# Cybersicherheits-Selbsttest

## CyberScore: 


Erstellungsdatum des Berichts: **08.11.2026 20:16**

> Dieser Bericht ist eine reine Selbsteinschätzung Ihres IT-Sicherheitsniveaus und beruht ausschließlich auf Ihren Antworten auf den von den Experten von Oxydian entwickelten Fragebogen. Er stellt in keinem Fall ein umfassendes technisches Audit dar. Er vermittelt Ihnen zwar einen ersten Überblick über Ihre Stärken und Schwachstellen im Bereich Cybersicherheit, ersetzt jedoch keine gründliche Analyse Ihrer Infrastruktur und Systeme. Wenn Sie weitergehen und ein vollständiges technisches Audit durchführen lassen möchten, kontaktieren Sie uns gerne:
>
> contact@oxydian.fr

## Zusammenfassung:

Ihr Sicherheitsniveau weist erhebliche Schwächen auf, die sofortige Aufmerksamkeit verdienen. Das Risiko, dass bestimmte Schwachstellen ausgenutzt werden, ist hoch und könnte die Gesamtsicherheit Ihrer Organisation gefährden. Wir empfehlen dringend, Korrekturmaßnahmen umzusetzen, und raten zu einer spezialisierten Begleitung, um ein umfassendes Audit durchzuführen.

## Ergebnisse je Kategorie im Detail (40.0%)

**Passwörter**



**Datensicherheit**



**Überwachung und Erkennung**



**Interne Sicherheit**



**Externe Sicherheit**



**Sicherheitsmanagement**



**Risikoidentifikation**



**Physische Sicherheit**



# Individueller Maßnahmenplan:

Dieser Maßnahmenplan basiert auf den Ergebnissen Ihrer Bewertung. Wir empfehlen Ihnen, diese Hinweise umzusetzen, um Ihre IT-Sicherheit zu verbessern.

**Sichere Aufbewahrung von Passwörtern**
Stellen Sie sicher, dass alle Passwörter in einem sicheren Passwort-Manager gespeichert werden und nicht auf unsicheren Medien.

**Ein Antivirenprogramm einsetzen**
Stellen Sie sicher, dass alle Ihre Server und Rechner mit einem aktuellen Antivirenprogramm ausgestattet sind, um Bedrohungen zu erkennen und zu blockieren.

**Ersatz veralteter Rechner**
Ersetzen oder migrieren Sie veraltete Rechner (Windows XP, Vista, 7, 8 oder Windows Server 2003 / 2008 / 2012), um das Risiko durch ungepatchte Schwachstellen zu verringern.

**Benutzer- und Administratorrechte trennen**
Dabei werden für tägliche Aufgaben und für administrative Aufgaben getrennte Konten vergeben. Das senkt das Risiko einer Kompromittierung erheblich, da erhöhte Berechtigungen nur für bestimmte Vorgänge genutzt werden, die tatsächlich Administratorrechte erfordern.

**Einführung einer Passwortrichtlinie**
Führen Sie eine strenge Passwortrichtlinie ein, um sicherzustellen, dass Passwörter sicher und komplex sind und regelmäßig erneuert werden.

**Schutz der E-Mail-Konten durch 2FA**
Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für alle E-Mail-Konten des Unternehmens (Microsoft 365, Google Workspace usw.). Die Kompromittierung von E-Mail-Konten ist der häufigste Angriffsweg gegen KMU, und die 2FA blockiert den Großteil dieser Angriffe.

**Regelmäßige Analyse der Passwörter**
Lassen Sie Ihre Passwörter regelmäßig von einem Fachmann oder Ihrer IT-Abteilung analysieren, um schwache und mehrfach verwendete Passwörter aufzuspüren und die Sicherheit zu erhöhen.

**Einführung der Festplattenverschlüsselung**
Wir empfehlen dringend, die Festplattenverschlüsselung auf allen PCs und Servern zu aktivieren, etwa mit BitLocker für Windows oder LUKS für Linux, um Ihre sensiblen Daten vor unbefugtem Zugriff zu schützen.

**Wiederherstellungstests der Backups**
Planen Sie regelmäßige Wiederherstellungstests (mindestens einmal pro Quartal), um zu prüfen, ob Ihre Backups tatsächlich nutzbar sind, und um die Zeit zu messen, die für die Wiederaufnahme Ihres Geschäftsbetriebs nötig ist.

**Erstellung einer Übersicht der externen Assets**
Aktualisieren und vervollständigen Sie regelmäßig die Übersicht Ihrer im Internet exponierten Assets, um das Sicherheitsmanagement zu verbessern.

