WCS

Beispielbericht, fiktive Daten

# IT-Sicherheitscheck

## Wo Ihr Unternehmen steht und was zuerst zu tun ist.

Musterunternehmen GmbH, fiktives Beispiel


Termin vor Ort
13. bis 15. Oktober 2026

Erstellt von
Wenske Cyber Solutions GmbH

Stand
Version 1.0 · 22. Oktober 2026

1

# Zusammenfassung für die Geschäftsführung

Die Grundlagen stimmen: Virenschutz, Updates der Arbeitsplätze und die tägliche Datensicherung laufen. Ein Angreifer käme aber zu leicht hinein, und die Datensicherung wäre bei einem Angriff vermutlich mit betroffen.

| Gesamtbild | Dringend | Verbessern | In Ordnung |
|---|---|---|---|
| Erhöhtes Risiko | 6 | 11 | 7 |

Anzahl der 24 geprüften Punkte je Bewertung.

## Die drei dringendsten Punkte

1. **Zugang von unterwegs mit zweitem Faktor schützen**
   Heute genügt ein Passwort, um von außen ins Firmennetz zu kommen.
2. **Eine Kopie der Datensicherung getrennt aufbewahren**
   Sonst trifft eine Verschlüsselung auch die Sicherung, und Sie können nicht wieder anfangen.
3. **Alte Administratorkonten sperren**
   Drei Konten mit vollen Rechten gehören Personen, die nicht mehr für Sie arbeiten.

## Was als Nächstes zu tun ist

Die drei Punkte oben sind in wenigen Tagen erledigt. Danach folgt der Maßnahmenplan in Kapitel 8. Zwei Maßnahmen brauchen Ihre Entscheidung: neue Server und die Aufteilung des Netzes.

## Übersicht der geprüften Bereiche

| Kap. | Bereich | Kurz gesagt | Bewertung |
|---|---|---|---|
| 2 | Netzwerk und Firewall | Ein gemeinsames Netz für alle Geräte. | Verbessern |
| 3 | Fernzugriff | Zugang von außen nur mit Passwort. | Dringend |
| 4 | Server und Active Directory | Zu viele Administratoren, zwei veraltete Server. | Dringend |
| 5 | Arbeitsplätze | Gut geschützt, mit einzelnen Lücken. | Verbessern |
| 6 | E-Mail und Cloud-Dienste | Zu viele Ausnahmen beim zweiten Faktor. | Verbessern |
| 7 | Datensicherung und Notfallvorsorge | Sicherung nicht getrennt, kein Notfallplan. | Dringend |

2

# Netzwerk und Firewall

Verbessern

Die Firewall schützt nach außen ordentlich. Im Inneren hängen aber alle Geräte in einem gemeinsamen Netz.

| Prüfpunkt | Ergebnis | Bewertung |
|---|---|---|
| Von außen erreichbare Dienste | Nur VPN und Webmail erreichbar, keine Verwaltungsoberflächen. | In Ordnung |
| Unterteilung des internen Netzes | Server, Arbeitsplätze, Drucker und Gäste-WLAN in einem Netz. | Verbessern |
| Aktualität der Firewall | Letztes Update vor 14 Monaten. | Verbessern |
| Gäste-WLAN | Vom Firmennetz getrennt. | In Ordnung |

Befund 2.1

## Alle Geräte hängen in einem gemeinsamen Netz

| | |
|---|---|
| Was das bedeutet | Wer einen einzigen Arbeitsplatz übernimmt, etwa über eine präparierte E-Mail, erreicht von dort aus direkt alle Server, auch die Warenwirtschaft und die Datensicherung. |
| Was zu tun ist | Das Netz in Bereiche aufteilen: Server, Arbeitsplätze, Drucker und Telefone, Gäste. Zwischen den Bereichen ist nur erlaubt, was der Betrieb braucht. |
| Fundstelle für die IT | Firewall Hauptsitz, Regelwerk: interne Regel erlaubt jeden Verkehr zwischen allen internen Adressen. Keine VLAN-Trennung am Core-Switch. |

