QUANSATECH IT

MUSTERBERICHT - FIKTIVES BEISPIEL

# IT-Sicherheitscheck

Verständliche Sicherheitsbewertung für kleine und mittlere Unternehmen

| | |
|---|---|
| Unternehmen | Musterbetrieb GmbH |
| Berichtsnummer | QS-DEMO-2026-001 |
| Prüfdatum | 29. August 2026 |
| Leistung | IT-Sicherheitscheck - 599 EUR netto |

**Wichtiger Hinweis**

Dieser Bericht zeigt Aufbau und Verständlichkeit des Ergebnisses. Unternehmen, Systeme und Befunde sind vollständig fiktiv. Technische Rohdaten, interne Werkzeuge und konkrete Prüfschritte sind im Muster bewusst nicht enthalten.

MANAGEMENT-ZUSAMMENFASSUNG

# Was die Geschäftsführung wissen sollte

**Gesamteinschätzung: Handlungsbedarf vorhanden**

Im vereinbarten externen Prüfumfang wurde kein Hinweis auf einen bereits eingetretenen Sicherheitsvorfall festgestellt. Zwei Punkte sollten jedoch zeitnah mit dem bestehenden IT-Betreuer geklärt beziehungsweise verbessert werden.

| 2 | 1 | 2 | 0 |
|---|---|---|---|
| bestätigte Befunde | intern zu prüfen | unauffällige Bereiche | akute Vorfälle |

## Einordnung in klaren Worten

Die wichtigsten Unternehmensdienste waren zum Prüfzeitpunkt erreichbar und die Hauptwebsite nutzte eine gültige Transportverschlüsselung. Verbesserungsbedarf besteht beim Schutz der Unternehmens-E-Mail-Domain. Zusätzlich sollte der Wartungsstand eines öffentlich erreichbaren Dienstes intern bestätigt werden.

Aus diesen Punkten folgt nicht, dass das Unternehmen bereits kompromittiert wurde. Sie zeigen, wo mit überschaubarem Aufwand unnötiges Risiko reduziert werden kann.

## Bewertungslogik

| Status | Bedeutung | Entscheidung |
|---|---|---|
| **Bestätigt** | Der Befund ist im vereinbarten Umfang nachvollziehbar belegt. | Maßnahme planen |
| **Prüfen** | Ein Hinweis benötigt interne Informationen oder eine eigene Freigabe. | Zuständigkeit klären |
| **Beobachten** | Kein akuter Handlungsdruck, Verbesserung ist dennoch sinnvoll. | Termin vormerken |
| **In Ordnung** | Im geprüften Umfang war kein relevanter Hinweis erkennbar. | Regelmäßig erneut prüfen |

## Prüfumfang und Grenzen

Vereinbart waren eine Unternehmensdomain, bis zu zwei öffentlich erreichbare Adressen, ein priorisierter Bericht und eine Ergebnisbesprechung. Interne Netze, Benutzerkonten, Anwendungen hinter einer Anmeldung und störende Eingriffe waren nicht Teil dieses Einstiegschecks.

BEFUNDE IM ÜBERBLICK

# Prioritäten statt technischer Warnungslisten

Jeder Punkt ist so formuliert, dass die Geschäftsführung die Auswirkung und den nächsten Schritt erkennen kann. Technische Nachweise werden im echten Kundenbericht separat referenziert und können an den bestehenden IT-Betreuer übergeben werden.

| ID | Befund | Status | Priorität | Empfohlener Termin |
|---|---|---|---|---|
| **B-01** | Schutz der Unternehmens-E-Mail-Domain ist unvollständig | **Bestätigt** | **1** | innerhalb 7 Tagen |
| **B-02** | Öffentlich sichtbare technische Information auf einem Nebensystem | **Bestätigt** | **2** | innerhalb 30 Tagen |
| **P-01** | Wartungsstand eines erreichbaren Unternehmensdienstes bestätigen | **Prüfen** | **2** | innerhalb 14 Tagen |
| **O-01** | Transportverschlüsselung der Hauptwebsite | **In Ordnung** | - | jährlich erneut prüfen |
| **O-02** | Weiterleitung auf die verschlüsselte Hauptadresse | **In Ordnung** | - | bei Änderungen prüfen |

### Was diese Übersicht nicht behauptet

Ein bestätigter Befund ist kein Beweis für einen erfolgreichen Angriff. Ein unauffälliger Punkt ist keine dauerhafte Sicherheitsgarantie. Der Bericht beschreibt den beobachteten Stand zum Prüfzeitpunkt innerhalb des vereinbarten Umfangs.

