Impersonation Fraud erkennen und vorbeugen

Best Practices für Prävention und Abwehr

CEO-Fraud, Impersonation Fraud, Geschäftsführertrick, Business-E-Mail-Compromise – der digitale Betrug von Unternehmen auf Basis falscher Identitäten hat viele Namen. Gemeint ist in der Regel immer das Gleiche: die Manipulation von Mitarbeitenden, um diese zur Überweisung hoher Geldsummen zu bewegen.

Alleine in den Vereinigten Staaten wurde 2021 ein Schaden i.H.v. 2,4 Milliarden US-Dollar durch dieses Betrugsmuster verursacht.[1]

Auch in Deutschland stellt Impersonation Fraud für Unternehmen eine große Herausforderung dar. Doch Unternehmen sind dieser besonders heimtückischen Betrugsart nicht schutzlos ausgeliefert – es gibt Mittel und Wege, um Versuche frühzeitig zu erkennen oder mittels präventiver Maßnahmen schon von Beginn an im Keim zu ersticken.

1 FBI IC3 Internet Crime Report 2021

pwc

In welchen Formen tritt Impersonation Fraud häufig auf?

Methode 1
CEO-Fraud

1. Täter:innen **kontaktieren Mitarbeitende** und geben sich als **hochrangige Führungskräfte** des Unternehmens aus.
2. Die Täter:innen verlangen unter absoluter **Vertraulichkeit** eine **dringende Überweisung von Geldern** und erhöhen durch vermeintliche Zeitknappheit oder rechtliche Konsequenzen den **Druck auf die Zielperson.**
3. **Die Zielperson veranlasst die Überweisung** des Geldes auf ein von den Täter:innen kontrolliertes Konto, welches dann umgehend auf weitere Konten im Ausland umgeleitet wird.

Methode 2
Payment Diversion

1. Täter:innen **kontaktieren Mitarbeitende** und geben sich als **Angestellte eines Lieferanten** aus.
2. Die Täter:innen informieren die Angestellten über **eine Änderung der Bankverbindung,** die das Unternehmen für die Bezahlung von Dienstleistungen oder Materialien nutzt. Sie bitten darum, die nächsten **Zahlungen auf das neue Konto** zu überweisen.
3. Das Unternehmen **bemerkt den Betrug** erst, wenn sich die tatsächlichen Lieferanten über **nicht bezahlte Rechnungen** beschweren.

Methode 3
Security Breach Scam

1. **Die Täter:innen** kontaktieren Mitarbeitende und geben sich als **IT-Spezialist:innen** aus.
2. Die Täter:innen informieren über eine **Sicherheitsverletzung im System** des Unternehmens.
3. Die Täter:innen fordern das **Herunterladen einer Fernzugriff-Software.**
4. Mithilfe der erlangten Zugänge und Daten überweisen die Täter:innen **Geld vom Konto des Unternehmens auf ihre eigenen Konten.**

Wie können Sie Impersonation Fraud vorbeugen?

Notfallplan

Schadensfall vorbereiten - Ansprechpartner und Verantwortlichkeiten bestimmen sowie Eingrenzungsmaßnahmen definieren

Mitarbeitende

Mitarbeitende regelmäßig im Rahmen von verpflichtenden Trainings für Betrugsmuster und den Umgang mit Informationen sensibilisieren

IT-Infrastruktur

Ganzheitliches Patch-Management zur Vermeidung von Sicherheitslücken etablieren

Compliance

Internes Kontrollsystem (IKS) mit geeigneten Kontrollmechanismen etablieren, 4-Augen-Prinzip und Vertretungsregelungen implementieren

Social Media

Überlegter Umgang mit sozialen Netzwerken, insbesondere im Hinblick auf die Weitergabe von (persönlichen) Daten und Informationen

Kontakt Verifizierung

Sensibilisierung bezüglich „Social Engineering“; sorgfältige Überprüfung des Absenders durch Abgleich der Stammdaten (Stammdatenmanagement), kritisches Hinterfragen der Kontaktaufnahme und der angefragten Transaktion

Kommunikationskanäle

Alternative Kommunikationskanäle nutzen, bspw. Nutzung eines zweiten Kommunikationskanals zur Verifizierung der Transaktion

