

Risiko-Check ACREDIA Trust^A

Wie gut ist Ihr Unternehmen gegen Wirtschaftskriminalität, wie zum Beispiel Betrug, Diebstahl und eCrime, gesichert?

1 Vorschadensituation

1. Gab es in den vergangenen 5 Jahren ungeklärte Verluste und/oder sind Ihnen Umstände bekannt, die zu einem Versicherungsfall im Rahmen der Vertrauensschadenversicherung¹ führen können?
2. Gab es in den vergangenen 5 Jahren Schäden² im Sinne der Vertrauensschadenversicherung?

2 Kontrollsystem

1. Wird bei allen Mitarbeitenden (ausgenommen Ehepartner und eigene Kinder) im Geld-/Finanzbereich bei Einstellung die Strafregisterbescheinigung überprüft?
2. Bestehen klare Kompetenzregeln für die Durchführung von Zahlungsanweisungen für bestimmte Beträge und werden diese auch eingehalten/kontrolliert?
3. Unterliegt Ihr Unternehmen der gesetzlichen Prüfpflicht?
 - a. Werden die Empfehlungen der externen Wirtschaftsprüfung befolgt?
 - b. Gab es in den vergangenen 3 Jahren Beanstandungen?
4. Ist ein Lager vorhanden?
 - a. Wird der Warenbestand regelmäßig von anderen als den dafür verantwortlichen Personen geprüft (Inventurprüfung)?
5. Konsumieren Mitarbeiter im Finanzbereich mindestens zwei Wochen durchgehend Urlaub pro Jahr?

3 Zahlungsströme

1. Gilt für Vermögensverfügungen (z.B. Zahlungen, Überweisungen) das uneingeschränkte 4-Augenprinzip?
2. Sind Einzelpersonen berechtigt, Bankkonten für ein zu versicherndes Unternehmen zu eröffnen?
3. Werden ungewöhnliche Zahlungsanweisungen von Führungskräften von den angewiesenen Mitarbeitern erst nach persönlicher Rücksprache und Bestätigung durch die Führungskraft erledigt?
4. Wird bei Änderungen der Bankdaten eines Lieferanten bei diesem persönlich³ eine Rückbestätigung eingeholt, bevor die Zahlung erfolgt?
5. Wird bei Erstbestellungen eines Neukunden mit einem Auftragswert von mehr als EUR 50.000,- oder ungewöhnlichen⁴ Bestellungen eines Bestandskunden bei diesem persönlich⁵ eine Rückbestätigung eingeholt, bevor die Ware ausgeliefert wird?
6. Werden Anfragen von Kreditinstituten zu Kundendaten und klärungsbedürftigen Zahlungsvorgängen erst nach Rückbestätigung durch eine Führungskraft beantwortet?
7. Sind Buchhaltung und Kasse personell getrennt?

¹⁺² Darunter fallen insbesondere Vermögensstraftaten durch Mitarbeiter oder Dritte, Geheimnisverrat, gezielte Angriffe über das Internet oder wissentliche Pflichtverletzung.

³⁺⁵ Unter Verwendung einer öffentlich abrufbaren oder aus früheren Bestellungen bereits bekannten Telefonnummer oder E-Mail-Adresse.

⁴ Als ungewöhnlich in diesem Sinne gelten z.B. Bestellungen, bei denen die **Lieferadresse** von jener/jenen aus früheren Bestellungen **abweicht** oder die Lieferung an eine **unbekannte Betriebsstätte** des Kunden erfolgen soll; entgegen der bisherigen Geschäftspraxis eine **Abholung durch den Kunden** erfolgt; **die Bestellmenge überdurchschnittlich groß ist** (im Vergleich zur Unternehmensgröße oder früheren Bestellungen); oder die bestellte Ware nicht zum Unternehmensgegenstand des Kunden passt.

4 EDV-/IT-System

1. Gibt es Vorgaben für die Bildung von Passwörtern und werden diese entsprechend allgemeiner IT-Standards regelmäßig geändert?
2. Sind die EDV-/IT-Systeme durch regelmäßig aktualisierte Schutzprogramme sowie eine Firewall vor Virusschäden und vor unberechtigten Änderungen und Zugriffen geschützt?
3. Werden mindestens einmal wöchentlich Daten-Backups erstellt und so gesichert, dass sie bei einem Hackerangriff auf die Originaldaten voraussichtlich nicht gleichzeitig betroffen sind?
4. Werden Angriffe auf das EDV-/IT-System erkannt und protokolliert?

5 Social Engineering⁶

Werden regelmäßig Maßnahmen ergriffen, um bei Beschäftigten das Bewusstsein für Gefahren durch Social Engineering zu schärfen?

6 Mitversicherte Unternehmen

1. Möchten Sie weitere Unternehmen in den Versicherungsschutz einschließen?
2. Sind Abweichungen zu den vorher genannten Antworten zur Risikobeurteilung in einzelnen zu mitversichernden Unternehmen möglich?
3. In welchen Ländern haben Sie Betriebsstätten bzw. Tochterunternehmen und wie viele Mitarbeiter sind dort beschäftigt? ■

⁶ Beschreibt ein Verfahren, bei dem die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen ausgenutzt wird, um beispielsweise an vertrauliche Daten zu gelangen oder die Mitarbeiter zu bestimmten Aktionen zu bewegen.