IT-Sicherheit im Mittelstand: Zehn Fragen, die weiterhelfen

Finden Sie die nächste sinnvolle Maßnahme für Ihren Betrieb

Die wichtigste Frage lautet oft nicht, welches Sicherheitsprodukt noch fehlt. Hilfreicher ist: **Welche geschäftskritische Aufgabe könnten wir morgen nicht mehr erledigen, und wie wären wir darauf vorbereitet?**

Mit diesen zehn Fragen können Geschäftsführung und IT gemeinsam offene Punkte sichtbar machen. Die Fragen sind eine redaktionelle Orientierung von network4you. Sie sind kein Penetrationstest, kein BSI-Zertifikat, kein formeller CyberRisikoCheck und keine Bestätigung gesetzlicher oder versicherungsvertraglicher Anforderungen.

Bewerten Sie jede Frage mit **nachgewiesen**, **teilweise** oder **ungeklärt**. „Nachgewiesen“ bedeutet: Eine verantwortliche Person kann den aktuellen Stand anhand eines Dokuments, einer Konfiguration oder eines Tests erläutern. Sammeln Sie keine Kennwörter in dieser Liste.

Die zehn Fragen

1. Wissen wir, welche Systeme für den Betrieb entscheidend sind?

Benennen Sie die wichtigsten Anwendungen, Daten und Arbeitsabläufe. Halten Sie fest, wer sie betreut und welche Abhängigkeiten bestehen. Eine Liste aller Computer allein zeigt noch nicht, was den Betrieb zum Stillstand bringen würde.

Nachweis: eine aktuelle Übersicht der kritischen Abläufe mit technischen und fachlichen Verantwortlichen.

2. Ist der Zugriff auf wichtige Konten angemessen abgesichert?

Prüfen Sie besonders Administratoren, E-Mail und Fernzugriffe. Wo unterstützt und passend eingerichtet, stärkt MFA die Anmeldung durch einen weiteren Nachweis. Sie ersetzt weder passende Rechte noch die Prüfung auffälliger Zugriffe. Microsoft unterscheidet dafür verschiedene Konfigurations- und Lizenzmodelle. [1]

Nachweis: geprüfte Anmelderegeln, notwendige Ausnahmen und ein getesteter Wiederzugang für Notfälle.

3. Werden Rechte bei Eintritt, Wechsel und Austritt angepasst?

Eine Person kann das Unternehmen verlassen, während Zugänge, Freigaben oder alte Fernwartungsrechte weiter bestehen. Klären Sie, wer Änderungen meldet, umsetzt und kontrolliert. Für technische Konten braucht es ebenfalls einen zuständigen Besitzer.

Nachweis: ein nachvollziehbarer Ablauf und die letzte abgeschlossene Berechtigungsprüfung.

4. Werden Sicherheitsupdates erkannt, geplant und überprüft?

Erfassen Sie Betriebssysteme, Anwendungen, Netzwerkgeräte und öffentlich erreichbare Dienste. Legen Sie fest, wer Herstellerhinweise bewertet, Updates testet und den erfolgreichen Abschluss kontrolliert. Nicht mehr unterstützte Systeme brauchen eine bewusst geplante Entscheidung. Die Bedeutung aktueller Software gehört auch zu den grundlegenden BSI-Empfehlungen für KMU. [2]

Nachweis: dokumentierter Updatezustand und ein Verfahren für dringende Schwachstellen.

5. Können wir wichtige Daten tatsächlich wiederherstellen?

Ein erfolgreicher Sicherungsjob ist ein wichtiges Signal, aber noch kein praktischer Wiederanlauf. Lassen Sie einen geeigneten Wiederherstellungstest durchführen und prüfen Sie, ob benötigte Daten und Anwendungen innerhalb der vorgesehenen Zeit nutzbar werden. Testen Sie so, dass der produktive Betrieb nicht unbeabsichtigt verändert wird.

Nachweis: Datum, Umfang, Dauer und Ergebnis eines Wiederherstellungstests sowie offene Abweichungen.

