

FÜR UNTERNEHMEN & SELBSTSTÄNDIGE

Wenn der Betrieb digital stillsteht.

Cyber-Risiken verstehen.
Versicherung gezielt prüfen.

Ihr kompakter Leitfaden zu KuBuS® Cyber der Continentale:
mit Risiko-Check, Beratungsvorbereitung und Notfallblatt.



Klarheit für den nächsten Schritt.

Quellen geprüft am 03.10.2026 · Kostenloser Leitfaden

01 / RISIKEN EINORDNEN

Was würde morgen fehlen?

Cyber-Risiken werden greifbar, wenn Sie sie an Ihren eigenen Abläufen prüfen. Drei Beispiele helfen beim Einstieg.

01 Aufträge sind plötzlich nicht erreichbar.

Schadsoftware verschlüsselt Daten. Termine, Rechnungen oder Produktion stocken. Entscheidend ist, wie lange Sie ohne diese Systeme arbeiten können.

02 Vertrauliche Daten geraten nach außen.

Ein fremder Zugriff oder eine fehlgeleitete Nachricht legt Kundendaten offen. Neben der technischen Klärung können Benachrichtigungen und Ansprüche Dritter folgen.

03 Eine Zahlung geht auf das falsche Konto.

Eine manipulierte Nachricht wirkt glaubwürdig. Prüfen Sie Zahlungsfreigaben und Rückrufe bei geänderten Bankdaten. Versicherungsschutz gegen Betrug ist gesondert zu klären.

Drei Antworten für Ihren Betrieb

Welcher digitale Ablauf muss zuerst wieder funktionieren?

Wie lange könnten wir ohne ihn sinnvoll weiterarbeiten?

Welche Daten wären bei einem Verlust besonders kritisch?

Ihre Antworten sind Gesprächsgrundlage, keine Risikobewertung oder Deckungszusage.

Grundlage: eigene Beispielszenarien; Continentale Produktseite und Vorteilsdarstellung. Quellen: Seite 8.

02 / LEISTUNGEN VERSTEHEN

Drei Aufgaben. Ein Schutzkonzept.

KuBuS® Cyber richtet sich an den gewerblichen Bereich. Die Bausteine werden individuell vereinbart und betreffen unterschiedliche Kosten eines versicherten Vorfalls.

SERVICE- UND KOSTENLEISTUNGEN

Die Lage klären und handlungsfähig werden.

Soforthilfe, IT-Forensik sowie vereinbarte Unterstützung bei Benachrichtigungen und Krisenkommunikation. Die Continentale beschreibt Notfall- und Krisenhilfe rund um die Uhr.

Das ist eine Versichererleistung. Die Agentur ist keine 24/7-Notfallzentrale.

EIGENSCHÄDEN

Die wirtschaftlichen Folgen im Betrieb begrenzen.

Dazu gehören im vereinbarten Umfang Datenwiederherstellung und Ertragsausfall bei einer versicherten Betriebsunterbrechung oder Beeinträchtigung.

Betriebsunterbrechung: 12 Monate Haftzeit; für die ersten 8 Stunden wird kein Ertragsausfall ersetzt.

DRITTSCHÄDEN

Mit Forderungen anderer richtig umgehen.

Bei versicherten Haftpflichtansprüchen prüft der Versicherer die Berechtigung, wehrt unbegründete Forderungen ab und stellt von berechtigten Schadenersatzpflichten frei.

Der konkrete Anspruch muss unter den Vertrag fallen. Nicht jede Forderung oder Vertragsstrafe ist versichert.

Kurzüberblick, keine vollständige Leistungsbeschreibung. AVB A2, A3 und A4; Produktseite. Quellen: Seite 8.

03 / LÜCKEN VERMEIDEN

Zusatzschutz bewusst auswählen.

Die folgenden Leistungen sind auf der Produktseite als optional aufgeführt. Entscheidend ist, was ausdrücklich vereinbart und im Versicherungsschein ausgewiesen ist.

01 Cloud und Technik

Cloud-Ausfall durch eine Sicherheitsverletzung beim direkt und entgeltlich beauftragten Anbieter; eigener Zusatzschutz für technische Probleme und IT-Hardware.

