BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Datenlecks & Schatten-IT

Die meisten Datenlecks 2026 stammen nicht aus Hacker-Angriffen, sondern aus offen konfigurierten Cloud-Speichern, vergessenen SaaS-Trials und ChatGPT-Eingaben. Wir zeigen, wie Schatten-IT erkannt und kanalisiert wird.

min Lesezeit: 7 min **Aktualisiert:** 14. März 2026 **Risiko:** Hohes Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/data-leaks-shadow-it

Was sind Datenlecks durch Schatten-IT?

Schatten-IT bezeichnet alle Hard- und Software-Lösungen, die Mitarbeitende ohne Wissen oder Genehmigung der IT-Abteilung im Unternehmenskontext einsetzen. Dazu zählen private Dropbox-Accounts, die für die Dateiübertragung genutzt werden, ungenehmigte SaaS-Abonnements (Trello, Notion, Monday.com), KI-Assistenten (ChatGPT, Copilot in der freien Version) und App-Downloads auf Firmengeräten.

Das grundlegende Problem ist nicht Böswilligkeit, sondern eine Lücke zwischen Bedarf und IT-Angebot: Wenn genehmigte Tools zu langsam, zu teuer oder zu umständlich sind, greifen Mitarbeitende zu dem, was funktioniert. Das Ergebnis ist eine unkontrollierte Ausbreitung von Unternehmensdaten auf externe Dienste, die nicht geprüft, nicht verschlüsselt und nicht im Datenschutzregister erfasst sind.

Datenlecks entstehen in diesem Kontext häufig nicht durch Angreifer, sondern durch Fehlkonfiguration: Ein S3-Bucket, der auf "öffentlich" gestellt wird; ein Notion-Dokument, das versehentlich per Link teilbar ist; interne Strategiepapiere, die als ChatGPT-Prompt eingegeben werden. Diese Lecks sind oft wochenlang offen, bevor jemand sie bemerkt.

Auf einen Blick

01

Fehlkonfiguration überholt Hacking

Öffentlich zugängliche Cloud-Speicher und falsch konfigurierte Sharing-Einstellungen verursachen mehr Datenlecks als aktive Angriffe. Die Gefahr kommt von innen.

02

KI-Chatbots als Datenschutz-Risiko

Inhalte, die in kommerzielle KI-Assistenten eingegeben werden, können für Trainings-Zwecke genutzt werden. Interne Kalkulationen, Kundendaten oder Quellcode gehören nicht in öffentliche KI-Dienste.

03

Schatten-IT ist ein Symptom, kein Problem

Wo Schatten-IT wächst, fehlt ein geeignetes genehmigtes Werkzeug. IT-Sicherheit, die nur verbietet, ohne Alternativen zu bieten, verschiebt das Problem, löst es aber nicht.

Woran erkennen Sie Schatten-IT und Datenlecks?

Öffentlich zugängliche Object-Storage-Buckets
S3-, Azure-Blob- oder GCS-Buckets mit unsicherer Konfiguration, die bei einer einfachen Internet-Suche gefunden werden können.

Mitarbeiter-Accounts mit privater E-Mail
SaaS-Dienste, die unter privater E-Mail-Adresse registriert und für dienstliche Daten genutzt werden - außerhalb jeder IT-Governance.

KI-Chatbot-Eingabe interner Dokumente
Mitarbeitende kopieren Vertragsentwürfe, Finanzdaten oder Kundendaten in ChatGPT, Gemini oder ähnliche Dienste, um Texte zu verbessern oder Fragen zu stellen.

Vergessene Test-Domains und Demo-Umgebungen
Subdomains oder Staging-Umgebungen, die für Tests eingerichtet, aber nie geschlossen wurden und Unternehmensdaten enthalten.

Ungenehmigte Browser-Extensions
Produktivitäts-Extensions, die Tastatureingaben oder Seiteninhalt lesen, können Zugangsdaten oder sensible Seiteninhalte exfiltrieren.

Dateifreigabe über Consumer-Cloud
"Ich habe es kurz auf Dropbox geteilt" oder "der Link läuft in 7 Tagen ab" - aber wer hat noch Zugriff, und wo ist die Datei jetzt gespeichert?

So schützen Sie sich

Für Mitarbeitende

- **Genehmigte Tools nutzen** und IT-Abteilung aktiv fragen, wenn keine passende Lösung existiert - statt selbst eine zu suchen.
- **Keine internen Daten in öffentliche KI-Dienste eingeben:** Kundennamen, Vertragsdetails, Finanzdaten und Quellcode haben nichts in kommerziellen Chatbots zu suchen.
- **Sharing-Einstellungen bewusst wählen:** Bevor ein Link geteilt wird, prüfen: Ist er wirklich nur für die gewünschte Person zugänglich? Oder für "jeden mit Link"?
- **Ungenehmigte Apps und Extensions melden**, nicht einfach installieren. IT kann Bedarf evaluieren und sichere Alternativen bereitstellen.

