Infoblatt: ISO 27001 & Pentest

Zwei Sicherheitsnachweise auf einen Blick

Worum es geht

„Unsere Software ist sicher“ – das behauptet jeder Anbieter. Ob das stimmt, zeigen prüfbare Belege. Das Schutzniveau eines Anbieters misst sich an drei Schutzzielen. Um sie glaubhaft zu belegen, braucht es zwei Nachweise, die sich ergänzen, aber nicht ersetzen.

Vertraulichkeit
Nur Befugte sehen die Daten.

Integrität
Die Daten sind unverfälscht.

Verfügbarkeit
Die Daten sind da, wenn Sie sie brauchen.

Die zwei Bausteine im Vergleich

	Baustein 1: ISO 27001	Baustein 2: Penetrationstest
Prüft	Organisation, Prozesse, Verantwortlichkeiten	Technik, konkrete Systeme, reale Angriffswege
Frage	Gibt es ein funktionierendes System für Sicherheit?	Hält die Umsetzung einem echten Angriff stand?
Prüfer	Akkreditierte Zertifizierungsstelle	Spezialisierter Sicherheitsdienstleister
Rhythmus	Zertifikat 3 Jahre, jährliche Überwachungsaudits	Anlassbezogen und regelmäßig
Blinder Fleck ohne den anderen	Gute Prozesse, ungeprüfte Technik	Geprüfte Technik, keine Struktur dahinter

Baustein 1: ISO 27001

Was das Zertifikat belegt

- ✓ Informationssicherheit wird **systematisch** betrieben: Risiken erfassen, Maßnahmen ableiten, Wirksamkeit messen
- ✓ Sicherheit hängt an **Prozessen**, nicht an einer einzelnen Person

Was es nicht belegt

- × Dass eine konkrete Anwendung **technisch angriffsfest** ist
- × Ein ISMS beschreibt, wie geprüft wird – es **ersetzt die Prüfung nicht**

Talent2Go

Infoblatt: ISO 27001 & Pentest

Zwei Sicherheitsnachweise auf einen Blick

ISO 27001: Darauf sollten Sie achten

1. **Zertifiziert oder „orientiert an“?** Formulierungen wie „wir arbeiten nach ISO 27001“ bedeuten: keine Zertifizierung.
2. **Geltungsbereich (Scope):** Zertifikat als PDF anfordern und den Abschnitt „Scope“ selbst lesen – deckt er die Software ab, die Ihre Azubis nutzen?
3. **Rechenzentrum:** Auch das Hosting sollte zertifiziert und der Serverstandort geklärt sein.

Baustein 2: Penetrationstest

Der Begriff „Penetrationstest“ ist nicht geschützt. Auch ein automatisierter Schwachstellenscan wird manchmal so verkauft. Der Unterschied entscheidet darüber, wie belastbar der Sicherheitsnachweis wirklich ist.

	Automatisierter Schwachstellenscan	Penetrationstest
Findet	Bekannte, katalogisierte Schwachstellen	Auch unbekannte Lücken und Logikfehler
Methode	Werkzeuggesteuert	Überwiegend manuell, hypothesengetrieben
Kontext	Generische Risikobewertung	Bewertung im konkreten Anwendungskontext
Aufwand	Stunden	Tage bis Wochen
Ergebnis	Toolreport	Bericht mit Nachweisen, Einordnung, Empfehlungen

Achtung: Einen vollständigen Pentestbericht bekommen Sie nicht – und sollten Sie auch nicht. Erwarten dürfen Sie eine Zusammenfassung oder Bestätigung: wer wann getestet hat, in welchem Umfang und ob nachgeprüft wurde.

Die passenden Fragen fürs Auswahlgespräch finden Sie in unserer Checkliste „Sicherheitsfragen für Ihren Ausbildungssoftware-Anbieter“. →

Infoblatt: ISO 27001 & Pentest

Zwei Sicherheitsnachweise auf einen Blick

Diese Unterlagen sollten Sie anfordern

Nachweis	Zuständig / bis wann	☑
ISO-27001-Zertifikat **inklusive Geltungsbereich** (als PDF)		☐
Entwurf des AVV nach Art. 28 DSGVO		☐
TOM-Übersicht mit mindestens drei benannten Maßnahmen		☐
Pentest-Bestätigung: Prüfer, Zeitpunkt, Umfang, Retest		☐
Angaben zu Rechenzentrum, Serverstandort und Unternehmenssitz		☐

Glossar

ISMS
Informationssicherheits-Managementsystem: der Rahmen, mit dem ein Unternehmen Risiken erkennt, Maßnahmen festlegt und deren Wirksamkeit prüft.

TOM
Technisch-organisatorische Maßnahmen, z. B. Zugangs- und Zugriffskontrolle, Verfügbarkeitskontrolle (Backups, Notfallpläne) und Protokollierung.

AVV
Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Pflicht, sobald ein Anbieter personenbezogene Daten für Sie verarbeitet.

Scope
Geltungsbereich eines Zertifikats: welche Unternehmensteile und Leistungen tatsächlich zertifiziert sind.

Retest
Nachprüfung nach einem Penetrationstest. Erst sie belegt, dass gefundene Lücken wirklich geschlossen wurden.

SOC 2
In den USA verbreiteter, wiederkehrender Prüfbericht eines Wirtschaftsprüfers – kein Zertifikat mit fester Laufzeit.

Ausbildung digital – und sicher

Talent2Go ist ISO-27001-zertifiziert, wird in Deutschland gehostet und regelmäßig extern auf IT-Sicherheit geprüft.

Jetzt Demo vereinbaren →

