwache Algorithmen (MD5/SHA1) durch SHA-256+ bzw. für Passwörter durch bcrypt/scrypt/Argon2 ersetzen. Keine Eigenbau-Kryptographie.

SPEC-eb3a7778: TLS-Zertifikat mit zu kurzem Schlüssel (1024 Bit): portal.musterversicherung.de:443

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Schwache Kryptographie · CWE-326 · Asset: portal.musterversicherung.de:443/certificate · Fundstelle: portal.musterversicherung.de:443/certificate · Quelle: tls_analyzer

```
key_type=RSA, key_bits=1024 - mindestens 2048
```

Gegenmaßnahme: Schwache Algorithmen (MD5/SHA1) durch SHA-256+ bzw. für Passwörter durch bcrypt/scrypt/Argon2 ersetzen. Keine Eigenbau-Kryptographie.

SPEC-3be756ee: Offener Zonentransfer (AXFR): musterversicherung.de

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: DNS-Sicherheit (DNSSEC/CAA/Zonentransfer) · CWE-200 · Asset: musterversicherung.de/AXFR · Fundstelle: musterversicherung.de/AXFR · Quelle: dns_analyzer

```
AXFR erlaubt - die komplette Zone (alle Hosts/Subdomains) ist abziehbar
```

Gegenmaßnahme: DNS absichern: DNSSEC aktivieren und die Zone signieren (Schutz vor Cache-Poisoning/Spoofing), CAA-Records setzen, damit nur autorisierte Zertifizierungsstellen ausstellen dürfen, Zonentransfer (AXFR) auf berechtigte Secondaries beschränken, Wildcard-Einträge vermeiden bzw. eng fassen und ungenutzte CNAME-Verweise (dangling) entfernen, um Subdomain-Takeover zu verhindern.

SPEC-66f4c521: Dangling CNAME (Subdomain-Takeover-Risiko): alt-portal.musterversicherung.de -> muster-portal.azurewebsites.net

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: DNS-Sicherheit (DNSSEC/CAA/Zonentransfer) · CWE-350 · Asset: musterversicherung.de/CNAME · Fundstelle: musterversicherung.de/CNAME · Quelle: dns_analyzer

```
alt-portal.musterversicherung.de -> muster-portal.azurewebsites.net - Ziel nicht mehr in Betrieb; übernehmbar durch Angreifer
```

Gegenmaßnahme: DNS absichern: DNSSEC aktivieren und die Zone signieren (Schutz vor Cache-Poisoning/Spoofing), CAA-Records setzen, damit nur autorisierte Zertifizierungsstellen ausstellen dürfen, Zonentransfer (AXFR) auf berechtigte Secondaries beschränken, Wildcard-Einträge vermeiden bzw. eng fassen und ungenutzte CNAME-Verweise (dangling) entfernen, um Subdomain-Takeover zu verhindern.

SPEC-eff3e013: SPF erlaubt beliebige Absender (+all/?all): musterversicherung.de

Hoch

CVSS-Lite: 8.0 (Hoch) · Kategorie: E-Mail-Spoofing/Phishing (SPF/DKIM/DMARC) · CWE-290 · Asset: musterversicherung.de/SPF · Fundstelle: musterversicherung.de/SPF · Quelle: email_security_analyzer

```
SPF=v=spf1 include:_spf.google.com +all - Qualifier hebt den Schutz praktisch auf
```

Gegenmaßnahme: E-Mail-Spoofing verhindern: SPF mit -all (bzw. mindestens ~all) setzen, DKIM mit >= 2048-Bit-Schlüssel signieren und DMARC schrittweise auf p=quarantine, dann p=reject anheben. rua-Reportadresse konfigurieren und die Berichte regelmäßig auswerten (Schutz vor CEO-Fraud/BEC).

SPEC-740f2a96: NSG offen ins Internet (0.0.0.0/0) auf Port 3389: nsg-db

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/nsg/nsg-db · Fundstelle: 00000000-1111-2222-3333-444444444444/nsg/nsg-db · Quelle: azure_analyzer

```
open_to_internet_ports enthält 3389
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-5ac988ef: NSG offen ins Internet (0.0.0.0/0) auf Port 1433: nsg-db

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/nsg/nsg-db · Fundstelle: 00000000-1111-2222-3333-444444444444/nsg/nsg-db · Quelle: azure_analyzer

```
open_to_internet_ports enthält 1433
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-808a27fa: Azure-SQL-Server öffentlich erreichbar: sql-kunden

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/sql/sql-kunden · Fundstelle: 00000000-1111-2222-3333-444444444444/sql/sql-kunden · Quelle: azure_analyzer

```
public_access=true
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-da15ca55: Security-Group offen ins Internet (0.0.0.0/0) auf Port 3306

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 123456789012/sg/db-sg · Fundstelle: 123456789012/sg/db-sg · Quelle: aws_analyzer

```
open_to_world_ports enthält 3306
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-509d3748: Security-Group offen ins Internet (0.0.0.0/0) auf Port 22

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 123456789012/sg/db-sg · Fundstelle: 123456789012/sg/db-sg · Quelle: aws_analyzer

```
open_to_world_ports enthält 22
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-ca4cb183: Management-Interface aus dem Internet erreichbar

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: fw-hq-fortigate/management · Fundstelle: fw-hq-fortigate/management · Quelle: firewall_analyzer

```
public=true, exposed=['https', 'ssh'] - Verwaltungsebene gehört nur ins interne/Out-of-Band-Netz
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-b0fed1ef: Sensibler Dienst offen ins Internet (MSSQL): db-exposed

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: fw-hq-fortigate/rule/db-exposed · Fundstelle: fw-hq-fortigate/rule/db-exposed · Quelle: firewall_analyzer

```
source=any -> Port 1433 (MSSQL)
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-35ebde7f: Datenbank öffentlich erreichbar: mysql

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-668 · Asset: mysql:3306 · Fundstelle: mysql:3306 · Quelle: database_analyzer

```
Der Datenbank-Port ist aus fremden Netzen erreichbar - gehört hinter Firewall/VPN, niemals offen ins Internet
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-3c0a33fd: Datenbank öffentlich erreichbar: redis

Hoch

CVSS-Lite: 7.8 (Hoch) · Kategorie: Exponierter Dienst/Port · CWE-668 · Asset: redis:6379 · Fundstelle: redis:6379 · Quelle: database_analyzer

```
Der Datenbank-Port ist aus fremden Netzen erreichbar - gehört hinter Firewall/VPN, niemals offen ins Internet
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-da8669ef: Key Vault öffentlich erreichbar: kv-prod

Hoch

CVSS-Lite: 7.5 (Hoch) · Kategorie: Fehlkonfiguration · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/keyvault/kv-prod · Fundstelle: 00000000-1111-2222-3333-444444444444/keyvault/kv-prod · Quelle: azure_analyzer

```
public_network_access=true - sollte privat sein
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-ef62db9d: Any-Any-Freigabe in der Firewall: permit-any-out

Hoch

CVSS-Lite: 7.5 (Hoch) · Kategorie: Fehlkonfiguration · CWE-284 · Asset: fw-hq-fortigate/rule/permit-any-out · Fundstelle: fw-hq-fortigate/rule/permit-any-out · Quelle: firewall_analyzer

```
action=allow, source=any, destination=any, service=any - hebt die Segmentierung praktisch auf
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-ae52a1f1: Exchange-ECP (Admin-Oberfläche) extern erreichbar

Hoch

CVSS-Lite: 7.5 (Hoch) · Kategorie: Fehlkonfiguration · CWE-284 · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de/ecp · Quelle: exchange_analyzer

```
external_services enthält 'ECP' - Admin-Panel sollte nicht im Internet stehen
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-2507f908: Weder Security Defaults noch Conditional Access aktiv

Hoch

CVSS-Lite: 7.5 (Hoch) · Kategorie: Fehlkonfiguration · CWE-1188 · Asset: mustermann.onmicrosoft.com · Fundstelle: mustermann.onmicrosoft.com · Quelle: entra_analyzer

```
security_defaults_enabled=false und keine aktive CA-Richtlinie
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-aeca0f0f: VM mit veraltetem Betriebssystem: vm-legacy-app

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Veraltete Komponente/Abhängigkeit (bekannte CVE) · CWE-1104 · Asset: 00000000-1111-2222-3333-444444444444/vm/vm-legacy-app · Fundstelle: 00000000-1111-2222-3333-444444444444/vm/vm-legacy-app · Quelle: azure_analyzer

```
os=Windows Server 2012 R2
```

Gegenmaßnahme: Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.

SPEC-6e3adf1e: Veraltetes/abgekündigtes VPN-Gateway: site-to-site-legacy

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Veraltete Komponente/Abhängigkeit (bekannte CVE) · CWE-1104 · Asset: fw-hq-fortigate/vpn/site-to-site-legacy · Fundstelle: fw-hq-fortigate/vpn/site-to-site-legacy · Quelle: firewall_analyzer