Für Administratoren

- **Shadow-IT-Discovery:** CASB (Cloud Access Security Broker) oder Proxy-Logs auswerten, um nicht genehmigte SaaS-Dienste zu identifizieren.
- **Cloud-Konfigurationsaudits:** S3, Azure und GCP regelmäßig auf öffentlich zugängliche Ressourcen scannen (Tools: Prowler, ScoutSuite, Cloudmapper).
- **Approved SaaS-Katalog:** Eine gepflegte Liste genehmigter Werkzeuge senkt den Anreiz für Schatten-IT erheblich.
- **KI-Nutzungsrichtlinie** für ChatGPT, Copilot und Co.: Welche Datenklassen dürfen in welchen KI-Diensten genutzt werden? Unternehmens-Instanzen (Azure OpenAI, Microsoft 365 Copilot mit Datenschutzvertrag) sind Consumer-Versionen vorzuziehen.
- **DLP-Regeln** für bekannte Datei-Sharing-Sites und KI-Dienste konfigurieren - Uploads sensibler Daten blockieren oder alarmen.

Echte Beispiele

FALL 01 · SOFTWAREUNTERNEHMEN · DE · Q4/2025

Ein Entwickler konfigurierte einen S3-Bucket für interne Deployment-Artefakte und setzte die Berechtigung versehentlich auf öffentlich - eine verbreitete Fehlkonfiguration. Der Bucket enthielt Environment-Variablen, darunter Datenbankpasswörter und API-Schlüssel. Ein automatisierter Scanner fand ihn innerhalb von Stunden.

Schaden: Datenbank kompromittiert, Kundendaten abgeflossen · **Erkennung:** Bug-Bounty-Meldung drei Tage nach Fehlkonfiguration · **Lehre:** Bucket-Policies als Infrastructure-as-Code mit Pflicht-Review; Cloud-Security-Posture-Management (CSPM) hätte sofort alarmiert.

FALL 02 · UNTERNEHMENSBERATUNG · CH · Q1/2026

Mehrere Berater nutzten ChatGPT (kostenlose Version), um Kundenpräsentationen zu optimieren. Dabei wurden Kundennamen, Umsatzzahlen und strategische Empfehlungen als Kontext eingegeben. Die Daten lagen damit in OpenAIs Trainings-Pipeline.

Schaden: Datenschutzverletzung (nach DSG meldepflichtig), Vertragsrisiken gegenüber Kunden · **Erkennung:** Interne Compliance-Prüfung · **Lehre:** KI-Richtlinie fehlte. Microsoft 365 Copilot mit Unternehmens-Datenschutzvertrag wäre die korrekte Alternative gewesen.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Zugang sofort schließen:** Öffentlichen Bucket auf privat setzen, Sharing-Link deaktivieren, SaaS-Zugang widerrufen.
2. **Umfang ermitteln:** Welche Daten waren betroffen? Seit wann war der Zugang offen? (Access-Logs auswerten)
3. **DSGVO/DSG-Meldepflicht prüfen:** Bei personenbezogenen Daten ggf. 72-Stunden-Meldefrist für Aufsichtsbehörden.
4. **Betroffene Personen und Kunden informieren**, wenn deren Daten kompromittiert wurden - frühzeitig und transparent.
5. **IT-Security und Compliance einbinden** - nicht alleine handeln, um Eskalation nicht zu verzögern.
6. **Forensische Analyse:** Wurden die Daten tatsächlich abgerufen? Access-Logs, CDN-Logs und Monitoring prüfen.

Häufige Fragen

Darf ich ChatGPT für die Arbeit nutzen?

Das hängt von der Unternehmensrichtlinie und der Datensensitivität ab. Öffentliche Versionen ohne Datenschutzvertrag sind für interne, vertrauliche oder personenbezogene Daten nicht geeignet. Unternehmens-Versionen (Azure OpenAI, Microsoft 365 Copilot) mit entsprechenden Verträgen sind datenschutzrechtlich zulässiger.

Was ist ein CASB und brauchen wir das?

Ein Cloud Access Security Broker sitzt zwischen Nutzer und Cloud-Diensten und setzt Richtlinien durch: welche SaaS-Dienste erlaubt sind, welche Daten hochgeladen werden dürfen. Für Unternehmen ab ca. 50 Mitarbeitenden mit ausgeprägter SaaS-Nutzung lohnt es sich zu evaluieren.

Wie erkenne ich, welche Schatten-IT meine Mitarbeitenden nutzen?

DNS-Logs und Proxy-Daten geben Hinweise auf nicht genehmigte Dienste. Alternativ liefern CASB-Lösungen und Shadow-IT-Discovery-Features in modernen SASE-Plattformen strukturierte Übersichten.

Sind vergessene SaaS-Trials ein echtes Risiko?

Ja - besonders wenn sie mit Unternehmens-Daten gefüllt wurden und dann nicht mehr aktiv überwacht werden. Daten in einem vergessenen Trial-Account können jahrelang gespeichert bleiben und sind nicht mehr in der Kontrolle des Unternehmens.

Weitere Themen

Schatten-IT und unkontrollierte Datenweitergabe überschneiden sich stark mit Insider Threats und schwachen Zugangsdaten. Wer diese drei Bereiche zusammen adressiert, deckt einen Grossteil der nicht-technischen Angriffsfläche ab.