VERTRAULICH

TG TechGuard IT Solutions

Sicherheits-Risikobewertung

Analyse kompromittierter Zugangsdaten

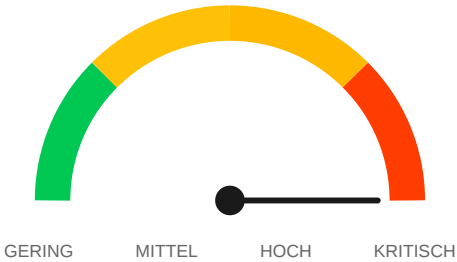
beispiel-gmbh.de

Erstellt exklusiv für

TechGuard IT Solutions

12. Dezember 2025

Zusammenfassung



100

KRITISCH

👤

4

KOMPROMITTIERTE IDENTITÄTEN

🔓

17

GESTOHLENE PASSWÖRTER

🦠

4

MALWARE-INFEKTIONEN

Das Unternehmen beispiel-gmbh.de weist einen kritischen Risikostatus von 100/100 auf. Aktive Stealer-Malware-Infektionen (Lumma, RedLine) ermöglichen Angreifern direkten Zugriff auf Bankkonten, geschäftliche Sessions und sensible Daten. Sofortige, drastische Gegenmaßnahmen sind zwingend erforderlich.

Außerdem bilden 17 gestohlene Passwörter und kompromittierte private Konten auf Firmengeräten ein direktes Einfallstor für Ransomware. Fehlende E-Mail-Sicherheit (SPF, DMARC) potenziert das Risiko weiterer Phishing-Angriffe und Datenlecks.

Kritische Malware-Funde (Stealer Logs)

Diese Daten stammen von infizierten Geräten. Die betroffenen Computer wurden mit Schadsoftware (Infostealer) kompromittiert, die Passwörter, Browser-Cookies und Sitzungsdaten gestohlen hat. Das Risiko einer Ransomware-Attacke oder Kontenübernahme ist akut.

E-Mail	Passwort	Quelle	Datum	Logins
ge***@beispiel-gmbh.de	••••***	Lumma Stealer	15. Okt. 2025 VOR 58 TAGEN	beispiel-gmbh.de linkedin.com ... 4x
in***@beispiel-gmbh.de	••••***	Generic Stealer	1. Okt. 2025 VOR 72 TAGEN	beispiel-gmbh.de mailchimp.com ... 4x
bu***@beispiel-gmbh.de	••••***	RedLine Stealer	20. Sept. 2025 VOR 83 TAGEN	beispiel-gmbh.de datev.de ... 5x
az***@beispiel-gmbh.de	••••***	Generic Stealer	15. Sept. 2025 VOR 88 TAGEN	beispiel-gmbh.de grabcad.com ... 4x

* **Lumma Stealer**: Stiehlt Online-Banking-Zugänge und Browser-Sessions. Angreifer können sich als Ihr Mitarbeiter ausgeben.
* **Generic Stealer**: Passwörter wurden von infiziertem Gerät gestohlen. Das Gerät muss identifiziert und bereinigt werden.
* **RedLine Stealer**: Meistverbreitete Malware 2024. Stiehlt VPN-Zugänge – Angreifer können ins Firmennetzwerk eindringen.

E-Mail-Sicherheit

External Attack Surface

❌ CEO-Fraud Risiko

HOCH

Aktuell kann jeder Kriminelle eine E-Mail schreiben, die technisch so aussieht, als käme sie direkt von @beispiel-gmbh.de. Ihre Rechnungsabteilung könnte getäuscht werden.

❌ SPF (Sender Policy Framework)

Kritisch

Kein SPF-Eintrag. Domain ist anfällig für E-Mail-Spoofing.

❌ DMARC (Domain-based Message Authentication)

Kritisch

Kein DMARC-Eintrag. Kein Schutz gegen Phishing-Angriffe.

Bedrohungs-Index

Keine E-Mail-Authentifizierung

Handlungsempfehlungen

Sofortmaßnahmen

⚠️ WICHTIGE FRAGE

"Hat Ihr aktueller IT-Dienstleister Sie über diese Sicherheitslücken informiert?"

Falls nicht: Warum nicht?

Identifizierte Lücke	Empfohlene Maßnahme
⚠ Malware-Infektionen	✅ EDR-Lösung + 24/7 Threat Monitoring
⚠ Kompromittierte Passwörter	✅ Enterprise Password Manager + Automatische Rotation
⚠ Fehlende MFA	✅ MFA-Rollout für alle kritischen Systeme
⚠ Phishing-Anfälligkeit	✅ Security Awareness Training

Nächster Schritt

📧 kontakt@techguard-it.de 📞 +49 89 123 456-0

Jetzt Sicherheitsberatung anfragen

Sofortmaßnahmen-Checkliste

Priorisierte Aufgaben basierend auf Ihrer Risikoanalyse

SOFORT (0-4 Stunden)

- [ ] Infiziertes Gerät identifizieren: **ge***@beispiel-gmbh.de**
- [ ] Infiziertes Gerät identifizieren: **in***@beispiel-gmbh.de**
- [ ] Infiziertes Gerät identifizieren: **bu***@beispiel-gmbh.de**
- [ ] Infiziertes Gerät identifizieren: **az***@beispiel-gmbh.de**

DRINGEND (24-48 Stunden)

- [ ] MFA aktivieren: **ge***@beispiel-gmbh.de**
- [ ] Passwort zurücksetzen: **ge***@beispiel-gmbh.de**
  für linkedin.com, xing.com, microsoft365.com
- [ ] MFA aktivieren: **in***@beispiel-gmbh.de**
- [ ] Passwort zurücksetzen: **in***@beispiel-gmbh.de**
  für mailchimp.com, canva.com, dropbox.com
- [ ] MFA aktivieren: **bu***@beispiel-gmbh.de**
- [ ] Passwort zurücksetzen: **bu***@beispiel-gmbh.de**
  für datev.de, lexoffice.de, paypal.com, sparkasse.de
- [ ] MFA aktivieren: **az***@beispiel-gmbh.de**
- [ ] Passwort zurücksetzen: **az***@beispiel-gmbh.de**
  für grabcad.com, autodesk.com, github.com

Diese Woche

- [ ] SPF-Eintrag konfigurieren: `beispiel-gmbh.de`
- [ ] DMARC-Eintrag konfigurieren: `beispiel-gmbh.de`