```
eol/outdated=true - kein Sicherheits-Support mehr
```

Gegenmaßnahme: Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.

SPEC-2344fb21: Verwundbare Abhängigkeit: django 2.2.0 (CVE-2022-28346)

Hoch

CVSS-Lite: 8.1 (Hoch) · Kategorie: Veraltete Komponente/Abhängigkeit (bekannte CVE) · CWE-1395 · Asset: portal-backend/pypi/django · Fundstelle: portal-backend/pypi/django · Quelle: dependency_analyzer

```
Version 2.2.0 erfüllt Advisory CVE-2022-28346 (verwundbar: >=2.0,<2.2.28; behoben in 2.2.28) - SQL Injection über QuerySet.annotate()
```

Gegenmaßnahme: Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.

SPEC-59ebfd95: SSH-Fernzugang der Firewall öffentlich erreichbar

Hoch

CVSS-Lite: 8.2 (Hoch) · Kategorie: Exponierter Fernzugang (RDP/VPN) · CWE-284 · Asset: fw-hq-fortigate/management · Fundstelle: fw-hq-fortigate/management · Quelle: firewall_analyzer

```
ssh in exposed_interfaces bei public=true
```

Gegenmaßnahme: Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.

SPEC-d99145a3: RDP aus dem Internet erreichbar: rdp-support

Hoch

CVSS-Lite: 8.2 (Hoch) · Kategorie: Exponierter Fernzugang (RDP/VPN) · CWE-284 · Asset: fw-hq-fortigate/rule/rdp-support · Fundstelle: fw-hq-fortigate/rule/rdp-support · Quelle: firewall_analyzer

```
source=0.0.0.0/0 -> Port 3389 (RDP) offen - Fernzugang gehört hinter VPN/MFA
```

Gegenmaßnahme: Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.

SPEC-36c120b8: SSH aus dem Internet erreichbar: ssh-admin

Hoch

CVSS-Lite: 8.2 (Hoch) · Kategorie: Exponierter Fernzugang (RDP/VPN) · CWE-284 · Asset: fw-hq-fortigate/rule/ssh-admin · Fundstelle: fw-hq-fortigate/rule/ssh-admin · Quelle: firewall_analyzer

```
source=0.0.0.0/0 -> Port 22 (SSH) offen - Fernzugang gehört hinter VPN/MFA
```

Gegenmaßnahme: Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.

SPEC-d7420465: VPN-Zugang ohne MFA: site-to-site-legacy

Hoch

CVSS-Lite: 8.2 (Hoch) · Kategorie: Exponierter Fernzugang (RDP/VPN) · CWE-308 · Asset: fw-hq-fortigate/vpn/site-to-site-legacy · Fundstelle: fw-hq-fortigate/vpn/site-to-site-legacy · Quelle: firewall_analyzer

```
mfa=false - Fernzugang ohne zweiten Faktor
```

Gegenmaßnahme: Fernzugang (RDP/VPN) nie direkt ins Internet. MFA erzwingen, hinter VPN/Zero-Trust-Gateway legen, auf benötigte Quell-IPs beschränken, Accounts nach Fehlversuchen sperren und Zugriffe protokollieren.

SPEC-2096328f: Kein HSTS (Strict-Transport-Security): https://portal.musterversicherung.de

Hoch

CVSS-Lite: 7.6 (Hoch) · Kategorie: Unsichere Transportverschlüsselung · CWE-319 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
HSTS-Header fehlt - Downgrade-/MITM-Risiko
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-cecc004e: Schwache TLS-Protokolle aktiv: tlsv1.0

Hoch

CVSS-Lite: 7.6 (Hoch) · Kategorie: Unsichere Transportverschlüsselung · CWE-327 · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de · Quelle: exchange_analyzer

```
tls.protocols enthält ['tlsv1.0']
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-cf11a791: TLS-Zertifikat abgelaufen: portal.musterversicherung.de:443

Hoch

CVSS-Lite: 7.6 (Hoch) · Kategorie: Unsichere Transportverschlüsselung · CWE-298 · Asset: portal.musterversicherung.de:443/certificate · Fundstelle: portal.musterversicherung.de:443/certificate · Quelle: tls_analyzer

```
days_until_expiry=-4 - abgelaufenes Zertifikat, Warnungen/MITM-Risiko
```

> **Gegenmaßnahme:** TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-860c1690: Veraltetes TLS-/SSL-Protokoll aktiv (SSLv3): portal.musterversicherung.de:443

Hoch

CVSS-Lite: 7.6 (Hoch) · Kategorie: Unsichere Transportverschlüsselung · CWE-327 · Asset: portal.musterversicherung.de:443/protocols · Fundstelle: portal.musterversicherung.de:443/protocols · Quelle: tls_analyzer

```
SSLv3 unterstützt - deaktivieren, nur TLS 1.2/1.3 zulassen
```

> **Gegenmaßnahme:** TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-639bec34: Alter Access-Key (430 Tage): deploy-bot [#1]

Mittel

CVSS-Lite: 5.7 (Mittel) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-798 · Asset: deploy-bot · Fundstelle: 123456789012/user/deploy-bot##1 · Quelle: aws_analyzer

```
access_key #1 age_days=430
```

> **Gegenmaßnahme:** Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-e998b432: Deaktiviertes Konto weiterhin in privilegierter Gruppe: ex-admin

Mittel

CVSS-Lite: 5.7 (Mittel) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-269 · Asset: ex-admin · Fundstelle: mustermann.local/ex-admin · Quelle: ad_analyzer

```
enabled=false, aber Mitglied einer privilegierten Gruppe
```

> **Gegenmaßnahme:** Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-8e312c49: Inaktives Gastkonto (seit 240 Tagen): gast@partnerfirma.de

Mittel

CVSS-Lite: 5.7 (Mittel) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-1108 · Asset: gast@partnerfirma.de · Fundstelle: mustermann.onmicrosoft.com/gast@partnerfirma.de · Quelle: entra_analyzer

```
guest=true, last_sign_in_days=240
```

> **Gegenmaßnahme:** Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-e2bb84db: Aktives, aber ungenutztes Konto (seit 410 Tagen): m.weber

Mittel

CVSS-Lite: 5.7 (Mittel) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · CWE-1108 · Asset: m.weber · Fundstelle: mustermann.local/m.weber · Quelle: ad_analyzer

```
enabled=true, last_logon_days=410
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-849cfb9b: Schwache IAM-Passwort-Policy (Mindestlänge 8)

Mittel

CVSS-Lite: 5.5 (Mittel) · Kategorie: Schwache Authentifizierung · CWE-521 · Asset: 123456789012 · Fundstelle: 123456789012 · Quelle: aws_analyzer

```
password_policy.minimum_length=8
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-479ebfef: Passwörter laufen nie ab

Mittel

CVSS-Lite: 5.5 (Mittel) · Kategorie: Schwache Authentifizierung · CWE-262 · Asset: mustermann.local · Fundstelle: mustermann.local · Quelle: ad_analyzer

```
password_policy.max_age_days = 0
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-f4dd1f32: Service-Konto mit SPN (Kerberoasting-Exposition): svc-mssql

Mittel

CVSS-Lite: 5.5 (Mittel) · Kategorie: Schwache Authentifizierung · CWE-522 · Asset: svc-mssql · Fundstelle: mustermann.local/svc-mssql · Quelle: ad_analyzer

```
service_principal_names=['MSSQL/db01.mustermann.local']
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-d8fe72a0: Konto ohne MFA: vertrieb@mustermann.de

Mittel

CVSS-Lite: 5.5 (Mittel) · Kategorie: Schwache Authentifizierung · CWE-308 · Asset: vertrieb@mustermann.de · Fundstelle: mustermann.onmicrosoft.com/vertrieb@mustermann.de · Quelle: entra_analyzer

```
mfa_registered=false
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-c6512174: Backup-Konsole ohne MFA: fileserver-daily

Mittel

CVSS-Lite: 5.6 (Mittel) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-308 · Asset: Muster Versicherung AG/backup/fileserver-daily · Fundstelle: Muster Versicherung AG/backup/fileserver-daily · Quelle: backup_analyzer

```
mfa_on_console=false - Angreifer können Backups aus der Konsole löschen
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-aa92b7e8: Backup nicht verschlüsselt: fileserver-daily

Mittel

CVSS-Lite: 5.6 (Mittel) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-311 · Asset: Muster Versicherung AG/backup/fileserver-daily · Fundstelle: Muster Versicherung AG/backup/fileserver-daily · Quelle: backup_analyzer

```
encrypted=false - Datenabfluss aus Backups (DSGVO-relevant)
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-ab435e13: Zu kurze Backup-Aufbewahrung (7 Tage): fileserver-daily

Mittel

CVSS-Lite: 5.6 (Mittel) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-693 · Asset: Muster Versicherung AG/backup/fileserver-daily · Fundstelle: Muster Versicherung AG/backup/fileserver-daily · Quelle: backup_analyzer

```
retention_days=7 - unter 30 Tagen kann eine spät entdeckte Kompromittierung alle Kopien betreffen
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-e8d96d07: Host-Networking aktiv: legacy-web

Mittel

CVSS-Lite: 5.6 (Mittel) · Kategorie: Container-/Docker-Sicherheit · CWE-668 · Asset: legacy-web · Fundstelle: legacy-web · Quelle: container_analyzer

```
network=host hebt die Netzwerk-Isolation auf - der Container sieht alle Host-Interfaces
```

Gegenmaßnahme: Container härten: nicht privilegiert und als unprivilegierter Benutzer laufen (USER != root), das Docker-Socket niemals in Container mounten, Host-Networking vermeiden, nur die minimal nötigen Capabilities vergeben (--cap-drop=ALL, gezielt einzelne --cap-add), Images mit festem Tag/Digest pinnen (kein :latest) und regelmäßig aktualisieren, Ports nur auf benötigte Quell-IPs/127.0.0.1 veröffentlichen und den Docker-Daemon nicht ungeschützt exponieren.