Befund 2.2

## Die Firewall ist seit über einem Jahr nicht aktualisiert

| | |
|---|---|
| Was das bedeutet | Bekannte Sicherheitslücken in der Firewall bleiben offen. Gerade diese Geräte sind ein häufiges Ziel, weil sie direkt am Internet hängen. |
| Was zu tun ist | Aktuelle Firmware einspielen und einen festen Termin für Updates vereinbaren, zum Beispiel monatlich. |
| Fundstelle für die IT | Firewall Hauptsitz und Außenlager, Firmware-Stand vom August 2025. |

3

# Fernzugriff

● Dringend

Der Zugang von unterwegs ist nur mit einem Passwort geschützt. Ein Dienstleister hat einen dauerhaft offenen Zugang.

| Prüfpunkt | Ergebnis | Bewertung |
|---|---|---|
| VPN-Zugang der Mitarbeitenden | Anmeldung nur mit Passwort, ohne zweiten Faktor. | ● Dringend |
| Fernwartung durch Dienstleister | Ein Zugang dauerhaft freigeschaltet, ohne Protokoll. | ● Dringend |
| Übersicht der Zugänge | Liste vorhanden, aber nicht aktuell. | ● Verbessern |

Befund 3.1

## Der VPN-Zugang ist nur mit einem Passwort geschützt

| | |
|---|---|
| Was das bedeutet | Ein erratenes oder bei einem anderen Dienst gestohlenes Passwort genügt, um von außen ins Firmennetz zu kommen. Das ist einer der häufigsten Wege, über die Angreifer in Unternehmen gelangen. |
| Was zu tun ist | Für alle VPN-Konten einen zweiten Faktor einrichten, zum Beispiel eine App auf dem Diensthandy. Konten, die niemand mehr nutzt, löschen. |
| Fundstelle für die IT | VPN-Gateway der Firewall Hauptsitz, 38 aktive Konten, davon 6 seit über 90 Tagen ohne Anmeldung. |

Befund 3.2

## Ein Fernwartungszugang steht dauerhaft offen

| | |
|---|---|
| Was das bedeutet | Der Softwarehersteller der Warenwirtschaft kann sich jederzeit verbinden, ohne dass jemand im Haus davon erfährt. Wird der Hersteller angegriffen, ist auch Ihr Netz erreichbar. |
| Was zu tun ist | Den Zugang nur bei Bedarf freischalten, mit Freigabe durch Ihre IT, und jede Sitzung protokollieren. |
| Fundstelle für die IT | Fernwartungssoftware auf dem Anwendungsserver, Dienst startet automatisch, unbeaufsichtigter Zugriff aktiv. |

4

# Server und Active Directory

● Dringend

Zu viele Konten haben volle Administratorrechte. Zwei Server erhalten keine Sicherheitsupdates mehr.

| Prüfpunkt | Ergebnis | Bewertung |
|---|---|---|
| Konten mit Administratorrechten | 9 Konten mit vollen Rechten, davon 3 nicht mehr in Gebrauch. | ● Dringend |
| Trennung von Alltags- und Adminkonten | Administratoren arbeiten mit demselben Konto wie im Alltag. | ● Verbessern |
| Updates der Server | Zwei Server mit Betriebssystem ohne Herstellerunterstützung. | ● Dringend |
| Kennwortregeln | Angemessen eingestellt. | ● In Ordnung |

