Insider Bedrohung - Datenabfluss

Shape the future with confidence

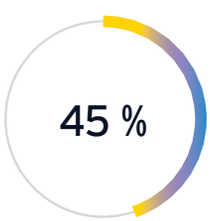
The better the question. The better the answer. The better the world works.

Studien zeigen, dass Mitarbeitende, besonders beim Unternehmensaustritt, immer häufiger sensible Unternehmensdaten stehlen. Diese Daten können sensible Informationen, wie Kundendaten, oder Geschäftsgeheimnisse, umfassen und somit ein hohes Unternehmensrisiko darstellen. Gerne unterstützen wir Sie durch gezielte IT-forensische Analysen, um potenziellen Datenabfluss zu identifizieren.

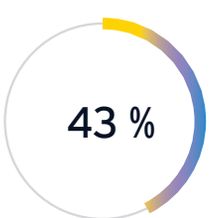
Der Austritt von Mitarbeitenden aus dem Unternehmen stellt nicht nur eine organisatorische Herausforderung im Rahmen des Off-Boarding-Prozesses dar, sondern kann auch ein erhebliches Unternehmensrisiko beinhalten. Mitarbeitende in einem gekündigten Dienstverhältnis können verleitet sein, vertrauliche Unternehmensinformationen, wie etwa Kundendaten, Geschäftsgeheimnisse, Finanzdaten oder interne E-Mails vor dem Verlassen des Unternehmens über diverse Kanäle zu exfiltrieren. Ob beabsichtigt oder unbeabsichtigt, das Exfiltrieren von Daten durch Mitarbeitende beim Verlassen des Unternehmens kann schwerwiegende finanzielle und rechtliche Folgen nach sich ziehen.

Unternehmen vertrauen darauf, dass Mitarbeitende die Interessen des Unternehmens wahren. Diese können jedoch mit oder ohne Vorsatz vertrauliche Unternehmensdaten vor dem Austritt exfiltrieren. Die Motive hierfür reichen von mangelndem Bewusstsein über persönliche Rechtfertigung bis hin zur Vergeltungsmaßnahme. Im Speziellen haben Mitarbeitende in leitenden Positionen oder mit administrativen Zugriffsrechten häufig Zugang zu sensiblen Informationen.

EY unterstützt Sie mit ausgewählten und zielgerichteten IT-forensischen Analysen, um potenziellen Datenabfluss zu identifizieren und diesen gerichtsfest aufzuarbeiten. Art und Umfang unserer Analysen stimmen wir im individuell mit Ihnen ab.



Laut branchenübergreifenden Untersuchungen nehmen 45 % der ausscheidenden Mitarbeitenden Unternehmensdaten mit – darunter auch sensible Unternehmensinformationen, geistiges Eigentum oder Geschäftsgeheimnisse.



Datenabfluss über E-Mails, die an private Adressen gesendet werden, sind mit 43 % die häufigste Variante des Datenabflusses.

Ihre Vorteile auf einen Blick

Unser lokales und erfahrenes IT-Forensik-Team greift auf eine bewährte Untersuchungsmethodologie für die Analyse von Datenabfluss zurück. Dadurch decken wir Datenexfiltrationen zeitnah auf, wodurch Sie das Risiko und potenziellen Schaden bestmöglich minimieren.

Im Rahmen IT-forensischen Analysen bieten wir Ihnen die nachfolgenden Mehrwerte:

- Identifikation von Datenexfiltration zum Schutz von Unternehmensdaten
- Gerichtsfeste IT-forensische Analyse inklusive Berichtserstellung
- Aktive Risikomanagement-Maßnahme im Rahmen des Off-Boarding Prozesses

1.

Basis Quick-Check

Beinhaltet:

- Durchführung von IT-forensischen Sicherungen
- Teilautomatisierte Analyse von Microsoft 365, E-Mail- und Cloud-Logdateien
- Erstellung eines gerichtsfesten IT-Forensik Berichts

2.

Erweiterter Quick-Check

Beinhaltet:

- Durchführung von IT-forensischen Sicherungen
- Teilautomatisierte Analyse von Microsoft 365, E-Mail-, Cloud-Logdateien sowie eines Laptops und externer Speichermedien
- Überprüfung des Versands von Dateien an privat genutzte E-Mailaccounts
- Feststellung von Datentransfer über Cloud-Dienste oder Datenübertragungs-software
- Erstellung eines gerichtsfesten IT-Forensik Berichts

3.

Umfassende IT-Forensische Analyse

Beinhaltet:

- Durchführung von IT-forensischen Sicherungen
- Ausführliche Analyse von Microsoft 365, Cloud-Logdateien sowie eines/mehrerer Laptops und externer Speichermedien
- IT-forensische Untersuchung von mobilen Endgeräten
- Überprüfung des Versands von Dateien an privat genutzte E-Mailaccounts
- Feststellung von Datentransfer über Cloud-Dienste oder Datenübertragungssoftware
- Erstellung eines gerichtsfesten IT-Forensik Berichts

Unsere laufenden oder anlassbezogenen standardisierten IT-forensischen Analysen für eine oder mehrerer Mitarbeitende stellen eine wertvolle Ergänzung Ihres Off-Boarding-Prozesses dar. Wir stimmen unsere Vorgehen auf Ihre technischen Gegebenheiten ab, um Datenabfluss kosteneffizient und trotzdem möglichst vollumfänglich zu identifizieren.

> Wir unterstützen Sie dabei, sich aktiv vor den zunehmenden Insider Bedrohungen und deren potenziellen Auswirkungen auf Ihre Geschäftsgeheimnisse, Kundendaten und Ihren Ruf zu schützen.

Ihre Ansprechpartner

Anton Moser
Director Cyberforensik
+43 664 6000 31158
anton.moser@at.ey.com

Robert Pölzelbauer
Senior Manager Cyberforensik
Allgemein beeideter und gerichtlich zertifizierter Sachverständiger
+43 664 60003 1124
robert.poelzelbauer@at.ey.com

EY | Building a better working world

© 2026 Ernst & Young Wirtschaftsprüfungsgesellschaft m.b.H.
All Rights Reserved. ELA 2604-000 | ED None

ey.com/at