SPEC-9830f5b6: Container läuft als root: legacy-web

Mittel

CVSS-Lite: 5.6 (Mittel) · Kategorie: Container-/Docker-Sicherheit · CWE-250 · Asset: legacy-web · Fundstelle: legacy-web · Quelle: container_analyzer

```
user=root - nach Ausbruch direkt Host-root; besser als unprivilegierter Benutzer laufen
```

Gegenmaßnahme: Container härten: nicht privilegiert und als unprivilegierter Benutzer laufen (USER != root), das Docker-Socket niemals in Container mounten, Host-Networking vermeiden, nur die minimal nötigen Capabilities vergeben (--cap-drop=ALL, gezielt einzelne --cap-add), Images mit festem Tag/Digest pinnen (kein :latest) und regelmäßig aktualisieren, Ports nur auf benötigte Quell-IPs/127.0.0.1 veröffentlichen und den Docker-Daemon nicht ungeschützt exponieren.

SPEC-f7bbd47b: Azure-SQL ohne Transparent Data Encryption (TDE): sql-kunden

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Schwache Kryptographie · CWE-311 · Asset: 00000000-1111-2222-3333-444444444444/sql/sql-kunden · Fundstelle: 00000000-1111-2222-3333-444444444444/sql/sql-kunden · Quelle: azure_analyzer

```
tde_enabled=false
```

Gegenmaßnahme: Schwache Algorithmen (MD5/SHA1) durch SHA-256+ bzw. für Passwörter durch bcrypt/scrypt/Argon2 ersetzen. Keine Eigenbau-Kryptographie.

SPEC-03b8a4b0: Schwache Cipher-Suite angeboten (RC4-SHA): portal.musterversicherung.de:443

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Schwache Kryptographie · CWE-327 · Asset: portal.musterversicherung.de:443/ciphers · Fundstelle: portal.musterversicherung.de:443/ciphers · Quelle: tls_analyzer

```
RC4-SHA - schwache/veraltete Cipher, aus der Liste entfernen
```

Gegenmaßnahme: Schwache Algorithmen (MD5/SHA1) durch SHA-256+ bzw. für Passwörter durch bcrypt/scrypt/Argon2 ersetzen. Keine Eigenbau-Kryptographie.

SPEC-b47d7cb3: Schwache Cipher-Suite angeboten (DES-CBC3-SHA): portal.musterversicherung.de:443

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Schwache Kryptographie · CWE-327 · Asset: portal.musterversicherung.de:443/ciphers · Fundstelle: portal.musterversicherung.de:443/ciphers · Quelle: tls_analyzer

```
DES-CBC3-SHA - schwache/veraltete Cipher, aus der Liste entfernen
```

Gegenmaßnahme: Schwache Algorithmen (MD5/SHA1) durch SHA-256+ bzw. für Passwörter durch bcrypt/scrypt/Argon2 ersetzen. Keine Eigenbau-Kryptographie.

SPEC-5238d4fd: DNSSEC nicht aktiv: musterversicherung.de

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: DNS-Sicherheit (DNSSEC/CAA/Zonentransfer) · CWE-345 · Asset: musterversicherung.de/DNSSEC · Fundstelle: musterversicherung.de/DNSSEC · Quelle: dns_analyzer

```
Kein DNSSEC (ad-Flag) - DNS-Antworten sind nicht signiert, Cache-Poisoning/Spoofing möglich
```

Gegenmaßnahme: DNS absichern: DNSSEC aktivieren und die Zone signieren (Schutz vor Cache-Poisoning/Spoofing), CAA-Records setzen, damit nur autorisierte Zertifizierungsstellen ausstellen dürfen, Zonentransfer (AXFR) auf berechtigte Secondaries beschränken, Wildcard-Einträge vermeiden bzw. eng fassen und ungenutzte CNAME-Verweise (dangling) entfernen, um Subdomain-Takeover zu verhindern.

SPEC-ec420beb: DMARC nur im Monitoring-Modus (p=none): musterversicherung.de

Mittel

CVSS-Lite: 5.6 (Mittel) · Kategorie: E-Mail-Spoofing/Phishing (SPF/DKIM/DMARC) · CWE-290 · Asset: musterversicherung.de/DMARC · Fundstelle: musterversicherung.de/DMARC · Quelle: email_security_analyzer

```
DMARC=v=DMARC1; p=none - keine Durchsetzung; Ziel ist p=quarantine oder p=reject
```

Gegenmaßnahme: E-Mail-Spoofing verhindern: SPF mit -all (bzw. mindestens ~all) setzen, DKIM mit >= 2048-Bit-Schlüssel signieren und DMARC schrittweise auf p=quarantine, dann p=reject anheben. rua-Reportadresse konfigurieren und die Berichte regelmäßig auswerten (Schutz vor CEO-Fraud/BEC).

SPEC-5d7d0996: NSG offen ins Internet (0.0.0.0/0) auf Port 80: nsg-web

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/nsg/nsg-web · Fundstelle: 00000000-1111-2222-3333-444444444444/nsg/nsg-web · Quelle: azure_analyzer

```
open_to_internet_ports enthält 80
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-0db1a30f: NSG offen ins Internet (0.0.0.0/0) auf Port 443: nsg-web

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/nsg/nsg-web · Fundstelle: 00000000-1111-2222-3333-444444444444/nsg/nsg-web · Quelle: azure_analyzer

```
open_to_internet_ports enthält 443
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-294f9637: VM direkt aus dem Internet erreichbar (Public IP): vm-legacy-app

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 00000000-1111-2222-3333-444444444444/vm/vm-legacy-app · Fundstelle: 00000000-1111-2222-3333-444444444444/vm/vm-legacy-app · Quelle: azure_analyzer

```
public_ip=true
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-dd9e0feb: Security-Group offen ins Internet (0.0.0.0/0) auf Port 80

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 123456789012/sg/web-sg · Fundstelle: 123456789012/sg/web-sg · Quelle: aws_analyzer

```
open_to_world_ports enthält 80
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-f344b172: Security-Group offen ins Internet (0.0.0.0/0) auf Port 443

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Exponierter Dienst/Port · CWE-284 · Asset: 123456789012/sg/web-sg · Fundstelle: 123456789012/sg/web-sg · Quelle: aws_analyzer

```
open_to_world_ports enthält 443
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-e457f432: Container-Port auf allen Interfaces veröffentlicht: legacy-web (0.0.0.0:8080->80/tcp)

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Exponierter Dienst/Port · CWE-668 · Asset: legacy-web · Fundstelle: legacy-web · Quelle: container_analyzer

```
Port-Bindung 0.0.0.0:8080->80/tcp - auf benötigte Quell-IP/127.0.0.1 einschränken
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-ea453cdb: OWA extern erreichbar (Angriffsfläche/Password-Spraying)

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Exponierter Dienst/Port · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de/owa · Quelle: exchange_analyzer

```
external_services enthält 'OWA'
```

Gegenmaßnahme: Dienst hinter Firewall/VPN legen, auf benötigte Quell-IPs beschränken und nicht benötigte Ports schließen.

SPEC-0e4d623a: VPN nutzt veraltetes IKEv1: site-to-site-legacy

Mittel

CVSS-Lite: 5.1 (Mittel) · Kategorie: Fehlkonfiguration · CWE-327 · Asset: fw-hq-fortigate/vpn/site-to-site-legacy · Fundstelle: fw-hq-fortigate/vpn/site-to-site-legacy · Quelle: firewall_analyzer

```
ike_version=1 - auf IKEv2 umstellen
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-fc03679f: Selbstsigniertes TLS-Zertifikat: mail.musterversicherung.de:443

Mittel

CVSS-Lite: 5.1 (Mittel) · Kategorie: Fehlkonfiguration · CWE-295 · Asset: mail.musterversicherung.de:443/certificate · Fundstelle: mail.musterversicherung.de:443/certificate · Quelle: tls_analyzer

```
self_signed=true - kein vertrauenswürdiger Aussteller, Nutzer werden an Warnungen gewöhnt
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-cc8a4010: Nicht mehr gepflegte Abhängigkeit: lodash

Mittel

CVSS-Lite: 5.7 (Mittel) · Kategorie: Veraltete Komponente/Abhängigkeit (bekannte CVE) · CWE-1104 · Asset: portal-backend/npm/lodash · Fundstelle: portal-backend/npm/lodash · Quelle: dependency_analyzer

```
deprecated=true (Version 4.17.11) - kein Sicherheits-Support mehr
```

Gegenmaßnahme: Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.

