ENDOLUM SENTINEL · BEISPIELBERICHT

Aussensicht auf Ihre öffentliche Infrastruktur.

example-gmbh.ch

SCAN VOM 20. APRIL 2026

ZUSAMMENFASSUNG

Sentinel hat die öffentlich erreichbare Infrastruktur von example-gmbh.ch untersucht und 7 gruppierte Befunde an 5 exponierten Diensten gefunden. Zwei Befunde erfordern sofortiges Handeln: ein Microsoft Exchange Server ohne Hersteller Support und eine aus dem Internet erreichbare Datenbank ohne Passwortschutz.

VERDIKT

Ihr Exchange Server hat den Support verloren, Ihre Datenbank ist ohne Passwort erreichbar. Beides wird aktiv von automatisierten Angriffen ausgenutzt. Kontaktieren Sie Ihren IT Dienstleister noch heute.

1	2	1	2	1
KRITISCH	HOCH	MITTEL	NIEDRIG	INFO

Dieser Bericht ist auf der Basis eines echten Sentinel Scans gegen ein synthetisches Ziel erzeugt. Sämtliche Hostnamen, IP Adressen und Identifikatoren sind anonymisiert. Schweregrad, Belege und Behebungsschritte spiegeln das tatsächliche Format eines bezahlten Sentinel Berichts.

Endolum GmbH · Oberdorfstrasse 8, 8853 Lachen SZ · CHE-297.991.738 · endolum.io

KRITISCH

Microsoft Exchange Server 2013 ohne Hersteller Support

Ihr Mailserver unter mail.example-gmbh.ch läuft auf Exchange Server 2013. Microsoft hat den Support im April 2023 eingestellt. Jede seither veröffentlichte Schwachstelle in Exchange 2013 bleibt auf diesem Server dauerhaft ungepatcht.

RISIKO

Automatisierte Angriffe scannen jede Schweizer IP Adresse mit exponiertem Exchange mehrmals täglich. Ein erfolgreicher Angriff verschafft Zugriff auf sämtliche Postfächer und ist typischerweise der erste Schritt vor einer Ransomware Verschlüsselung im internen Netzwerk. Cyber Versicherungen lehnen Schadenersatz häufig ab, wenn End of Life Software als Ursache identifiziert wird.

BEHEBUNG

Planen Sie die Migration aus Exchange 2013 in den nächsten Wochen. Für die meisten KMU ist der Umzug auf Microsoft 365 die praktikable Antwort. Ihr IT Dienstleister begleitet Scoping und Ausführung.

TECHNISCHE UMSETZUNG

> Zielsystem: Microsoft 365 Business Standard oder Exchange Server SE. Vorgehen: M365 Mandant aufsetzen, Azure AD Connect oder Entra Cloud Sync aktivieren, Postfächer in Wellen via EAC oder Drittanbieter Tool migrieren, MX Records umstellen, on prem Server abschalten. Zeitrahmen 2 bis 4 Wochen.

BELEG

> OWA unter https://mail.example-gmbh.ch/owa/ liefert X-OWA-Version: 15.0.1497.2. Letztes verfügbares Sicherheitsupdate für Exchange 2013 erschien im Mai 2023.

Referenz: https://learn.microsoft.com/en-us/exchange/new-features/updates

HOCH

MongoDB Datenbank auf Port 27017 offen ohne Authentifizierung

Eine MongoDB Datenbank nimmt Verbindungen aus dem öffentlichen Internet entgegen, ohne ein Passwort zu verlangen. Jeder, der den Port findet, kann sämtliche Inhalte lesen, ändern oder löschen.

RISIKO

Offene MongoDB Instanzen werden routinemässig von Erpresser Bots gefunden und gelöscht. Falls die Datenbank Kunden oder Mitarbeiterdaten enthält, gilt jeder unautorisierte Zugriff nach Schweizer DSG als meldepflichtige Datenschutzverletzung. Bereits die Exposition begründet ein regulatorisches Risiko.

BEHEBUNG

Schliessen Sie Port 27017 noch heute auf der Firewall und verlangen Sie ein Passwort für Verbindungen. Ihr IT Dienstleister kann die Datenbank an localhost binden und Authentifizierung im nächsten Wartungsfenster aktivieren.

