Übersicht: Typische Praxisfallen bei TOMs

Praxisfalle	Warum das problematisch ist	Das können Sie tun
Berechtigungen wachsen über Jahre unkontrolliert an.	Beschäftigte sammeln im Laufe der Zeit häufig immer mehr Zugriffsrechte an. Alte Berechtigungen bleiben bestehen und werden selten hinterfragt.	Prüfen Sie regelmässig bestehende Berechtigungen und lassen Sie nicht mehr benötigte Zugriffe entfernen.
Gemeinsam genutzte Accounts	Werden Benutzerkonten gemeinsam verwendet, lässt sich häufig nicht mehr nachvollziehen, wer tatsächlich auf Daten zugegriffen hat.	Setzen Sie sich für die Nutzung personenbezogener Benutzerkonten ein und hinterfragen Sie Sammelaccounts kritisch.
Löschkonzepte existieren nur auf dem Papier.	Häufig sind zwar Löschfristen definiert, technisch oder organisatorisch werden diese jedoch nicht zuverlässig umgesetzt.	Lassen Sie sich die praktische Umsetzung von Löschprozessen regelmässig nachweisen.
Homeoffice-Regeln werden im Alltag umgangen.	Beschäftigte nutzen private Geräte, unsichere Netzwerke oder speichern Daten lokal ab, um Arbeitsabläufe zu vereinfachen.	Überprüfen Sie, ob die Vorgaben für Homeoffice tatsächlich eingehalten werden, und sensibilisieren Sie die Beschäftigten regelmässig.
Schatten-IT bleibt lange unbemerkt.	Private Cloudspeicher, Messenger oder externe Tools werden häufig genutzt, ohne dass Datenschutz oder IT hiervon wissen.	Fragen Sie regelmässig nach neu eingesetzten Tools und stimmen Sie sich eng mit der IT-Abteilung ab.
KI-Systeme werden spontan genutzt.	Inhalte werden schnell in KI-Tools kopiert, ohne dass klar ist, welche Daten dort bearbeitet oder gespeichert werden.	Prüfen Sie den Einsatz von KI-Anwendungen und etablieren Sie klare Nutzungsregeln.
Datenschutzvorfälle werden zu spät gemeldet.	Beschäftigte erkennen Vorfälle oft nicht oder wissen nicht, an wen sie sich wenden müssen.	Kontrollieren Sie, ob Meldewege bekannt sind, und führen Sie regelmässige Sensibilisierungsmassnahmen durch.
Dienstleister werden nach Vertragsabschluss kaum noch geprüft.	Veränderungen bei Unterauftragnehmern, KI-Funktionen oder Datenflüssen bleiben dadurch häufig unbemerkt.	Überprüfen Sie Auftragsbearbeiter regelmässig und fordern Sie aktuelle Informationen zu deren TOMs sowie vorhandene Zertifizierungen (z. B. TISAX oder ISO 27001) an.
Administratorrechte werden zu grosszügig vergeben.	Dauerhafte oder unnötige Adminrechte erhöhen das Risiko interner Fehlhandlungen erheblich.	Fragen Sie nach dem Berechtigungskonzept und prüfen Sie, ob Administratorrechte auf das notwendige Mass beschränkt sind.
TOM-Dokumente werden jahrelang nicht aktualisiert.	Prozesse, Software und Arbeitsweisen verändern sich deutlich schneller als bestehende Dokumentationen.	Kontrollieren Sie regelmässig, ob die TOM-Dokumentation noch den tatsächlichen Verhältnissen und dem Stand der Technik entspricht.
Offboarding-Prozesse werden nicht konsequent umgesetzt.	Beim Ausscheiden von Beschäftigten bleiben Zugänge und Berechtigungen teilweise länger aktiv als erforderlich. Dadurch entstehen vermeidbare Sicherheitsrisiken.	Prüfen Sie stichprobenartig, ob Zugänge nach dem Ausscheiden tatsächlich deaktiviert und Berechtigungen vollständig entzogen werden.
Sicherheitsupdates werden zu spät eingespielt.	Veraltete oder ungepatchte Systeme zählen zu den häufigsten Einfallstoren für Cyberangriffe. Sicherheitslücken sind Angreifern oft bereits bekannt.	Lassen Sie sich Patch- und Updateprozesse erläutern und überprüfen Sie regelmässig, ob Sicherheitsupdates zeitnah umgesetzt werden.
Neue Software wird eingeführt, ohne die TOMs anzupassen.	Prozesse, Datenflüsse und Risiken verändern sich häufig durch neue Anwendungen oder Funktionen. Die TOM-Dokumentation bildet diese Änderungen jedoch oft nicht mehr ab.	Kontrollieren Sie, ob bei technischen oder organisatorischen Änderungen auch die TOMs und die übrige Datenschutzdokumentation aktualisiert werden.