Befund 4.1

## Neun Konten haben volle Administratorrechte

| | |
|---|---|
| Was das bedeutet | Jedes dieser Konten kann das gesamte Netz übernehmen. Drei gehören zu ehemaligen Mitarbeitenden oder einem früheren Dienstleister und sind trotzdem noch aktiv. |
| Was zu tun ist | Die drei alten Konten sofort sperren. Volle Rechte auf zwei bis drei Personen beschränken, die dafür ein eigenes Konto nur für Verwaltungsaufgaben nutzen. |
| Fundstelle für die IT | Active Directory, Gruppe Domänen-Admins: 9 Mitglieder, 3 ohne Anmeldung seit über 180 Tagen. |

Befund 4.2

## Zwei Server bekommen keine Sicherheitsupdates mehr

| | |
|---|---|
| Was das bedeutet | Für das Betriebssystem dieser Server veröffentlicht der Hersteller keine Updates mehr. Neue Lücken bleiben dauerhaft offen. |
| Was zu tun ist | Die Ablösung planen und als Budgetentscheidung vorlegen. Bis dahin die beiden Server im Netz so abschotten, dass nur die nötigen Verbindungen möglich sind. |
| Fundstelle für die IT | Dateiserver und Druckserver, Windows Server 2012 R2 (Herstellerunterstützung seit Oktober 2023 beendet). |

5

# Arbeitsplätze

Verbessern

Virenschutz und Updates laufen zuverlässig. Einige Laptops sind nicht verschlüsselt, und viele Mitarbeitende haben Administratorrechte.

| Prüfpunkt | Ergebnis | Bewertung |
|---|---|---|
| Virenschutz | Auf allen geprüften Geräten aktiv und aktuell. | In Ordnung |
| Updates von Windows und Office | Automatisch, Stand aktuell. | In Ordnung |
| Verschlüsselung der Laptops | 6 von 41 Laptops nicht verschlüsselt. | Verbessern |
| Administratorrechte der Mitarbeitenden | Rund ein Drittel der Nutzer ist lokaler Administrator. | Verbessern |

Befund 5.1

## Sechs Laptops sind nicht verschlüsselt

| | |
|---|---|
| Was das bedeutet | Geht einer dieser Laptops verloren, kann jeder die Daten darauf lesen, auch Kundendaten und gespeicherte Zugänge. |
| Was zu tun ist | Die Verschlüsselung auf allen Laptops einschalten und zentral prüfen, ob sie aktiv bleibt. |
| Fundstelle für die IT | Geräteverwaltung, 6 Geräte ohne aktive Laufwerksverschlüsselung (BitLocker). |

Befund 5.2

## Viele Mitarbeitende haben Administratorrechte am eigenen Gerät

| | |
|---|---|
| Was das bedeutet | Öffnet jemand versehentlich eine Schadsoftware, kann sie sich mit diesen Rechten ungehindert einnisten. |
| Was zu tun ist | Die Rechte entziehen. Wer sie für einzelne Programme braucht, bekommt eine Lösung für genau diesen Fall. |
| Fundstelle für die IT | Lokale Gruppe Administratoren auf 14 von 43 geprüften Geräten mit Benutzerkonto erweitert. |

6

# E-Mail und Cloud-Dienste

Verbessern

Die Anmeldung mit zweitem Faktor ist eingeführt, hat aber zu viele Ausnahmen. Gefälschte E-Mails in Ihrem Namen werden noch nicht abgewiesen.

| Prüfpunkt | Ergebnis | Bewertung |
|---|---|---|
| Anmeldung mit zweitem Faktor | Eingeführt, 12 Konten ausgenommen. | Verbessern |
| Schutz vor gefälschten Absendern | Nur im Beobachtungsmodus. | Verbessern |
| Freigaben nach außen | Dateien per Link ohne Anmeldung teilbar. | Verbessern |
| Schutz vor Schadsoftware in E-Mails | Aktiv. | In Ordnung |