TECHNISCHE UMSETZUNG

> In /etc/mongod.conf: net.bindIp: 127.0.0.1 und security.authorization: enabled setzen. Admin User anlegen: use admin; db.createUser({user: 'admin', pwd: '<stark>', roles: ['root']}). mongod neu starten. Auf der Firewall eingehenden 27017/tcp Verkehr von allen externen Adressen blockieren.

BELEG

> TCP 27017 offen auf 203.0.113.42. MongoDB 4.4.18. isMaster lieferte ok: 1 ohne Anmeldedaten.

HOCH

Remote Desktop (RDP) aus dem Internet erreichbar

Port 3389 auf Ihrem Server ist aus dem öffentlichen Internet erreichbar. Aus dem Netz exponierter Remote Desktop ist der mit Abstand häufigste Einstiegspunkt für Ransomware Angriffe gegen Schweizer KMU.

RISIKO

Automatisiertes Passwort Raten trifft exponiertes RDP mehrere tausend Mal pro Stunde. Selbst mit starkem Passwort betrifft jede neue Windows Schwachstelle, die RDP berührt, Ihren Betrieb. Eine erfolgreiche Kompromittierung führt typischerweise innerhalb von 24 Stunden zur Ransomware Verschlüsselung.

BEHEBUNG

Entfernen Sie Remote Desktop diese Woche aus dem öffentlichen Internet. Routen Sie administrativen Zugriff über VPN oder Zero Trust. Ihr IT Dienstleister erledigt das in wenigen Stunden.

TECHNISCHE UMSETZUNG

> 3389/tcp auf der Perimeter Firewall blockieren. Optionen für Admin Zugriff: WireGuard oder OpenVPN Site to Site, Tailscale, Cloudflare Access mit Service Tokens, oder RDP Gateway mit MFA. Falls kurzfristige Exposition unvermeidbar ist: NLA aktivieren, Account Lockout bei 5 Versuchen für 30 Minuten konfigurieren, Rate Limiting pro Quell IP ergänzen.

BELEG

> TCP 3389 offen auf 203.0.113.42. Banner: Microsoft Terminal Services. TLS 1.2 mit Zertifikat CN=SERVER01.example-gmbh.local (selbstsigniert).

MITTEL

Veraltete TLS Versionen auf Mail und Webserver akzeptiert

Ihr Mailserver und Ihre Website akzeptieren TLS 1.0 und TLS 1.1 Verbindungen. Beide Versionen weisen bekannte Schwächen auf und gelten nicht mehr als sicher. Moderne Clients bevorzugen ohnehin TLS 1.2 oder 1.3.

RISIKO

Ein Angreifer im selben Netz wie ein Mitarbeiter (öffentliches WLAN, kompromittierter Router) kann die Verbindung auf die ältere Version herabstufen und den Datenverkehr mitlesen. Compliance Audits und Cyber Versicherungs Fragebögen führen diesen Punkt regelmässig auf.

BEHEBUNG

TLS 1.0 und 1.1 auf beiden Servern durch Ihren IT Dienstleister abschalten lassen. Die Auswirkung auf Endnutzer ist minimal, moderne Clients sprechen ohnehin TLS 1.2 oder 1.3.

TECHNISCHE UMSETZUNG

```
IIS: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server Enabled=0 und DisabledByDefault=1 setzen (analog für TLS 1.1). Reboot.
nginx: ssl_protocols TLSv1.2 TLSv1.3; und nginx -s reload. Verifikation mit sslscan mail.example-gmbh.ch und sslscan www.example-gmbh.ch.
```

BELEG

```
mail.example-gmbh.ch:443 akzeptiert TLSv1.0 (RSA-AES128-SHA). www.example-gmbh.ch:443 akzeptiert TLSv1.1.
```

NIEDRIG

Security Header auf www.example-gmbh.ch fehlen

Ihre Website sendet mehrere HTTP Antwort Header nicht, mit denen Browser den Schaden eingrenzen, falls etwas auf der Seite aus dem Ruder läuft. Da die Seite keine Login Formulare oder Nutzereingaben enthält, ist das praktische Risiko gering.

RISIKO

Fehlende Header lassen einen Angreifer nicht herein. Falls aber ein Bug in der Seite Code Injektion erlaubt, würden diese Header den Bewegungsspielraum des Angreifers begrenzen.

BEHEBUNG

Standard Security Header durch Ihren IT Dienstleister ergänzen lassen. 15 Minuten Aufwand, keine funktionalen Auswirkungen auf die Seite.