SPEC-ef16fc68: Anonyme Freigabelinks aktiviert (SharePoint/OneDrive)

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Personenbezogene Daten (DSGVO-relevant) · CWE-284 · Asset: mustermann.onmicrosoft.com · Fundstelle: mustermann.onmicrosoft.com · Quelle: entra_analyzer

```
sharing.anonymous_links_enabled=true - DSGVO-Risiko
```

Gegenmaßnahme: Personenbezogene Daten nach DSGVO schützen: Datenminimierung, Verschlüsselung, Pseudonymisierung, Zugriff nach Least-Privilege, Löschkonzept und Verarbeitungsverzeichnis. Besondere Kategorien (Art. 9 DSGVO) gesondert schützen.

SPEC-af288b8a: Storage-Account erlaubt unverschlüsselten Zugriff (kein HTTPS-only): mustermannsa

Mittel

CVSS-Lite: 5.2 (Mittel) · Kategorie: Unsichere Transportverschlüsselung · CWE-319 · Asset: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Fundstelle: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Quelle: azure_analyzer

```
https_only=false
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-2324b554: Storage-Account mit schwacher TLS-Mindestversion: mustermannsa

Mittel

CVSS-Lite: 5.2 (Mittel) · Kategorie: Unsichere Transportverschlüsselung · CWE-327 · Asset: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Fundstelle: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Quelle: azure_analyzer

```
min_tls=TLS1.0
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-bfb3d30b: TLS-Zertifikat läuft in 12 Tagen ab: mail.musterversicherung.de:443

Mittel

CVSS-Lite: 5.2 (Mittel) · Kategorie: Unsichere Transportverschlüsselung · CWE-298 · Asset: mail.musterversicherung.de:443/certificate · Fundstelle: mail.musterversicherung.de:443/certificate · Quelle: tls_analyzer

```
days_until_expiry=12 - rechtzeitig erneuern
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-91ee5192: Unverschlüsselter Datenbank-Transport: mysql

Mittel

CVSS-Lite: 5.2 (Mittel) · Kategorie: Unsichere Transportverschlüsselung · CWE-319 · Asset: mysql:3306 · Fundstelle: mysql:3306 · Quelle: database_analyzer

```
Verbindungen ohne TLS - Zugangsdaten und Daten sind im Netz mitlesbar
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-e3fccd39: Veraltetes TLS-/SSL-Protokoll aktiv (TLSv1.0): portal.musterversicherung.de:443

Mittel

CVSS-Lite: 5.2 (Mittel) · Kategorie: Unsichere Transportverschlüsselung · CWE-327 · Asset: portal.musterversicherung.de:443/protocols · Fundstelle: portal.musterversicherung.de:443/protocols · Quelle: tls_analyzer

```
TLSv1.0 unterstützt - deaktivieren, nur TLS 1.2/1.3 zulassen
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-f12a9cc2: Unverschlüsselter Datenbank-Transport: redis

Mittel

CVSS-Lite: 5.2 (Mittel) · Kategorie: Unsichere Transportverschlüsselung · CWE-319 · Asset: redis:6379 · Fundstelle: redis:6379 · Quelle: database_analyzer

```
Verbindungen ohne TLS - Zugangsdaten und Daten sind im Netz mitlesbar
```

Gegenmaßnahme: TLS-Zertifikatsprüfung aktivieren (verify=True), aktuelle TLS-Version erzwingen und HSTS setzen.

SPEC-496ecfb5: Keine Content-Security-Policy: https://portal.musterversicherung.de

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-1021 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
CSP-Header fehlt - erschwert wirksamen XSS-Schutz
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-03237399: Clickjacking-Schutz fehlt (X-Frame-Options): https://portal.musterversicherung.de

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-1021 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
X-Frame-Options fehlt (alternativ CSP frame-ancestors)
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-0225f5fd: Cookie ohne Secure-Flag: SESSIONID

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-614 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
secure=false - Übertragung auch unverschlüsselt möglich
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-3f7a23d8: Cookie ohne HttpOnly-Flag: SESSIONID

Mittel

CVSS-Lite: 5.4 (Mittel) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-1004 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
httponly=false - per JavaScript auslesbar (XSS-Diebstahl)
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-94ce407b: adminCount=1 ohne aktuelle Privilegien (AdminSDHolder-Rest): a.fischer

Niedrig

CVSS-Lite: 3.3 (Niedrig) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · Asset: a.fischer · Fundstelle: mustermann.local/a.fischer · Quelle: ad_analyzer

```
admin_count=1, aber nicht in privilegierter Gruppe
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-0d45439a: Ungenutzter Access-Key: deploy-bot [#1]

Niedrig

CVSS-Lite: 3.3 (Niedrig) · Kategorie: Fehlerhafte Zugriffskontrolle (IDOR/Privesc) · Asset: deploy-bot · Fundstelle: 123456789012/user/deploy-bot##1 · Quelle: aws_analyzer

```
access_key #1 last_used_days=380
```

Gegenmaßnahme: Zugriffskontrolle serverseitig pro Objekt/Ressource prüfen (Deny-by-default). Direkte Objektreferenzen (IDs) nicht ohne Berechtigungsprüfung akzeptieren.

SPEC-dcecd21d: IAM-Passwort-Policy ohne Sonderzeichen-Pflicht

Niedrig

CVSS-Lite: 3.1 (Niedrig) · Kategorie: Schwache Authentifizierung · Asset: 123456789012 · Fundstelle: 123456789012 · Quelle: aws_analyzer

```
password_policy.require_symbols=false
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-20a0fce8: IAM-Passwörter laufen nie ab

Niedrig

CVSS-Lite: 3.1 (Niedrig) · Kategorie: Schwache Authentifizierung · Asset: 123456789012 · Fundstelle: 123456789012 · Quelle: aws_analyzer

```
password_policy.max_age_days=0
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-82f5aa78: Passwort-Historie zu kurz (3)

Niedrig

CVSS-Lite: 3.1 (Niedrig) · Kategorie: Schwache Authentifizierung · Asset: mustermann.local · Fundstelle: mustermann.local · Quelle: ad_analyzer

```
password_policy.history_length = 3
```

Gegenmaßnahme: Starke Passwort-/MFA-Richtlinien, sichere Session-Verwaltung und serverseitige Rechteprüfung durchsetzen. Standard-Zugangsdaten entfernen.

SPEC-e72a3770: Kein dokumentiertes Backup-/Wiederanlaufkonzept

Niedrig

CVSS-Lite: 3.2 (Niedrig) · Kategorie: Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test) · CWE-1053 · Asset: Muster Versicherung AG/policy · Fundstelle: Muster Versicherung AG/policy · Quelle: backup_analyzer

```
policy.documented=false - ohne dokumentiertes Konzept fehlt im Ernstfall die Handlungssicherheit
```

Gegenmaßnahme: 3-2-1-Regel umsetzen: mindestens 3 Kopien, 2 verschiedene Medien, 1 Kopie offsite - und mindestens eine offline bzw. unveränderbar (WORM/Immutable) gegen Ransomware. Restores regelmäßig testen (mind. jährlich, besser quartalsweise), die Backup-Konsole mit MFA schützen, Aufbewahrung an die Angreifer-Verweildauer anpassen (>= 30 Tage) und Backups verschlüsseln. Wiederanlauf-/Notfallkonzept dokumentieren und üben.

SPEC-7407c660: Ungepinntes Image (:latest): legacy-web

Niedrig

CVSS-Lite: 3.2 (Niedrig) · Kategorie: Container-/Docker-Sicherheit · CWE-1104 · Asset: legacy-web · Fundstelle: legacy-web · Quelle: container_analyzer

```
image=nginx:latest - kein fester Tag/Digest; Builds sind nicht reproduzierbar und können ungeprüft wechseln
```

Gegenmaßnahme: Container härten: nicht privilegiert und als unprivilegierter Benutzer laufen (USER != root), das Docker-Socket niemals in Container mounten, Host-Networking vermeiden, nur die minimal nötigen Capabilities vergeben (--cap-drop=ALL, gezielt einzelne --cap-add), Images mit festem Tag/Digest pinnen (kein :latest) und regelmäßig aktualisieren, Ports nur auf benötigte Quell-IPs/127.0.0.1 veröffentlichen und den Docker-Daemon nicht ungeschützt exponieren.

SPEC-31e16d0a: DKIM-Schlüssel nicht mehr zeitgemäß (1024 Bit, Selector google): musterversicherung.de

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: Schwache Kryptographie · CWE-326 · Asset: musterversicherung.de/DKIM · Fundstelle: musterversicherung.de/DKIM · Quelle: email_security_analyzer

```
key_bits=1024 - empfohlen sind 2048 Bit
```

Gegenmaßnahme: Schwache Algorithmen (MD5/SHA1) durch SHA-256+ bzw. für Passwörter durch bcrypt/scrypt/Argon2 ersetzen. Keine Eigenbau-Kryptographie.