Befund 6.1

## Zwölf Konten melden sich ohne zweiten Faktor an

| | |
|---|---|
| Was das bedeutet | Darunter sind zwei Sammelpostfächer und das Konto der Geschäftsführung. Ein gestohlenes Passwort reicht dort für den Zugriff auf alle E-Mails. |
| Was zu tun ist | Jede Ausnahme prüfen. Sammelpostfächer ohne eigene Anmeldung betreiben, alle übrigen Konten mit zweitem Faktor schützen. |
| Fundstelle für die IT | Microsoft 365, Richtlinie für bedingten Zugriff: Ausschlussgruppe mit 12 Mitgliedern. |

Befund 6.2

## Gefälschte E-Mails in Ihrem Namen werden zugestellt

| | |
|---|---|
| Was das bedeutet | Angreifer können E-Mails verschicken, die aussehen, als kämen sie von Ihnen, etwa eine geänderte Bankverbindung an Ihre Kunden. |
| Was zu tun ist | Die Absenderprüfung schrittweise von „beobachten“ auf „abweisen“ umstellen. |
| Fundstelle für die IT | DNS der Domain: DMARC-Eintrag mit Richtlinie p=none. |

Befund 6.3

## Dateien lassen sich ohne Anmeldung nach außen teilen

| | |
|---|---|
| Was das bedeutet | Ein weitergeleiteter Link öffnet die Datei für jeden, der ihn hat. Wer was geteilt hat, ist kaum nachzuvollziehen. |
| Was zu tun ist | Freigaben nur noch für bestimmte Personen zulassen und bestehende offene Links prüfen. |
| Fundstelle für die IT | SharePoint und OneDrive, Freigabeeinstellung „Jeder mit dem Link“, 57 aktive Links. |

7

# Datensicherung und Notfallvorsorge

● Dringend

Die Datensicherung läuft täglich, ist aber mit denselben Zugängen erreichbar wie die Server. Einen Notfallplan gibt es nicht.

| Prüfpunkt | Ergebnis | Bewertung |
|---|---|---|
| Tägliche Datensicherung | Läuft, Protokolle vollständig. | ● In Ordnung |
| Getrennte Aufbewahrung | Sicherung im selben Netz, mit Adminkonto erreichbar. | ● Dringend |
| Wiederherstellung getestet | Kein dokumentierter Test. | ● Verbessern |
| Notfallplan und Zuständigkeiten | Nicht vorhanden. | ● Dringend |
| Sensibilisierung der Mitarbeitenden | Letzte Schulung vor über zwei Jahren. | ● Verbessern |

Befund 7.1

## Ein Angreifer könnte die Datensicherung mit verschlüsseln

| | |
|---|---|
| Was das bedeutet | Die Sicherung liegt im selben Netz und ist mit denselben Administratorkonten erreichbar. Bei einem Angriff mit Verschlüsselung wäre sie wahrscheinlich ebenfalls betroffen. Dann gibt es nichts, womit Sie wieder anfangen können. |
| Was zu tun ist | Eine Kopie getrennt aufbewahren, die sich nicht nachträglich ändern oder löschen lässt, und eigene Zugangsdaten nur für die Sicherung verwenden. |
| Fundstelle für die IT | Sicherungsserver im Servernetz, Anmeldung mit Domänen-Admin möglich, keine unveränderliche Kopie. |

Befund 7.2

## Niemand weiß, was im Ernstfall zu tun ist

| | |
|---|---|
| Was das bedeutet | Fällt die IT aus, ist unklar, wer entscheidet, wen man anruft und in welcher Reihenfolge Systeme wieder anlaufen. Das verlängert jeden Stillstand. |
| Was zu tun ist | Einen kurzen Notfallplan schreiben: Zuständigkeiten, Telefonliste auf Papier, Reihenfolge der wichtigsten Systeme. Die Wiederherstellung in einem eigenen Termin testen. |
| Fundstelle für die IT | Kein Notfallhandbuch, keine dokumentierte Wiederherstellungsprobe. |

8

# Maßnahmenplan

Was zuerst zu tun ist und was warten kann. Jede Maßnahme kann Ihre eigene IT, Ihr IT-Dienstleister oder WCS umsetzen. Sie entscheiden.