02 Erpressung

Technische und rechtliche Unterstützung. Lösegeld ist kein pauschales Leistungsversprechen; es gelten enge Bedingungen und die Zustimmung des Versicherers.

03 Betrug und Waren

Cyber-Betrug / Cyber-Diebstahl sowie Warenversand: nur die jeweils beschriebenen Tatbestände und Grenzen sind erfasst.

04 Ansprüche und Aufklärung

E-Payment, bestimmte Vertragsstrafen und Täterermittlung. Auch hier gelten eigene Voraussetzungen und Höchstbeträge.

Im Angebot vier Punkte konkret prüfen

Versicherungssumme und jährliche Höchstleistung · Selbstbeteiligungen · eigene Höchstbeträge je Zusatzleistung · Ausschlüsse und vertragliche Pflichten.

Beispiele für Grenzen

Der Grundsatz ist keine allgemeine Hardware-, Personen- oder Sachschadenversicherung. Infrastruktur-Ausfälle und weitere Fälle können ausgeschlossen sein. Auslandsstandorte und geltend gemachte Ansprüche im Ausland müssen gesondert geprüft werden.

AVB A1-3, A1-10/11, A1-17 sowie Teil C. Optionen und Grenzen sind hier nur auszugsweise dargestellt.

04 / DEN EIGENEN STAND PRÜFEN

Sicherheit braucht Nachweise.

Gehen Sie die Punkte mit Ihrer IT-Verantwortung durch. Ein Haken ersetzt keinen Nachweis. Offene Antworten gehören auf die Maßnahmenliste.

PRÜFPUNKT	JA	NEIN	OFFEN
Nutzer und Rechte Individuelle Zugänge, getrennte Admin-Nutzung, technische Passwortvorgaben.	☐	☐	☐
Schutz der Geräte Zusatzschutz für exponierte und mobile Systeme; aktueller Schutz vor Schadsoftware.	☐	☐	☐
Sicherheitsupdates Fristen: 14 Tage bei erhöhtem Risiko, sonst 30 Tage. Umgang mit bekannten Lücken klären.	☐	☐	☐
Backups und Wiederanlauf Mindestens wöchentlich; gegen gemeinsames Verändern oder Löschen schützen. Wiederherstellung mindestens jährlich prüfen und dokumentieren.	☐	☐	☐
Menschen und Abläufe Phishing üben, Zahlungen verlässlich freigeben und MFA dort einsetzen, wo es sinnvoll ist.	☐	☐	☐
Notfallkontakte Aktuelle Kontaktliste und Vertragsunterlagen auch ohne Firmen-IT verfügbar halten.	☐	☐	☐

Vertragliche Grundlage der ersten vier Punkte: AVB B3-3.1.1 a-e, Seiten 28-29. Individuelle Vereinbarungen mitprüfen.

Meine nächste Maßnahme / verantwortlich / bis wann:

Unvollständige Auswahl. Pflichtverletzungen können je nach Verschulden und Vertragsregel zur Kürzung oder Leistungsfreiheit führen.

05 / BERATUNG VORBEREITEN

Aus Antworten wird ein Angebot.

Legen Sie vorhandene Unterlagen bereit und notieren Sie offene Punkte. Kennwörter oder Zugangscodes gehören nicht in dieses Blatt.

Unterlagen für das Gespräch

- ☐ Tätigkeit, Jahresumsatz, Standorte und mitzuversichernde Unternehmen
- ☐ Wichtige Systeme, Cloud-Anbieter und betreuender IT-Dienstleister
- ☐ Dokumentation zu Updates, Backups und letztem Wiederherstellungstest
- ☐ Bestehende Versicherungen, frühere Vorfälle und bekannte Sicherheitslücken

Drei Fragen, die Ihr Angebot beantworten sollte

Welche Kosten laufen bei einem Stillstand weiter, und welcher Gewinn entfällt?

Welche Zusatzleistungen brauchen unsere Abläufe wirklich?

Welche Summe, Selbstbeteiligung und Höchstbeträge passen zum Betrieb?