SPEC-1e4094d8: Keine CAA-Records: musterversicherung.de

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: DNS-Sicherheit (DNSSEC/CAA/Zonentransfer) · CWE-295 · Asset: musterversicherung.de/CAA · Fundstelle: musterversicherung.de/CAA · Quelle: dns_analyzer

```
Ohne CAA darf jede Zertifizierungsstelle Zertifikate ausstellen (Mis-Issuance-Risiko)
```

Gegenmaßnahme: DNS absichern: DNSSEC aktivieren und die Zone signieren (Schutz vor Cache-Poisoning/Spoofing), CAA-Records setzen, damit nur autorisierte Zertifizierungsstellen ausstellen dürfen, Zonentransfer (AXFR) auf berechtigte Secondaries beschränken, Wildcard-Einträge vermeiden bzw. eng fassen und ungenutzte CNAME-Verweise (dangling) entfernen, um Subdomain-Takeover zu verhindern.

SPEC-68452bef: Wildcard-DNS-Eintrag (*): musterversicherung.de

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: DNS-Sicherheit (DNSSEC/CAA/Zonentransfer) · CWE-183 · Asset: musterversicherung.de/Wildcard · Fundstelle: musterversicherung.de/Wildcard · Quelle: dns_analyzer

```
Wildcard-A/AAAA fängt beliebige Subdomains ab - erschwert Missbrauchserkennung
```

Gegenmaßnahme: DNS absichern: DNSSEC aktivieren und die Zone signieren (Schutz vor Cache-Poisoning/Spoofing), CAA-Records setzen, damit nur autorisierte Zertifizierungsstellen ausstellen dürfen, Zonentransfer (AXFR) auf berechtigte Secondaries beschränken, Wildcard-Einträge vermeiden bzw. eng fassen und ungenutzte CNAME-Verweise (dangling) entfernen, um Subdomain-Takeover zu verhindern.

SPEC-3d54856e: DMARC ohne Auswertungs-Reports (kein rua): musterversicherung.de

Niedrig

CVSS-Lite: 3.2 (Niedrig) · Kategorie: E-Mail-Spoofing/Phishing (SPF/DKIM/DMARC) · Asset: musterversicherung.de/DMARC · Fundstelle: musterversicherung.de/DMARC · Quelle: email_security_analyzer

```
DMARC=v=DMARC1; p=none - ohne rua-Adresse keine Sichtbarkeit über Missbrauch
```

Gegenmaßnahme: E-Mail-Spoofing verhindern: SPF mit -all (bzw. mindestens ~all) setzen, DKIM mit >= 2048-Bit-Schlüssel signieren und DMARC schrittweise auf p=quarantine, dann p=reject anheben. rua-Reportadresse konfigurieren und die Berichte regelmäßig auswerten (Schutz vor CEO-Fraud/BEC).

SPEC-16ad482d: Key Vault ohne Purge-Protection: kv-prod

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · Asset: 00000000-1111-2222-3333-444444444444/keyvault/kv-prod · Fundstelle: 00000000-1111-2222-3333-444444444444/keyvault/kv-prod · Quelle: azure_analyzer

```
purge_protection=false
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-7d961492: Storage-Account ohne Verschlüsselung im Ruhezustand: mustermannsa

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · CWE-311 · Asset: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Fundstelle: 00000000-1111-2222-3333-444444444444/storage/mustermannsa · Quelle: azure_analyzer

```
encryption=false
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-48aaab3a: VM ohne Datenträgerverschlüsselung: vm-legacy-app

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · CWE-311 · Asset: 00000000-1111-2222-3333-444444444444/vm/vm-legacy-app · Fundstelle: 00000000-1111-2222-3333-444444444444/vm/vm-legacy-app · Quelle: azure_analyzer

```
disk_encryption=false
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-cceeda9d: Autodiscover extern erreichbar

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de/autodiscover · Quelle: exchange_analyzer

```
external_services enthält 'Autodiscover'
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-2533da96: Sicherheits-Header fehlt: HSTS

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · CWE-693 · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de · Quelle: exchange_analyzer

```
Header 'HSTS' nicht gesetzt
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-600ec68b: Sicherheits-Header fehlt: X-Content-Type-Options

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · CWE-693 · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de · Quelle: exchange_analyzer

```
Header 'X-Content-Type-Options' nicht gesetzt
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-8e319607: Server-Header gibt Produkt/Version preis

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · CWE-200 · Asset: mail.mustermann.de · Fundstelle: mail.mustermann.de · Quelle: exchange_analyzer

```
Server: Microsoft-IIS/10.0
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-16352092: S3-Bucket ohne Verschlüsselung: mustermann-kunden-backups

Niedrig

CVSS-Lite: 2.7 (Niedrig) · Kategorie: Fehlkonfiguration · CWE-311 · Asset: s3://mustermann-kunden-backups · Fundstelle: s3://mustermann-kunden-backups · Quelle: aws_analyzer

```
encryption=false
```

Gegenmaßnahme: Sichere Standardkonfiguration erzwingen: Debug-Modus in Produktion aus, unnötige Dienste deaktivieren, Sicherheits-Header setzen.

SPEC-ecb2bd35: Ungepinnte Abhängigkeit: requests

Niedrig

CVSS-Lite: 3.3 (Niedrig) · Kategorie: Veraltete Komponente/Abhängigkeit (bekannte CVE) · CWE-1104 · Asset: portal-backend/pypi/requests · Fundstelle: portal-backend/pypi/requests · Quelle: dependency_analyzer

```
version=* - keine feste Version, reproduzierbare Builds und CVE-Zuordnung erschwert
```

Gegenmaßnahme: Komponente auf eine unterstützte, gepatchte Version aktualisieren. Patch-Management und ein Software-Inventar (SBOM) etablieren; veraltete, nicht mehr benötigte Dienste abschalten.

SPEC-4486ea03: X-Content-Type-Options nicht 'nosniff': https://portal.musterversicherung.de

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-693 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
MIME-Sniffing möglich
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-d2bd8738: Keine Referrer-Policy: https://portal.musterversicherung.de

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-200 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
Referrer-Policy-Header fehlt
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-e5a6e865: Keine Permissions-Policy: https://portal.musterversicherung.de

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-693 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
Permissions-Policy-Header fehlt
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-30aac4cf: Server-Banner verrät Software: Apache/2.4.29 (Ubuntu)

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-200 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
Server: Apache/2.4.29 (Ubuntu)
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-6f364f4d: X-Powered-By verrät Software: PHP/7.2.24

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-200 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
X-Powered-By: PHP/7.2.24
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

SPEC-8dcda088: Cookie ohne SameSite-Schutz: SESSIONID

Niedrig

CVSS-Lite: 3.0 (Niedrig) · Kategorie: Web-Sicherheit (HTTP-Header/Cookies) · CWE-1275 · Asset: https://portal.musterversicherung.de · Fundstelle: https://portal.musterversicherung.de/headers · Quelle: http_headers_analyzer

