



Schutz vor Wirtschaftskriminalität

Handlungsempfehlungen

Wirtschaftskriminalität entsteht häufig in Sekunden – meist durch überzeugend gefälschte Nachrichten oder manipulierte Zahlungsanweisungen. Viele Unternehmen fragen uns daher nach klaren Leitlinien, wie sie organisatorisch und technisch besser vorbeugen können. Auf Basis realer Schadenfälle und der aktuellen Anforderungen der Versicherer haben wir eine kompakte und praxiserprobte Checkliste entwickelt. Sie zeigt, welche Maßnahmen besonders wirksam sind und wie Unternehmen Abläufe so gestalten können, dass Betrugsversuche frühzeitig erkannt und verhindert werden.

Praktische Handlungsempfehlungen für Unternehmen

1. Klare Zuständigkeiten & Freigaberegeln schaffen

- Definieren Sie feste Betragsgrenzen, bis zu denen Zahlungen von Mitarbeitenden freigegeben werden dürfen, und dokumentieren Sie diese.
- Halten Sie Zuständigkeiten und Vertretungsregelungen schriftlich fest.
- Stellen Sie sicher, dass alle Mitarbeitenden diese Regeln kennen und anwenden.

2. Zahlungsprozesse absichern

- Das 4-Augen-Prinzip sollte bei allen Vermögensverfügungen verbindlich gelten.
- Bei ungewöhnlichen, dringenden oder besonders hohen Zahlungsanweisungen:
 - Rückbestätigung über einen anderen Kommunikationskanal einholen (telefonisch oder persönlich).
 - Dabei nur bekannte Telefonnummern aus internen Stammdaten verwenden, nicht aus aktuellen E-Mails.
- Bei Unsicherheiten oder Auffälligkeiten immer Rücksprache mit der zuständigen Führungskraft halten – gesundes Misstrauen ist ausdrücklich erlaubt.

Schutz vor Wirtschaftskriminalität

Handlungsempfehlungen

3. Änderungen von Bankdaten oder Lieferadressen prüfen

- Änderungen grundsätzlich im 4-Augen-Prinzip vornehmen.
- Immer eine zweite Bestätigung über einen bekannten Kommunikationsweg einholen – niemals über die „Antworten“-Funktion einer E-Mail.
- Bei Abweichungen oder ungewöhnlichen Anfragen auf Plausibilität achten und im Zweifel Rücksprache mit Vorgesetzten halten.

4. Umgang mit Anfragen von Banken und Kreditinstituten

- Vertrauliche Kundendaten nur nach Rückbestätigung durch die zuständige Führungskraft herausgeben.
- Unerwartete oder zeitkritische Anfragen kritisch hinterfragen – insbesondere, wenn Fristen gesetzt oder Druck aufgebaut wird.

5. Organisatorische & technische Schutzmaßnahmen

IT- und Datensicherheit

- Passwortregeln nach gängigen IT-Standards umsetzen: Komplexität, Länge und Einzigartigkeit der Passwörter sind wichtiger als regelmäßige Änderungen. Für jede Anwendung und jeden Nutzer sollte ein eigenes Passwort genutzt werden.
- Multifaktorauthentifizierung (MFA) für alle Fernzugriffe verpflichtend einrichten.
- Systemschutz sicherstellen: Auf allen Endgeräten und Servern aktuelle Antivirenprogramme und Firewalls einsetzen.
- Regelmäßige Backups erstellen und räumlich oder systemseitig getrennt sichern.

- Systeme aktuell halten: Sicherheitskritische Updates und Patches möglichst zeitnah einspielen und BSI-Hinweise beachten.
- Überwachung der IT-Systeme: Auf verdächtige Aktivitäten wie Intrusion Attempts oder Lateral Movement achten und entsprechende Sicherheitsmechanismen einsetzen.
- Sicherer Versand von Rechnungen per E-Mail: Interne Sicherheitsstandards überprüfen und ggf. erhöhen; insbesondere auf korrekte Verschlüsselung achten.

Awareness & Social Engineering

- Regelmäßige Schulungen zur Sensibilisierung gegenüber Social Engineering durchführen.

Umgang mit Kryptowerte

- Prüfen, ob das Unternehmen Kryptowerte verwahrt, handelt oder akzeptiert.
- Falls ja: besondere Sicherheitsmaßnahmen und interne Freigaben definieren.
- Hinweis: Schäden im Bereich Kryptowerte sind im Rahmen der VSV nicht versichert.

6. Personalprüfung (optional für Unternehmen mit besonders sensiblen Finanzbereichen)

- Vor Einstellung von Mitarbeitenden mit Finanzzugang:
 - Originale Abschlusszeugnisse prüfen
 - Referenzen einholen
 - Polizeiliches Führungszeugnis anfordern



Wir freuen uns, von Ihnen zu hören.

Wir sind für Sie da. Ob Beratung oder Fragen zu unseren Dienstleistungen – unser Team unterstützt Sie gerne bei Ihrem Anliegen.

Nehmen Sie einfach Kontakt mit uns auf und erfahren Sie, wie GGW Sie bei der Absicherung und dem Management von Risiken unterstützen kann.

Jan Kempermann

Leitung Geschäftsbereich
Wirtschaftskriminalität
Tel.: +49 40 23768090 381
Jan.Kempermann@ggw.de



Björn Albert

Geschäftsführer
GGW Kreditversicherungs-
Makler GmbH
Tel.: +49 40 328101-4730
Bjoern.Albert@ggw-kredit.de

