BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Insider Threats - wenn das Risiko schon drin ist

Nicht jeder Insider ist böswillig - die meisten Insider-Vorfälle sind Fahrlässigkeit. Wir unterscheiden absichtliche, fahrlässige und kompromittierte Insider und zeigen, wie kulturelle und technische Maßnahmen ineinandergreifen.

min Lesezeit: 7 min **Aktualisiert:** 14. März 2026 **Risiko:** Mittleres Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/insider-threats

Was sind Insider Threats?

Insider Threats entstehen durch Personen, die legitimen Zugang zu Systemen, Daten oder Gebäuden haben - und diesen Zugang bewusst oder unbewusst missbräuchlich nutzen. Der Begriff umfasst drei grundlegend verschiedene Profile:

Absichtliche Insider handeln böswillig: Sie stehlen Kundendaten vor dem Wechsel zum Mitbewerber, sabotieren Systeme aus Frustration oder verkaufen Zugangsdaten an externe Angreifer. Diese Fälle sind spektakulär, aber vergleichsweise selten.

Fahrlässige Insider sind statistisch häufiger: Mitarbeitende, die sensible Daten per E-Mail an die falsche Adresse schicken, einen USB-Stick verlieren, Schatten-IT-Dienste ohne Prüfung nutzen oder auf eine Phishing-Mail hereinfallen. Böse Absicht gibt es keine - aber der Schaden ist real.

Kompromittierte Insider wissen oft gar nicht, dass sie zum Werkzeug geworden sind: Ihre Zugangsdaten wurden gestohlen, ihr Gerät mit Malware infiziert, oder sie wurden durch Social Engineering zur Mitarbeit bewegt.

Auf einen Blick

01

Fahrlässigkeit überwiegt

In den meisten Insider-Vorfällen gibt es keine kriminelle Absicht. Mangelnde Schulung, Prozesslücken und Zeitdruck sind häufigere Ursachen als Böswilligkeit.

02

Insider umgehen technische Perimeter

Ein Mitarbeiter, der Daten legal herunterladen darf, löst keine Alarm-Regeln aus - selbst wenn er sie kurz vor seiner Kündigung massenweise kopiert.

03

Frühe Indikatoren sind oft kulturell

Ungewöhnliches Verhalten, soziale Rückzug, geäußerte Frustration oder auffällige Loyalitätsbrüche kündigen Insider-Vorfälle oft Wochen vorher an.

Woran erkennen Sie Insider Threats?

Ungewöhnlicher Datendownload
Massenhafte Downloads von Kundendaten, Vertragsdokumenten oder IP-Daten - besonders außerhalb der Arbeitszeiten oder kurz vor Kündigung/Austritt.

Zugriff außerhalb der eigenen Rolle
Ein Vertriebsmitarbeiter greift auf Entwicklungs-Repositories zu; eine Hilfskraft öffnet HR-Akten. Ungewöhnliche Zugangsmuster sind frühe Warnsignale.

Neue Privilegien-Eskalationen
Accounts, die sich plötzlich höhere Rechte verschaffen oder Access-Requests außerhalb normaler Prozesse stellen.

"Abdecken" unter Kollegen
Andere Mitarbeitende helfen jemandem, sein Verhalten zu erklären oder zu verbergen - kann auf bewusste Komplizenschaft oder auf sozialen Druck hinweisen.

Abrupte Loyalitätsbrüche
Plötzliche negative Haltung gegenüber dem Unternehmen, Erwähnung von Mitbewerber-Angeboten, auffällig neues Interesse an sensiblen Bereichen.

USB-Nutzung auf gesperrten Systemen
Versuche, Daten über nicht autorisierte Wege (USB, persönliche Cloud-Accounts, Screenshot) nach außen zu bringen.

So schützen Sie sich

Für Mitarbeitende

- **Ungewöhnliches Verhalten melden** - auch wenn es ein geschätzter Kollege ist. "Speak up"-Kanäle existieren für genau solche Situationen.
- **Keine Zugangsdaten teilen,** auch nicht innerhalb des Teams. Jeder Mitarbeitende sollte sein eigenes Konto verwenden.
- **Daten nur für legitime Zwecke verwenden:** Kunden- oder Produktdaten nach dem Ende eines Projekts oder bei Austritt zurückgeben, nicht mitnehmen.
- **Schatten-IT-Dienste melden,** statt einfach zu nutzen. IT-Abteilungen können oft schnelle Lösungen anbieten, wenn die Anforderung bekannt ist.