```
samesite=None - CSRF-Risiko
```

Gegenmaßnahme: Sicherheits-Header setzen: HSTS (max-age >= 1 Jahr, includeSubDomains), Content-Security-Policy, X-Frame-Options bzw. CSP frame-ancestors, X-Content-Type-Options: nosniff, Referrer-Policy und Permissions-Policy. Cookies mit Secure, HttpOnly und SameSite ausliefern; Server-/X-Powered-By-Banner reduzieren, damit keine Softwareversionen preisgegeben werden.

BSI-IT-Grundschutz-Mapping

Finding	Risiko	Bereich	BSI-Bezug	Priorität
SPEC-9f347b98	Root-Konto besitzt Access-Keys (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	123456789012	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Sehr hoch
SPEC-f7da8fca	Admin-Rolle von beliebigem Prinzipal annehmbar: ci-deploy (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	ci-deploy	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Sehr hoch
SPEC-81ea1be3	Root-Konto ohne MFA (Schwache Authentifizierung)	123456789012	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Sehr hoch
SPEC-11ba2f6f	Privilegiertes Konto ohne MFA: admin@mustermann.de (Schwache Authentifizierung)	admin@mustermann.de	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Sehr hoch
SPEC-1ebb5973	Privilegierter Container: legacy-web (Container-/Docker-Sicherheit)	legacy-web	SYS.1.6 Container; SYS.1.6 Container	Sehr hoch
SPEC-566a535b	Docker-Socket im Container gemountet: legacy-web (Container-/Docker-Sicherheit)	legacy-web	SYS.1.6 Container; SYS.1.6 Container	Sehr hoch
SPEC-7875a860	Standard-/Default-Zugangsdaten: mysql (Standard-/Default-Zugangsdaten)	mysql:3306	ORP.4 Identitäts- und Berechtigungsmanagement; APP.4.3 Relationale Datenbanksysteme	Sehr hoch
SPEC-6ed63e86	Veraltete Exchange-Version (Build 15.1.2044.4) (Veraltete Komponente/Abhängigkeit (bekannte CVE))	mail.mustermann.de	OPS.1.1.3 Patch- und Änderungsmanagement; APP.5.2 Microsoft Exchange und Outlook	Sehr hoch
SPEC-2fc81ec0	Verwundbare Abhängigkeit: log4j-core 2.14.1 (CVE-2021-44228) (Veraltete Komponente/Abhängigkeit (bekannte CVE))	portal-backend/maven/log4j-core	OPS.1.1.3 Patch- und Änderungsmanagement; OPS.1.1.3 Patch- und Änderungsmanagement	Sehr hoch
SPEC-0f4408c1	Zu viele Subscription-Owner (4) (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	00000000-1111-2222-3333-444444444444	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-39fe66f1	Überprivilegierter IAM-User (Admin): deploy-bot (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	deploy-bot	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-60bc5404	Zu viele privilegierte Konten in 'Domain Admins' (9) (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	mustermann.local	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Hoch
SPEC-00cc0dfd	Zu viele Konten in 'Global Administrator' (7) (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	mustermann.onmicrosoft.com	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-14595b9d	Überprivilegierte App-Registrierung: Alt-Sync-Tool (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	mustermann.onmicrosoft.com	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-abea65ca	IAM-Konsolenzugriff ohne MFA: deploy-bot (Schwache Authentifizierung)	deploy-bot	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-8e58f5be	Kerberos-Pre-Auth deaktiviert (AS-REP-Roasting): m.weber (Schwache	m.weber	ORP.4 Identitäts- und Berechtigungsmanagement;	Hoch

	Authentifizierung)		APP.2.2 Active Directory Domain Services	
SPEC-073d540b	Passwort-Mindestlänge zu gering (8 < 12) (Schwache Authentifizierung)	mustermann.local	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Hoch
SPEC-595866cd	Passwort-Komplexität nicht erzwungen (Schwache Authentifizierung)	mustermann.local	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Hoch
SPEC-beab5cf1	Keine Account-Lockout-Policy (Brute-Force ungebremst) (Schwache Authentifizierung)	mustermann.local	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Hoch
SPEC-00ea6f87	krbtgt-Passwort veraltet (1450 Tage) - Golden-Ticket-Risiko (Schwache Authentifizierung)	mustermann.local	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Hoch
SPEC-6da533f5	Keine MFA-Erzwingung (Security Defaults/CA) (Schwache Authentifizierung)	mustermann.onmicrosoft.com	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-59ddef66	Legacy-Authentifizierung nicht blockiert (Password-Spraying) (Schwache Authentifizierung)	mustermann.onmicrosoft.com	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-21b52553	Datenbank ohne Authentifizierung: redis (Schwache Authentifizierung)	redis:6379	ORP.4 Identitäts- und Berechtigungsmanagement; APP.4.3 Relationale Datenbanksysteme	Hoch
SPEC-6bdbf551	Privilegiertes Konto mit nie ablaufendem Passwort: svc-mssql (Schwache Authentifizierung)	svc-mssql	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Hoch
SPEC-d272723a	Restore-Test überfällig (400 Tage): erp-datenbank (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/erp-datenbank	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Hoch
SPEC-bcaae6c6	Höchstens eine Backup-Kopie (Single Point of Failure): fileserver-daily (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/fileserver-daily	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Hoch
SPEC-5c31f48c	Kein offline-/unveränderbares (Immutable) Backup: fileserver-daily (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/fileserver-daily	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Hoch
SPEC-6fee4a14	Keine Offsite-Kopie des Backups: fileserver-daily (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/fileserver-daily	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Hoch
SPEC-d3238e8e	Wiederherstellung nie getestet: fileserver-daily (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/fileserver-daily	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Hoch
SPEC-2e2444fa	Öffentlicher Blob-Zugriff auf Storage-Account: mustermannsa	00000000-1111-2222-3333-444444444444/storage/mustermannsa	OPS.2.2 Cloud-Nutzung; OPS.2.2 Cloud-Nutzung	Hoch

	(Offener/fehlkonfigurierter Cloud-Speicher)			
SPEC-7beab70b	Öffentlicher S3-Bucket: mustermann-kunden-backups (Offener/fehlkonfigurierter Cloud-Speicher)	s3://mustermann-kunden-backups	OPS.2.2 Cloud-Nutzung; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-f77359e5	Gefährliche Capabilities: legacy-web (NET_ADMIN, SYS_ADMIN) (Container-/Docker-Sicherheit)	legacy-web	SYS.1.6 Container; SYS.1.6 Container	Hoch
SPEC-d9e7a031	VPN mit schwacher Kryptographie: site-to-site-legacy (Schwache Kryptographie)	fw-hq-fortigate/vpn/site-to-site-legacy	CON.1 Kryptokonzept; NET.3.2 Firewall	Hoch
SPEC-cfe88ad8	TLS-Zertifikat mit schwacher Signatur: portal.musterversicherung.de:443 (Schwache Kryptographie)	portal.musterversicherung.de:443/certificate	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Hoch
SPEC-eb3a7778	TLS-Zertifikat mit zu kurzem Schlüssel (1024 Bit): portal.musterversicherung.de:443 (Schwache Kryptographie)	portal.musterversicherung.de:443/certificate	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Hoch
SPEC-3be756ee	Offener Zonentransfer (AXFR): musterversicherung.de (DNS-Sicherheit (DNSSEC/CAA/Zonentransfer))	musterversicherung.de/AXFR	APP.3.6 DNS-Server; APP.3.6 DNS-Server	Hoch
SPEC-66f4c521	Dangling CNAME (Subdomain-Takeover-Risiko): alt-portal.musterversicherung.de -> muster-portal.azurewebsites.net (DNS-Sicherheit (DNSSEC/CAA/Zonentransfer))	musterversicherung.de/CNAME	APP.3.6 DNS-Server; APP.3.6 DNS-Server	Hoch
SPEC-eff3e013	SPF erlaubt beliebige Absender (+all/?all): musterversicherung.de (E-Mail-Spoofing/Phishing (SPF/DKIM/DMARC))	musterversicherung.de/SPF	APP.5.3 Allgemeiner E-Mail-Client und -Server; APP.5.3 Allgemeiner E-Mail-Client und -Server	Hoch
SPEC-740f2a96	NSG offen ins Internet (0.0.0.0/0) auf Port 3389: nsg-db (Exponierter Dienst/Port)	00000000-1111-2222-3333-444444444444/nsg/nsg-db	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-5ac988ef	NSG offen ins Internet (0.0.0.0/0) auf Port 1433: nsg-db (Exponierter Dienst/Port)	00000000-1111-2222-3333-444444444444/nsg/nsg-db	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-808a27fa	Azure-SQL-Server öffentlich erreichbar: sql-kunden (Exponierter Dienst/Port)	00000000-1111-2222-3333-444444444444/sql/sql-kunden	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-da15ca55	Security-Group offen ins Internet (0.0.0.0/0) auf Port 3306 (Exponierter Dienst/Port)	123456789012/sg/db-sg	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-509d3748	Security-Group offen ins Internet (0.0.0.0/0) auf Port 22 (Exponierter Dienst/Port)	123456789012/sg/db-sg	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-ca4cb183	Management-Interface aus dem Internet erreichbar (Exponierter Dienst/Port)	fw-hq-fortigate/management	NET.1.1 Netzarchitektur und -design; NET.3.2 Firewall	Hoch