Ein guter Vergleich braucht mehr als den Jahresbeitrag.

Lassen Sie sich den versicherten Umfang, die Pflichten, Ausschlüsse und Zusatzklauseln am konkreten Betrieb erklären. Halten Sie Abweichungen vom gewünschten Schutz schriftlich fest.

Notizen / offene Entscheidung:

Arbeitsblatt von TrochaS. Beitrag und Annahme hängen vom individuellen Risiko und vereinbarten Schutz ab.

06 / FÜR DEN ERNSTFALL BEREITHALTEN

Ein ruhiger Ablauf hilft.

Dieses Blatt unterstützt die erste Orientierung bei einem vermuteten IT-Sicherheitsvorfall.
Technische Schritte mit Fachleuten abstimmen.

01 Intern alarmieren.

Geschäftsführung und IT-Verantwortliche informieren. Für Absprachen einen möglichst nicht betroffenen Kommunikationsweg nutzen.

02 Versicherer früh einbeziehen.

Schaden unverzüglich telefonisch melden: [0231 919 5000](tel:02319195000) (Continentale / Allysca, rund um die Uhr).
Vertragsnummer bereithalten und das Vorgehen abstimmen.

03 Ausbreitung begrenzen, Spuren erhalten.

IT-Fachleute betroffene Systeme gezielt isolieren lassen. Nicht unkoordiniert löschen, neu installieren oder wieder verbinden; Beweissicherung berücksichtigen.

04 Lage und Maßnahmen dokumentieren.

Zeitpunkt, betroffene Systeme, Meldungen und bereits veranlasste Schritte festhalten. IT, Datenschutz und rechtliche Beratung prüfen Meldepflichten und Fristen.

05 Wiederanlauf geordnet entscheiden.

Bereinigung und Rücksicherung mit Fachleuten planen, Wiederherstellung prüfen und Freigaben dokumentieren. Erpressungsforderungen nicht eigenmächtig bedienen.

JETZT AUSFÜLLEN UND AUCH OFFLINE AUFBEWAHREN

Interne IT / Vertretung:

Vertragsnummer:

Datenschutz / rechtliche Ansprechperson:

07 / WEITERFÜHRENDE INFORMATIONEN

Ihr nächster Schritt.

Nehmen Sie den ausgefüllten Risiko-Check mit in die Beratung. TrochaS bespricht mit Ihnen, welcher Schutz zu Ihrem Betrieb passt.

Bezirksdirektion TrochaS GmbH & Co. KG

Zum Pier 72 · 44536 Lünen

0231 9003357

info.trocha@continentale.de

Quellen und Stand

1 [Continentale: KuBuS® Cyber](#)

Produktseite; online geprüft am 03.10.2026.

2 [Allgemeine Versicherungsbedingungen \(46 Seiten\)](#)

Deckblatt: 01.02.2024. Download auf Produktseite mit Stand 10.2025 bezeichnet. Maßgeblich: der konkret vereinbarte Vertrag.

3 [Vorteilsdarstellung KuBuS® Cyber](#)

Druckstand 03.2025; Tarifgrundlage 02.2024. Kurzüberblick.

4 [BSI: 10 Tipps zur Cyber-Sicherheit für Unternehmen](#)

Ergänzende Prävention; online geprüft am 03.10.2026.

5 [BSI: Erste Hilfe bei einem IT-Sicherheitsvorfall](#)

Weiterführende technische und organisatorische Notfallhilfe.

6 [Offizielle Continentale-Seite der Bezirksdirektion TrochaS](#)

Kontakt und Anbieterangaben geprüft am 03.10.2026.

Herausgeber: Bezirksdirektion TrochaS GmbH & Co. KG. Versicherungsvertreter ausschließlich für Unternehmen des Continentale Versicherungsverbundes. Allgemeine Orientierung; individuelle Beratung und Vertragsunterlagen bleiben erforderlich.

Rechtliche Angaben zur Agentur

Titelmotiv: vorhandene KI-Illustration, keine realen Mitarbeitenden. Quellenprüfung / Ausgabe: 03.10.2026.