Für Administratoren

- **Least-Privilege-Prinzip konsequent umsetzen:** Zugriffsrechte auf das für die Rolle notwendige Minimum beschränken, regelmäßige Rezertifizierung.
- **Offboarding-Prozess schärfen:** Zugänge am letzten Arbeitstag (nicht erst danach) sperren, Equipment zurückgeben, Cloud-Konten deaktivieren.
- **User and Entity Behaviour Analytics (UEBA)** einsetzen, um Abweichungen von Baselines zu erkennen (Massendownload, Nacht-Zugriff, ungewöhnliche Geräte).
- **DLP (Data Loss Prevention):** Regeln für den Abfluss sensibler Daten über E-Mail, USB und Cloud-Uploads konfigurieren.
- **Hinweisgebersystem etablieren:** Niedrigschwelliger, anonymer Meldekanal für Kollegenverhalten - konform mit Hinweisgeberschutzgesetz (DE: HinSchG, CH: Obligationenrecht Art. 321a).

Echte Beispiele

FALL 01 · SOFTWAREUNTERNEHMEN · DE · Q2/2025

Ein Entwickler, der sich übergangen bei einer Beförderungsentscheidung fühlte, kopierte in seinen letzten zwei Arbeitswochen systematisch Source-Code und Kundenkonfigurationen auf einen privaten Cloud-Speicher. Er wechselte zur Konkurrenz und nutzte das Material für ein konkurrierendes Produkt.

Schaden: Verlust von Geschäftsgeheimnissen, Rechtsstreit · **Erkennung:** UEBA-Alert auf Massendownload drei Tage nach Kündigung · **Lehre:** DLP-Regeln und UEBA hätten die Datenexfiltration stoppen können, bevor sie abgeschlossen war.

FALL 02 · KLINIK · CH · Q4/2025

Eine Verwaltungsangestellte nutzte über Monate hinweg die Patientendaten-Zugriffe einer pensionierten Kollegin, deren Account versehentlich aktiv geblieben war. Sie verkaufte Patientenprofile an eine Marketingfirma.

Schaden: Verletzung des Arztgeheimnisses, Bußgeld, Patientenklage · **Erkennung:** Audit-Log-Analyse durch externen Prüfer · **Lehre:** Offboarding-Prozess hätte den Account spätestens am letzten Arbeitstag deaktiviert. Access-Reviews wären ein weiteres Sicherheitsnetz gewesen.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Zugänge des betroffenen Accounts sofort sperren** - nicht nach Rücksprache abwarten, sofort handeln.
2. **Keine Konfrontation ohne HR und Rechtsabteilung:** Insider-Vorfälle haben arbeitsrechtliche Konsequenzen, die falsches Vorgehen teuer machen können.
3. **Forensische Sicherung** vor Gerätezugriff: Log-Daten, Event-Logs und Speicherinhalte sichern, bevor das Gerät gereinigt wird.
4. **Umfang des Datenzugriffs ermitteln:** Was wurde heruntergeladen, wann, und wohin? Diese Information entscheidet über Meldepflichten.
5. **DSGVO/DSG-Meldepflicht prüfen:** Bei Datenschutzverletzungen ggf. Meldung an Aufsichtsbehörde innerhalb von 72 Stunden erforderlich.
6. **Strafanzeige prüfen** (besonders bei absichtlichem Diebstahl von Geschäftsgeheimnissen).

Häufige Fragen

Ist die Überwachung von Mitarbeitenden legal?

In Grenzen und mit Einschränkungen. In DE gilt das Bundesdatenschutzgesetz und der Betriebsrat hat Mitbestimmungsrechte. In CH gilt das DSG. Verhaltensbasierte Anomalie-Erkennung (UEBA) ist datenschutzrechtlich anders zu bewerten als lückenlose Tastaturüberwachung. Eine Betriebsvereinbarung / Personalreglement sollte die Grundlage bilden.

Was ist der Unterschied zwischen absichtlichem und fahrlässigem Insider?

Absichtlich: bewusste Schädigungsabsicht oder Eigennutz. Fahrlässig: Unaufmerksamkeit, Prozessumgehung aus Bequemlichkeit, schlechtes Urteil ohne böse Absicht. Rechtlich und im Umgang miteinander macht das einen erheblichen Unterschied - die technischen Maßnahmen überlappen sich aber stark.

Wie verhindere ich Insider Threats in kleinen Teams?

Durch Prozesse (4-Augen-Prinzip, Zugriffsminimierung, Offboarding-Checklisten) und Kultur (offene Kommunikation, psychologische Sicherheit). Technik allein greift in kleinen Unternehmen selten - Vertrauen und klare Erwartungen sind wichtiger.

Weitere Themen

Insider Threats überschneiden sich mit Ransomware (kompromittierte Insider als Einstiegspunkt), Datenlecks durch Schatten-IT und Social Engineering (externer Akteur nutzt internen Mitarbeiter als Werkzeug).