SPEC-b0fed1ef	Sensibler Dienst offen ins Internet (MSSQL): db-exposed (Exponierter Dienst/Port)	fw-hq-fortigate/rule/db-exposed	NET.1.1 Netzarchitektur und -design; NET.3.2 Firewall	Hoch

SPEC-35ebde7f	Datenbank öffentlich erreichbar: mysql (Exponierter Dienst/Port)	mysql:3306	NET.1.1 Netzarchitektur und -design; APP.4.3 Relationale Datenbanksysteme	Hoch
SPEC-3c0a33fd	Datenbank öffentlich erreichbar: redis (Exponierter Dienst/Port)	redis:6379	NET.1.1 Netzarchitektur und -design; APP.4.3 Relationale Datenbanksysteme	Hoch
SPEC-da8669ef	Key Vault öffentlich erreichbar: kv-prod (Fehlkonfiguration)	00000000-1111-2222-3333-444444444444/keyvault/kv-prod	SYS.1.1 Allgemeiner Server; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-ef62db9d	Any-Any-Freigabe in der Firewall: permit-any-out (Fehlkonfiguration)	fw-hq-fortigate/rule/permit-any-out	SYS.1.1 Allgemeiner Server; NET.3.2 Firewall	Hoch
SPEC-ae52a1f1	Exchange-ECP (Admin-Oberfläche) extern erreichbar (Fehlkonfiguration)	mail.mustermann.de	SYS.1.1 Allgemeiner Server; APP.5.2 Microsoft Exchange und Outlook	Hoch
SPEC-2507f908	Weder Security Defaults noch Conditional Access aktiv (Fehlkonfiguration)	mustermann.onmicrosoft.com	SYS.1.1 Allgemeiner Server; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-aeca0f0f	VM mit veraltetem Betriebssystem: vm-legacy-app (Veraltete Komponente/Abhängigkeit (bekannte CVE))	00000000-1111-2222-3333-444444444444/vm/vm-legacy-app	OPS.1.1.3 Patch- und Änderungsmanagement; OPS.2.2 Cloud-Nutzung	Hoch
SPEC-6e3adf1e	Veraltetes/abgekündigtes VPN-Gateway: site-to-site-legacy (Veraltete Komponente/Abhängigkeit (bekannte CVE))	fw-hq-fortigate/vpn/site-to-site-legacy	OPS.1.1.3 Patch- und Änderungsmanagement; NET.3.2 Firewall	Hoch
SPEC-2344fb21	Verwundbare Abhängigkeit: django 2.2.0 (CVE-2022-28346) (Veraltete Komponente/Abhängigkeit (bekannte CVE))	portal-backend/pypi/django	OPS.1.1.3 Patch- und Änderungsmanagement; OPS.1.1.3 Patch- und Änderungsmanagement	Hoch
SPEC-59ebfd95	SSH-Fernzugang der Firewall öffentlich erreichbar (Exponierter Fernzugang (RDP/VPN))	fw-hq-fortigate/management	OPS.1.2.5 Fernwartung; NET.3.2 Firewall	Hoch
SPEC-d99145a3	RDP aus dem Internet erreichbar: rdp-support (Exponierter Fernzugang (RDP/VPN))	fw-hq-fortigate/rule/rdp-support	OPS.1.2.5 Fernwartung; NET.3.2 Firewall	Hoch
SPEC-36c120b8	SSH aus dem Internet erreichbar: ssh-admin (Exponierter Fernzugang (RDP/VPN))	fw-hq-fortigate/rule/ssh-admin	OPS.1.2.5 Fernwartung; NET.3.2 Firewall	Hoch
SPEC-d7420465	VPN-Zugang ohne MFA: site-to-site-legacy (Exponierter Fernzugang (RDP/VPN))	fw-hq-fortigate/vpn/site-to-site-legacy	OPS.1.2.5 Fernwartung; NET.3.2 Firewall	Hoch
SPEC-2096328f	Kein HSTS (Strict-Transport-Security): https://portal.musterversicherung.de (Unsichere Transportverschlüsselung)	https://portal.musterversicherung.de	CON.1 Kryptokonzept; APP.3.1 Webanwendungen und Webservices	Hoch
SPEC-cecc004e	Schwache TLS-Protokolle aktiv: tlsv1.0 (Unsichere Transportverschlüsselung)	mail.mustermann.de	CON.1 Kryptokonzept; APP.5.2 Microsoft Exchange und Outlook	Hoch
SPEC-cf11a791	TLS-Zertifikat abgelaufen: portal.musterversicherung.de:443 (Unsichere Transportverschlüsselung)	portal.musterversicherung.de:443/certificate	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Hoch
SPEC-860c1690	Veraltetes TLS-/SSL-Protokoll aktiv (SSLv3): portal.musterversicherung.de:443	portal.musterversicherung.de:443/protocols	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Hoch

	(Unsichere Transportverschlüsselung)			
SPEC-639bec34	Alter Access-Key (430 Tage): deploy-bot [#1] (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	deploy-bot	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-e998b432	Deaktiviertes Konto weiterhin in privilegierter Gruppe: ex-admin (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	ex-admin	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Mittel
SPEC-8e312c49	Inaktives Gastkonto (seit 240 Tagen): gast@partnerfirma.de (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	gast@partnerfirma.de	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-e2bb84db	Aktives, aber ungenutztes Konto (seit 410 Tagen): m.weber (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	m.weber	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Mittel
SPEC-849cfb9b	Schwache IAM-Passwort-Policy (Mindestlänge 8) (Schwache Authentifizierung)	123456789012	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-479ebfef	Passwörter laufen nie ab (Schwache Authentifizierung)	mustermann.local	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Mittel
SPEC-f4dd1f32	Service-Konto mit SPN (Kerberoasting-Exposition): svc-mssql (Schwache Authentifizierung)	svc-mssql	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Mittel
SPEC-d8fe72a0	Konto ohne MFA: vertrieb@mustermann.de (Schwache Authentifizierung)	vertrieb@mustermann.de	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-c6512174	Backup-Konsole ohne MFA: fileserver-daily (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/fileserver-daily	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Mittel
SPEC-aa92b7e8	Backup nicht verschlüsselt: fileserver-daily (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/fileserver-daily	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Mittel
SPEC-ab435e13	Zu kurze Backup-Aufbewahrung (7 Tage): fileserver-daily (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/backup/fileserver-daily	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Mittel
SPEC-e8d96d07	Host-Networking aktiv: legacy-web (Container-/Docker-Sicherheit)	legacy-web	SYS.1.6 Container; SYS.1.6 Container	Mittel
SPEC-9830f5b6	Container läuft als root: legacy-web (Container-/Docker-Sicherheit)	legacy-web	SYS.1.6 Container; SYS.1.6 Container	Mittel
SPEC-f7bbd47b	Azure-SQL ohne Transparent Data Encryption (TDE): sql-kunden (Schwache Kryptographie)	00000000-1111-2222-3333-444444444444/sql/sql-kunden	CON.1 Kryptokonzept; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-03b8a4b0	Schwache Cipher-Suite angeboten (RC4-SHA): portal.musterversicherung.de:443 (Schwache Kryptographie)	portal.musterversicherung.de:443/ciphers	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Mittel

SPEC-b47d7cb3	Schwache Cipher-Suite angeboten (DES-CBC3-SHA): portal.musterversicherung.de:443 (Schwache Kryptographie)	portal.musterversicherung.de:443/ciphers	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Mittel
SPEC-5238d4fd	DNSSEC nicht aktiv: musterversicherung.de (DNS-Sicherheit (DNSSEC/CAA/Zonentransfer))	musterversicherung.de/DNSSEC	APP.3.6 DNS-Server; APP.3.6 DNS-Server	Mittel
SPEC-ec420beb	DMARC nur im Monitoring-Modus (p=none): musterversicherung.de (E-Mail-Spoofing/Phishing (SPF/DKIM/DMARC))	musterversicherung.de/DMARC	APP.5.3 Allgemeiner E-Mail-Client und -Server; APP.5.3 Allgemeiner E-Mail-Client und -Server	Mittel
SPEC-5d7d0996	NSG offen ins Internet (0.0.0.0/0) auf Port 80: nsg-web (Exponierter Dienst/Port)	00000000-1111-2222-3333-444444444444/nsg/nsg-web	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-0db1a30f	NSG offen ins Internet (0.0.0.0/0) auf Port 443: nsg-web (Exponierter Dienst/Port)	00000000-1111-2222-3333-444444444444/nsg/nsg-web	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-294f9637	VM direkt aus dem Internet erreichbar (Public IP): vm-legacy-app (Exponierter Dienst/Port)	00000000-1111-2222-3333-444444444444/vm/vm-legacy-app	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-dd9e0feb	Security-Group offen ins Internet (0.0.0.0/0) auf Port 80 (Exponierter Dienst/Port)	123456789012/sg/web-sg	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-f344b172	Security-Group offen ins Internet (0.0.0.0/0) auf Port 443 (Exponierter Dienst/Port)	123456789012/sg/web-sg	NET.1.1 Netzarchitektur und -design; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-e457f432	Container-Port auf allen Interfaces veröffentlicht: legacy-web (0.0.0.0:8080->80/tcp) (Exponierter Dienst/Port)	legacy-web	NET.1.1 Netzarchitektur und -design; SYS.1.6 Container	Mittel