## Sofort · in den nächsten zwei Wochen

| Maßnahme | Bereich | Aufwand | Entscheidung GF |
|---|---|---|---|
| Zweiten Faktor für den VPN-Zugang einrichten | Fernzugriff | Stunden | |
| Alte Administratorkonten sperren | Server und Active Directory | Stunden | |
| Getrennte, unveränderliche Kopie der Datensicherung | Datensicherung | Tage | Ja |
| Fernwartungszugang nur bei Bedarf freischalten | Fernzugriff | Stunden | |

## Bald · in den nächsten drei Monaten

| Maßnahme | Bereich | Aufwand | Entscheidung GF |
|---|---|---|---|
| Ausnahmen beim zweiten Faktor abbauen | E-Mail und Cloud | Stunden | |
| Firewall aktualisieren, Update-Termin festlegen | Netzwerk | Stunden | |
| Administratorrechte auf eigene Konten beschränken | Server und Active Directory | Tage | |
| Notfallplan schreiben, Wiederherstellung testen | Notfallvorsorge | Tage | Ja |
| Laptops verschlüsseln | Arbeitsplätze | Stunden | |

## Mittelfristig · innerhalb eines Jahres

| Maßnahme | Bereich | Aufwand | Entscheidung GF |
|---|---|---|---|
| Netz in Bereiche aufteilen | Netzwerk | Wochen | Ja |
| Zwei Server ablösen | Server | Wochen | Ja |
| Lokale Administratorrechte entziehen | Arbeitsplätze | Tage | |
| Absenderprüfung auf „abweisen“ umstellen | E-Mail | Stunden | |
| Freigaben nach außen einschränken | Cloud-Dienste | Stunden | |
| Mitarbeitende sensibilisieren | Notfallvorsorge | Tage | |

Aufwand als grobe Größenordnung. „Ja“: Entscheidung oder Budget der Geschäftsführung nötig.

9

# Über diesen Bericht

Der Bericht beschreibt den Stand Ihrer IT am Tag der Prüfung. Er belegt, dass Sie diesen Stand haben prüfen lassen, gegenüber Versicherer, Kunden und Prüfern.

## Was geprüft wurde

- Netzwerk und Firewall
- Fernzugriff, auch von Dienstleistern
- Server und Active Directory
- Arbeitsplätze
- E-Mail und Cloud-Dienste
- Datensicherung und Notfallvorsorge

## Wie geprüft wurde

- Termin vor Ort, 13. bis 15. Oktober 2026
- Gespräche mit Geschäftsführung und IT
- Einstellungen nur lesend ausgelesen, nichts verändert
- Zugänge nach der Prüfung wieder entfernt

## Was nicht Teil der Prüfung war

| Thema | Hinweis |
|---|---|
| Simulierter Angriff | Der Check prüft, wie Ihre IT aufgebaut und eingestellt ist. Einen Angriff simuliert er nicht. |
| Test der Wiederherstellung | Ob sich Daten aus der Sicherung tatsächlich zurückholen lassen, braucht mehr Zeit und gehört in einen eigenen Termin. |

## Bewertung

| Stufe | Bedeutung |
|---|---|
| Dringend | Ein Angreifer kann diese Lücke heute ausnutzen. Zeitnah schließen. |
| Verbessern | Erhöht das Risiko oder verlängert einen Ausfall. In den nächsten Monaten angehen. |
| In Ordnung | Entspricht dem, was für ein Unternehmen Ihrer Größe angemessen ist. |

Hinweis zu diesem Dokument

Dies ist ein Beispielbericht. Unternehmen, Zahlen und Befunde sind frei erfunden. Er zeigt Aufbau und Sprache des Berichts zum IT-Sicherheitscheck. Inhalt und Umfang Ihres Berichts richten sich nach Ihrer IT.