TECHNISCHE UMSETZUNG

> Im nginx Server Block (oder Apache Äquivalent) ergänzen: add_header Content-Security-Policy "default-src 'self'" always; add_header X-Frame-Options DENY always; add_header X-Content-Type-Options nosniff always; add_header Referrer-Policy strict-origin-when-cross-origin always; add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always. nginx neu laden. Verifikation auf securityheaders.com.

BELEG

> GET https://www.example-gmbh.ch/ Antwort enthält weder Content-Security-Policy noch X-Frame-Options noch X-Content-Type-Options noch Referrer-Policy noch Strict-Transport-Security.

Referenz: https://securityheaders.com

NIEDRIG

Webserver Version in HTTP Antworten sichtbar

Jede Antwort Ihrer Website enthält einen Header, der die exakte Software Version offenlegt. Angreifer, die nach verwundbaren Versionen suchen, lesen genau diesen Header.

RISIKO

Eine Versionsangabe alleine bricht nichts auf. Sie sorgt aber dafür, dass Ihre Adresse bei jeder neuen veröffentlichten Schwachstelle für Ihre konkrete Version schneller auf die Listen automatisierter Scanner gerät.

BEHEBUNG

Detaillierte Server Version in Antwort Headern durch Ihren IT Dienstleister ausblenden lassen. Kleine Änderung, keine Auswirkung auf Endnutzer.

TECHNISCHE UMSETZUNG

```
Apache: ServerTokens Prod und ServerSignature Off in der Hauptkonfiguration setzen, Reload. nginx: server_tokens off; im http Block setzen, Reload. Verifikation mit curl -sI https://www.example-gmbh.ch zeigt Server: Apache oder Server: nginx ohne Versionsangabe.
```

BELEG

```
HTTP/1.1 200 OK Antwort Header: Server: Apache/2.4.52 (Ubuntu).
```

INFO

Spoofing Schutz fehlt für example-gmbh.ch

Ihre Domain veröffentlicht weder einen SPF noch einen DMARC Eintrag. Diese DNS Einträge teilen anderen Mailservern mit, welche Systeme im Namen von @example-gmbh.ch senden dürfen und wie mit Nachrichten umzugehen ist, die diese Prüfung nicht bestehen.

RISIKO

Ohne diese Einträge kann jeder Mail im Namen Ihrer Domain senden, die echt aussieht. Mitarbeiter, Kunden und Lieferanten können mit überzeugenden gefälschten Mails phishing attackiert werden. Gleichzeitig landet Ihre legitime ausgehende Mail häufiger im Spam Ordner der Empfänger.

BEHEBUNG

SPF Eintrag und DMARC Eintrag durch Ihren IT Dienstleister ergänzen lassen. 10 Minuten Konfiguration plus DNS Propagationszeit.

TECHNISCHE UMSETZUNG

```
SPF: TXT Record auf example-gmbh.ch: v=spf1 include:spf.protection.outlook.com -all (include Wert an den tatsächlichen Mail Provider anpassen). DMARC: TXT Record auf _dmarc.example-gmbh.ch: v=DMARC1; p=quarantine; rua=mailto:dmarc@example-gmbh.ch. Mit p=none zwei Wochen starten, Aggregate Reports auswerten, dann auf p=quarantine und schliesslich p=reject anziehen.
```

BELEG

```
dig TXT example-gmbh.ch liefert keinen v=spf1 Eintrag. dig TXT _dmarc.example-gmbh.ch liefert NXDOMAIN.
```

Referenz: https://mxtoolbox.com/spf.aspx

Nächste Schritte

01 Bericht heute an Ihren IT Dienstleister weiterleiten. Auftrag erteilen, die Exchange Migration anzustossen und den offenen MongoDB Port sofort zu schliessen.

02 Diese Woche bestätigen, dass Remote Desktop nicht mehr aus dem Internet erreichbar ist und durch VPN oder Zero Trust ersetzt wurde.

03 Innerhalb eines Monats TLS 1.0 und 1.1 auf allen Servern abschalten und die Standard Security Header auf der Website ergänzen.

04 Vor dem nächsten Audit oder vor der Erneuerung der Cyber Versicherung SPF und DMARC Einträge publizieren und die Webserver Version verstecken.

05 Sentinel Business abonnieren, damit wöchentliche Rescans zeigen, was neu, behoben oder zurückgekehrt ist.