## So wird aus einem Befund eine Entscheidung

Priorität 1 bedeutet: kurzfristig zuständig machen und eine kontrollierte Änderung planen. Priorität 2 bedeutet: innerhalb des nächsten Wartungsfensters bewerten oder verbessern. Maßnahmen werden nicht automatisch verkauft oder ohne Freigabe umgesetzt.

BEISPIEL EINES DETAILBEFUNDS

# B-01: Schutz der E-Mail-Domain ist unvollständig

BESTÄTIGT | PRIORITÄT 1 | ZIEL: 7 TAGE

## Warum das für das Unternehmen relevant ist

Die E-Mail-Domain ist ein zentraler Teil der Unternehmensidentität. Eine unvollständige Schutzeinstellung kann es Dritten erleichtern, Nachrichten glaubwürdig im Namen des Unternehmens erscheinen zu lassen. Das erhöht das Risiko für Zahlungsbetrug, Zugangsdaten-Diebstahl und Rückfragen bei Kunden oder Lieferanten.

## Was bestätigt wurde

Zum Prüfzeitpunkt war für die fiktive Domain eine Schutzvorgabe öffentlich erkennbar, die nicht in allen Fällen eine konsequente Zurückweisung unberechtigter Nachrichten verlangt. Der Nachweis wurde dokumentiert und ist im Kundenbericht technisch referenziert.

### Nachweis im Muster bewusst gekürzt

Prüfobjekt: musterbetrieb.example
Prüfzeitpunkt: 29.08.2026, 10:15 Uhr
Nachweis-ID: B-01-E1
Technische Rohdaten: [nur im vertraulichen Kundenanhang]

## Was nicht behauptet wird

Es wurde kein Missbrauch eines Postfachs festgestellt. Es wurde kein Zugang zu E-Mail-Konten versucht und keine Nachricht an Mitarbeitende versendet. Der Befund bezieht sich ausschließlich auf die öffentlich erkennbare Schutzkonfiguration.

## Empfohlener nächster Schritt

Der bestehende IT-Betreuer sollte die E-Mail-Domain und alle berechtigten Versandwege prüfen, die Änderung zunächst kontrolliert vorbereiten und anschließend überwachen. Eine übereilte Umstellung ohne Bestandsaufnahme kann legitime Geschäftsmails beeinträchtigen.

### Entscheidung für die Geschäftsführung

Aufgabe an den IT-Betreuer vergeben, Verantwortlichen und Termin festlegen, nach der Änderung einen kurzen Wirksamkeitsnachweis anfordern. Ein Austausch der gesamten IT-Infrastruktur ist aus diesem Einzelbefund nicht ableitbar.

MASSNAHMEN UND NÄCHSTE SCHRITTE

# Ein Plan, den Sie selbst steuern können

Der Bericht soll eine Entscheidung ermöglichen, nicht zu einem Folgeauftrag zwingen. Die Maßnahmen können durch Quansatech, den bisherigen IT-Betreuer oder einen anderen qualifizierten Dienstleister umgesetzt werden.

| Zeitraum | Empfohlene Entscheidung | Ergebnisnachweis |
|---|---|---|
| **0 bis 7 Tage** | B-01 zuständig machen und kontrollierte Verbesserung der E-Mail-Domain planen. | Schriftliche Bestätigung und erneute Prüfung |
| **8 bis 30 Tage** | B-02 und P-01 mit dem IT-Betreuer bewerten; Wartungsstand und Zuständigkeit dokumentieren. | Dokumentierter Sollzustand |
| **Danach** | Sicherheitscheck jährlich und nach größeren Änderungen wiederholen. | Vergleich zum vorherigen Stand |

## Ihre Wahl nach dem Bericht

### Bestehender IT-Betreuer

Erhält den Bericht und kann die Punkte im gewohnten Umfeld beheben.

### Quansatech

Kann auf Wunsch ein separates Fixpreisangebot für klar abgegrenzte Maßnahmen erstellen.

## Grenzen der Aussage

Der IT-Sicherheitscheck ist eine zeitpunktbezogene externe Einschätzung und kein vollständiger Penetrationstest. Er garantiert keine absolute Sicherheit und ersetzt weder laufende Updates noch Datensicherung, Monitoring oder interne Kontrollen. Weitergehende Prüfungen benötigen immer eine eigene schriftliche Vereinbarung.

### IT-Sicherheitscheck zum Fixpreis

599 EUR netto - vorab klar abgegrenzt - ohne Abo und ohne Verpflichtung für Folgeaufträge

### Quansatech GmbH

Steyrtalstraße 88, 4523 Neuzeug
+43 720 895056
office@quansatech.at
www.quansatech.at/it-sicherheitscheck/