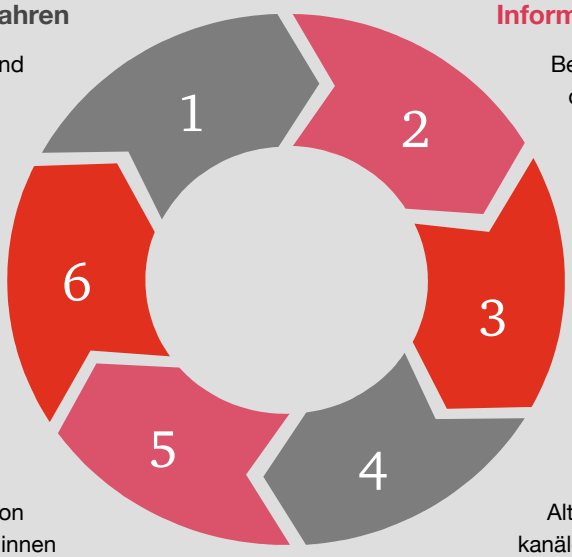
Treasury Management

Überprüfung von Vermögens-, Cash- und Liquiditätsmanagement sowie des finanziellen Risikomanagements, insbesondere bei Tochtergesellschaften

Sensible Daten

Definition von schutzwürdigen Daten und Implementierung geeigneter Schutzmaßnahmen

Wie reagieren Sie richtig auf akute Vorfälle?



Ruhe bewahren

Ruhig bleiben und nicht überstürzt handeln

Informieren

Bei Verdacht auf Betrug unverzüglich die Geschäftsleitung und involvierte Stellen wie den Compliance Officer, die Rechtsabteilung oder die Interne Revision einschalten

Unverzüglich handeln

Im Betrugsfall sofort an die Bank und die Behörden herantreten

Improvisieren

Alternative Kommunikationskanäle für Rücksprache mit bekannten Ansprechpartner:innen nutzen

Kontakt aufnehmen

Bei Verdacht auf Payment Diversion bereits bekannte Ansprechpartner:innen des Lieferanten kontaktieren

Kommunizieren

Mitarbeitenden vorwarnen und sensibilisieren

Wie können wir Sie unterstützen?

Wir unterstützen Sie in einem potentiellen Schadensfall bei der …

- Sachverhaltsaufklärung
- Gerichtsverwertbaren Sicherung und Auswertung von Beweisen unter Anwendung forensischer IT-Lösungen (eDiscovery)

Beispielsweise:

- Forensische Datenakquise – dafür kommen “Electronically Stored Information“ (ESI) wie z. B. Protokolldateien oder Betriebssystem-Artefakte in Betracht.

Digitalforensische Analyse der ESI mit folgenden Zielen:

- Ursachenanalyse
- Einschätzung der Angriffsauswirkung
- Identifizierung der Täter:innen
- Schadensquantifizierung

In zahlreichen Projekten haben wir bereits erfolgreich mit Ermittlungsbehörden und Rechtsanwält:innen zusammengearbeitet.

Wir beurteilen die Risikolage Ihres Unternehmens. Dazu führen wir mit Hilfe von Risiko Analyse, Penetration Tests, Einsatz von Red-Team-Expert:innen und Breach Indicator Assessments eine Gefährdungsanalyse Ihrer Prozesse und IT-Systeme durch. Darauf aufbauend leiten wir Empfehlungen für ein fachliches Notfallkonzept sowie eine wirksame Cyber Incident Response ab.

Wir helfen Ihnen bei der Weiterentwicklung Ihres internen Kontrollsystems, der Definition von Richtlinien, Berechtigungen und Vertretungsregelungen sowie von Prozessen zum Umgang mit dringenden Zahlungen. Gemeinsam mit Ihnen definieren wir besonders schutzwürdige Daten sowie Schutzmaßnahmen. Auch unterstützen wir Sie bei der Sensibilisierung Ihrer Mitarbeitenden, indem wir durch Schulungen und Trainings ein Bewusstsein für die Gefahren schaffen.

www.pwc.de/de/risk-regulatory.html

© 2022 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.
Alle Rechte vorbehalten. In diesem Dokument bezieht sich „PwC“ auf die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsfirma von PricewaterhouseCoopers International Limited (PwCIL) ist. Jede Mitgliedsfirma von PwCIL ist eine separate und unabhängige juristische Einheit.