**Einführung von 2FA für das VPN**
Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für alle VPN-Zugänge, um die Sicherheit von Fernverbindungen zu erhöhen.

**Verfahren zur Reaktion auf Sicherheitsvorfälle**
Dokumentieren Sie ein Verfahren zur Reaktion auf Sicherheitsvorfälle: Sofortmaßnahmen, Liste der Notfallkontakte (spezialisierter Dienstleister, Versicherung, zuständige Datenschutzaufsichtsbehörde bei einem Datenleck) und interne Rollen. Testen Sie es mindestens einmal pro Jahr in einer Planspielübung (Tabletop-Übung).

**Einführung der Zwei-Faktor-Authentifizierung**
Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) für alle Ihre kritischen Konten und Dienste, um eine zusätzliche Sicherheitsebene zu schaffen.

**Redundanz der Backups**
Wir empfehlen dringend, Ihre Backups an mehreren getrennten Orten aufzubewahren, um das Risiko eines Datenverlusts bei einem Schadensfall zu verringern.

**Umstieg auf eine EDR-Lösung**
Ersetzen oder ergänzen Sie Ihr klassisches Antivirenprogramm durch eine EDR-Lösung (Endpoint Detection and Response), die schädliches Verhalten erkennt und kompromittierte Rechner bei modernen Angriffen wie Ransomware isoliert.

**Zentrale Protokollierung**
Sammeln Sie die Protokolle Ihrer Server und kritischen Geräte zentral auf einem dedizierten Speicher und bewahren Sie sie mehrere Monate auf (6 bis 12 Monate empfohlen). So lassen sich Vorfälle erkennen und analysieren, selbst wenn der Angreifer lokale Spuren löscht.

**Erstellung einer Übersicht der internen Assets**
Aktualisieren und vervollständigen Sie regelmäßig die Übersicht Ihrer internen Assets, um das Sicherheitsmanagement zu verbessern.

**Segmentierung des WLANs**
Richten Sie mehrere WLAN-Netze ein, um öffentliche und interne Zugänge zu trennen, die Sicherheit zu erhöhen und gleichzeitig ein öffentliches WLAN ausschließlich für den Internetzugang anzubieten.

**Einführung einer externen Update-Richtlinie**
Führen Sie für alle Ihre externen Assets eine strenge Update-Richtlinie ein, um die Risiken durch Schwachstellen zu minimieren.

**Einführung einer IT-Nutzungsrichtlinie**
Stellen Sie sicher, dass alle Mitarbeitenden eine IT-Nutzungsrichtlinie unterzeichnen, die die Sicherheitsregeln und bewährten Verfahren festlegt, mit besonderem Augenmerk auf den Schutz personenbezogener Daten gemäß den Anforderungen der DSGVO.

**Regelmäßige Phishing-Simulationen**
Führen Sie mindestens einmal pro Jahr Phishing-Simulationen durch, um die Reaktionen Ihrer Mitarbeitenden unter realen Bedingungen zu messen und die Sensibilisierung gezielt auf die erkannten Schwachpunkte auszurichten.

**Regelung der Dienstleisterzugänge**
Regeln Sie die Zugänge Ihrer Dienstleister: eigene personenbezogene Konten, auf das unbedingt Notwendige beschränkte Rechte, konsequente Deaktivierung nach Abschluss des Einsatzes oder Vertragsende und Nachvollziehbarkeit der Verbindungen.

**Zugangskontrolle zum Serverraum**
Führen Sie eine strenge Zugangskontrolle für den Serverraum ein, um unbefugte Eingriffe zu verhindern.

**Einführung eines Onboarding-/Offboarding-Verfahrens**
Legen Sie ein klares Verfahren für den Eintritt und Austritt von Mitarbeitenden fest, einschließlich der Löschung von Konten und Zugängen, um das Unternehmen vor Sicherheitsrisiken zu schützen.

# Legende:

### INFORMATION

Kein Gesamtrisiko, es handelt sich lediglich um Hinweise aus der Bewertung.

### GERING

Geringes Gesamtrisiko, das keine umfangreichen Maßnahmen erfordert.

### MITTEL

Mittleres Gesamtrisiko, das mittelfristige Maßnahmen erfordert.

### HOCH

Hohes Gesamtrisiko, das kurzfristige Maßnahmen erfordert.

### KRITISCH

Kritisches Gesamtrisiko, das sofortige Maßnahmen erfordert.