6. Sind Sicherungen ausreichend vom laufenden Betrieb getrennt?

Prüfen Sie Speicherorte, Berechtigungen und den administrativen Zugriff auf die Sicherungsumgebung. Die Anmeldedaten eines normalen Arbeitsplatzes sollten nicht automatisch den vollständigen Zugriff auf jede Sicherung eröffnen. Das passende Trennungsmodell hängt von Umgebung und Wiederherstellungszielen ab.

Nachweis: erklärtes Zugriffskonzept und dokumentierte Zuständigkeiten für die Sicherungen.

7. Erkennen und bearbeiten wir auffällige Ereignisse?

Warnungen helfen nur, wenn jemand sie einordnet und den nächsten Schritt kennt. Definieren Sie, welche Meldungen relevant sind, wer sie bearbeitet und wie bei Abwesenheit vertreten wird. Ein installiertes Schutzprodukt ist noch kein vollständiger Reaktionsprozess.

Nachweis: ein geklärter Bearbeitungsweg und ein Beispiel einer abgeschlossenen Meldung.

8. Sind externe Zugänge und Dienstleister nachvollziehbar geregelt?

Halten Sie fest, wer von außen auf welche Systeme zugreifen darf. Prüfen Sie notwendige Zugriffswege, Berechtigungen, Protokollierung und die Beendigung eines Zugangs. Unbekannte dauerhafte Fernzugriffe sind ein Grund für eine nähere Bestandsaufnahme.

Nachweis: aktuelle Zugangsliste mit Zweck, Verantwortlichem und Prüftermin.

9. Wissen Mitarbeiter, wie sie verdächtige Nachrichten melden?

Ein verständlicher Meldeweg ist wichtiger als die Erwartung, dass jeder jede Täuschung erkennt. Klären Sie den Umgang mit verdächtigen E-Mails und ungewöhnlichen Zahlungsänderungen. Ein Rückruf zur Prüfung verwendet einen bereits bekannten Kontaktweg, nicht unkritisch die Angaben aus der verdächtigen Nachricht.

Nachweis: ein bekannter Meldeweg und eine kurze, regelmäßig aufgefrischte Einweisung.

10. Gibt es einen nutzbaren Notfallplan außerhalb der betroffenen Systeme?

Wenn E-Mail, Server oder Telefonie ausfallen, müssen die wichtigsten Kontaktdaten trotzdem erreichbar sein. Legen Sie technische und geschäftliche Verantwortliche fest. Üben Sie einen begrenzten Ausfallfall und dokumentieren Sie die offenen Punkte.

Nachweis: zugänglicher Notfallplan und das Ergebnis einer Übung.

Auswertung ohne falsche Sicherheit

Addieren Sie keine Punkte zu einem vermeintlichen Sicherheitszertifikat. Eine einzelne ungeklärte Frage kann wichtiger sein als mehrere erfüllte Punkte. Priorisieren Sie nach **geschäftlicher Auswirkung**, **Zugriffsmöglichkeit eines Angreifers** und **vorhandenen Nachweisen**.

Feststellung	Sinnvoller nächster Schritt
Kritische Daten, aber kein Wiederherstellungsnachweis	Einen geeigneten Test und Verantwortliche vereinbaren.
Wichtiger externer Zugang ohne bekannten Besitzer	Berechtigung und Zweck durch die zuständige IT klären lassen.
Viele Warnungen, aber keine Bearbeitung	Meldeweg, Zuständigkeit und Vertretung festlegen.

Wählen Sie anschließend **eine** Maßnahme mit einem konkreten Ergebnis und einer verantwortlichen Person. Beheben Sie akute Auffälligkeiten nicht durch unkoordinierte Änderungen; ein laufender Sicherheitsvorfall braucht eine gesonderte fachliche Behandlung.

Vorhaben unverbindlich besprechen

Besprechen Sie mit network4you, welche offene Frage Sie zuerst bearbeiten sollten und welche Nachweise für Ihre Umgebung sinnvoll sind.

Telefon: 089 7412060 · **Kontakt:** network4you.com/kontakt/

Quellen und Stand

Stand: 5. November 2026. Die zehn Fragen und die Auswertung sind eigene redaktionelle Empfehlungen.

- [1] Microsoft: MFA für Microsoft 365 einrichten.
- [2] BSI: Cybersicherheit für KMU.
- Ergänzend: Microsoft, Zero Trust im Überblick.