SPEC-ea453cdb	OWA extern erreichbar (Angriffsfläche/Password-Spraying) (Exponierter Dienst/Port)	mail.mustermann.de	NET.1.1 Netzarchitektur und -design; APP.5.2 Microsoft Exchange und Outlook	Mittel
SPEC-0e4d623a	VPN nutzt veraltetes IKEv1: site-to-site-legacy (Fehlkonfiguration)	fw-hq-fortigate/vpn/site-to-site-legacy	SYS.1.1 Allgemeiner Server; NET.3.2 Firewall	Mittel
SPEC-fc03679f	Selbstsigniertes TLS-Zertifikat: mail.musterversicherung.de:443 (Fehlkonfiguration)	mail.musterversicherung.de:443/certificate	SYS.1.1 Allgemeiner Server; CON.1 Kryptokonzept	Mittel
SPEC-cc8a4010	Nicht mehr gepflegte Abhängigkeit: lodash (Veraltete Komponente/Abhängigkeit (bekannte CVE))	portal-backend/npm/lodash	OPS.1.1.3 Patch- und Änderungsmanagement; OPS.1.1.3 Patch- und Änderungsmanagement	Mittel
SPEC-ef16fc68	Anonyme Freigabelinks aktiviert (SharePoint/OneDrive) (Personenbezogene Daten (DSGVO-relevant))	mustermann.onmicrosoft.com	CON.2 Datenschutz; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-af288b8a	Storage-Account erlaubt unverschlüsselten Zugriff (kein HTTPS-only): mustermannsa (Unsichere Transportverschlüsselung)	00000000-1111-2222-3333-444444444444/storage/mustermannsa	CON.1 Kryptokonzept; OPS.2.2 Cloud-Nutzung	Mittel
SPEC-2324b554	Storage-Account mit schwacher TLS-Mindestversion: mustermannsa	00000000-1111-2222-3333-444444444444/storage/mustermannsa	CON.1 Kryptokonzept; OPS.2.2 Cloud-Nutzung	Mittel

	(Unsichere Transportverschlüsselung)			
SPEC-bfb3d30b	TLS-Zertifikat läuft in 12 Tagen ab: mail.musterversicherung.de:443 (Unsichere Transportverschlüsselung)	mail.musterversicherung.de:443/certificate	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Mittel
SPEC-91ee5192	Unverschlüsselter Datenbank-Transport: mysql (Unsichere Transportverschlüsselung)	mysql:3306	CON.1 Kryptokonzept; APP.4.3 Relationale Datenbanksysteme	Mittel
SPEC-e3fccd39	Veraltetes TLS-/SSL-Protokoll aktiv (TLSv1.0): portal.musterversicherung.de:443 (Unsichere Transportverschlüsselung)	portal.musterversicherung.de:443/protocols	CON.1 Kryptokonzept; CON.1 Kryptokonzept	Mittel
SPEC-f12a9cc2	Unverschlüsselter Datenbank-Transport: redis (Unsichere Transportverschlüsselung)	redis:6379	CON.1 Kryptokonzept; APP.4.3 Relationale Datenbanksysteme	Mittel
SPEC-496ecfb5	Keine Content-Security-Policy: https://portal.musterversicherung.de (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Mittel
SPEC-03237399	Clickjacking-Schutz fehlt (X-Frame-Options): https://portal.musterversicherung.de (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Mittel
SPEC-0225f5fd	Cookie ohne Secure-Flag: SESSIONID (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Mittel
SPEC-3f7a23d8	Cookie ohne HttpOnly-Flag: SESSIONID (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Mittel
SPEC-94ce407b	adminCount=1 ohne aktuelle Privilegien (AdminSDHolder-Rest): a.fischer (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	a.fischer	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Niedrig
SPEC-0d45439a	Ungenutzter Access-Key: deploy-bot [#1] (Fehlerhafte Zugriffskontrolle (IDOR/Privesc))	deploy-bot	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Niedrig
SPEC-dcecd21d	IAM-Passwort-Policy ohne Sonderzeichen-Pflicht (Schwache Authentifizierung)	123456789012	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Niedrig
SPEC-20a0fce8	IAM-Passwörter laufen nie ab (Schwache Authentifizierung)	123456789012	ORP.4 Identitäts- und Berechtigungsmanagement; OPS.2.2 Cloud-Nutzung	Niedrig
SPEC-82f5aa78	Passwort-Historie zu kurz (3) (Schwache Authentifizierung)	mustermann.local	ORP.4 Identitäts- und Berechtigungsmanagement; APP.2.2 Active Directory Domain Services	Niedrig
SPEC-e72a3770	Kein dokumentiertes Backup-/Wiederanlaufkonzept (Backup-/Ransomware-Resilienz (3-2-1, Immutable, Restore-Test))	Muster Versicherung AG/policy	CON.3 Datensicherungskonzept; CON.3 Datensicherungskonzept	Niedrig

SPEC-7407c660	Ungepinntes Image (:latest): legacy-web (Container-/Docker-Sicherheit)	legacy-web	SYS.1.6 Container; SYS.1.6 Container	Niedrig
SPEC-31e16d0a	DKIM-Schlüssel nicht mehr zeitgemäß (1024 Bit, Selector google): musterversicherung.de (Schwache Kryptographie)	musterversicherung.de/DKIM	CON.1 Kryptokonzept; APP.5.3 Allgemeiner E-Mail-Client und -Server	Niedrig
SPEC-1e4094d8	Keine CAA-Records: musterversicherung.de (DNS-Sicherheit (DNSSEC/CAA/Zonentransfer))	musterversicherung.de/CAA	APP.3.6 DNS-Server; APP.3.6 DNS-Server	Niedrig
SPEC-68452bef	Wildcard-DNS-Eintrag (*): musterversicherung.de (DNS-Sicherheit (DNSSEC/CAA/Zonentransfer))	musterversicherung.de/Wildcard	APP.3.6 DNS-Server; APP.3.6 DNS-Server	Niedrig
SPEC-3d54856e	DMARC ohne Auswertungs-Reports (kein rua): musterversicherung.de (E-Mail-Spoofing/Phishing (SPF/DKIM/DMARC))	musterversicherung.de/DMARC	APP.5.3 Allgemeiner E-Mail-Client und -Server; APP.5.3 Allgemeiner E-Mail-Client und -Server	Niedrig
SPEC-16ad482d	Key Vault ohne Purge-Protection: kv-prod (Fehlkonfiguration)	00000000-1111-2222-3333-444444444444/keyvault/kv-prod	SYS.1.1 Allgemeiner Server; OPS.2.2 Cloud-Nutzung	Niedrig
SPEC-7d961492	Storage-Account ohne Verschlüsselung im Ruhezustand: mustermannsa (Fehlkonfiguration)	00000000-1111-2222-3333-444444444444/storage/mustermannsa	SYS.1.1 Allgemeiner Server; OPS.2.2 Cloud-Nutzung	Niedrig
SPEC-48aaab3a	VM ohne Datenträgerverschlüsselung: vm-legacy-app (Fehlkonfiguration)	00000000-1111-2222-3333-444444444444/vm/vm-legacy-app	SYS.1.1 Allgemeiner Server; OPS.2.2 Cloud-Nutzung	Niedrig
SPEC-cceeda9d	Autodiscover extern erreichbar (Fehlkonfiguration)	mail.mustermann.de	SYS.1.1 Allgemeiner Server; APP.5.2 Microsoft Exchange und Outlook	Niedrig
SPEC-2533da96	Sicherheits-Header fehlt: HSTS (Fehlkonfiguration)	mail.mustermann.de	SYS.1.1 Allgemeiner Server; APP.5.2 Microsoft Exchange und Outlook	Niedrig
SPEC-600ec68b	Sicherheits-Header fehlt: X-Content-Type-Options (Fehlkonfiguration)	mail.mustermann.de	SYS.1.1 Allgemeiner Server; APP.5.2 Microsoft Exchange und Outlook	Niedrig
SPEC-8e319607	Server-Header gibt Produkt/Version preis (Fehlkonfiguration)	mail.mustermann.de	SYS.1.1 Allgemeiner Server; APP.5.2 Microsoft Exchange und Outlook	Niedrig
SPEC-16352092	S3-Bucket ohne Verschlüsselung: mustermann-kunden-backups (Fehlkonfiguration)	s3://mustermann-kunden-backups	SYS.1.1 Allgemeiner Server; OPS.2.2 Cloud-Nutzung	Niedrig
SPEC-ecb2bd35	Ungepinnte Abhängigkeit: requests (Veraltete Komponente/Abhängigkeit (bekannte CVE))	portal-backend/pypi/requests	OPS.1.1.3 Patch- und Änderungsmanagement; OPS.1.1.3 Patch- und Änderungsmanagement	Niedrig
SPEC-4486ea03	X-Content-Type-Options nicht 'nosniff': https://portal.musterversicherung.de (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Niedrig
SPEC-d2bd8738	Keine Referrer-Policy: https://portal.musterversicherung.de (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Niedrig

SPEC-e5a6e865	Keine Permissions-Policy: https://portal.musterversicherung.de (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Niedrig
SPEC-30aac4cf	Server-Banner verrät Software: Apache/2.4.29 (Ubuntu) (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Niedrig
SPEC-6f364f4d	X-Powered-By verrät Software: PHP/7.2.24 (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Niedrig
SPEC-8dcda088	Cookie ohne SameSite-Schutz: SESSIONID (Web-Sicherheit (HTTP-Header/Cookies))	https://portal.musterversicherung.de	APP.3.1 Webanwendungen und Webservices; APP.3.1 Webanwendungen und Webservices	Niedrig

Scanner-Ergebnisse

Keine aktiven Scanner ausgeführt.

Scope-Hinweise & Limitierungen

- Freigegebene Netzwerk-Ziele: 203.0.113.0/24, muster-gmbh.de
- Aktive Scanner freigegeben: (keine)
- Aktionen außerhalb des Rahmens wurden technisch verweigert (fail-closed).
- Momentaufnahme zum Prüfzeitpunkt; statische Treffer sind zu verifizieren.
- AD-/Exchange-/Entra-Bewertungen aus bereitgestellten Exportdaten; keine Ausnutzung.

Nächste Schritte

1. Kritische/hohe Findings und Quick Wins kurzfristig beheben.
2. Angriffspfade priorisiert schließen.
3. Strategische Maßnahmen einplanen.
4. Nach Behebung gezielten Nachtest (Re-Test) durchführen.