Foto: iStock/Pekic

Bit für Bit zu mehr Vertriebserfolg
Mit Digitaler Sicherheit bei Firmenkunden punkten

Die Digitalisierung macht Geschäftsprozesse schneller und effizienter, birgt aber auch ernstzunehmende Risiken. Von raffinierten Betrugsattacken über technische Ausfälle bis hin zur Haftung bei Datenschutzverstößen: Die finanziellen Folgen sind oft existenzbedrohend. Um den Ernstfall zu verhindern, sollten Sie Ihre Firmenkunden für die Digitale Sicherheit im Unternehmen sensibilisieren – und dabei helfen, die richtigen Schutzmaßnahmen zu ergreifen.

Wir unterstützen Sie dabei, den Bedarf Ihrer Kunden zu identifizieren, gezielt anzusprechen und die passenden Versicherungslösungen anzubieten.

Inhalt

Cyberkriminalität in Zahlen: Die Gefahr ist real

Datendiebstahl, Industriespionage oder Sabotage:
Cyberattacken sind längst keine Seltenheit mehr, wie aktuelle Zahlen belegen.
Tendenz: steigend. Nutzen Sie die Faktenlage, um Ihre Kunden zum Handeln anzuregen.

Angriffe gehören zum Berufsalltag

87 %

aller deutschen Unternehmen waren in den letzten zwölf Monaten Opfer eines Cyberangriffs.[1]

59 %

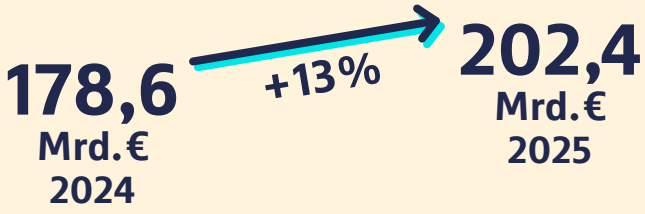
der Betriebe sehen sich durch Cyberattacken in ihrer Existenz bedroht.[1]

ø 119

neue Sicherheitslücken werden jeden Tag in IT-Systemen entdeckt.[2]

Immer höhere Wirtschaftsschäden

Allein in Deutschland stieg das Volumen im Jahr 2025 im Vergleich zum Vorjahr um 13%. Cyberangriffe machten damit zuletzt 70% des gesamten wirtschaftlichen Schadens aus. Zum Vergleich: 2021 lag der Anteil noch bei 59 %.[1]



KMUs besonders im Fokus…

80 %

der angezeigten Angriffe richten sich gezielt gegen kleine und mittlere Unternehmen (KMU) – diesen fehlt häufig das Wissen, um sich entsprechend zu schützen.[2]

67 %

der KMUs wurden in den letzten zwölf Monaten Opfer eines Cyberangriffs.[3]

…und dennoch mangelt es an der Absicherung

60 %

der Unternehmen sind nicht angemessen gegen Cyberangriffe abgesichert.[3]

Ransomware verursacht am häufigsten einen Schaden

Damit führt die digitale Erpressung mit 34% die Statistik für das Jahr 2025 an – gefolgt von DDoS-Attacken, Malware und Phishing.[2]

Quellen: [1]Bitkom Research (2025): Wirtschaftsschutz 2025, Berlin; [2]BSI-Lagebericht zur IT-Sicherheit in Deutschland 2025 (Bundesamt für Sicherheit in der Informationstechnik);
[3]Hiscox Cyber Readiness Report 2025

Digitale Sicherheit betrifft jeden und bietet viel Beratungspotenzial

Können Sie sich Ihren Berufsalltag eigentlich noch ohne Laptop und Smartphone vorstellen? Wohl eher kaum. Fast jeder hat tagtäglich mit digitalen Schnittstellen zu tun – vor allem im Gesundheitsbereich, in Verwaltungsangelegenheiten oder bei Bankgeschäften. Cyberattacken, IT-Fehler oder Datenschutzverstöße können hier große Schäden anrichten:
Der Sicherheit im digitalen Raum wird damit eine immer größere gesellschaftliche Rolle zuteil.

Mehr Pflicht als Kür: Warum die Absicherung von Cyberrisiken kein „nice-to-have“ ist

- Zunehmende Digitalisierung in allen Branchen und Geschäftsbereichen – unabhängig von Größe und Mitarbeiterzahl
- Neue gesetzliche Anforderungen, etwa hinsichtlich Datenschutz oder IT-Sicherheitsvorgaben (z.B. DSGVO-Richtlinien)
- Hohe Verwundbarkeit, insbesondere bei kleinen und mittleren Unternehmen ohne eigene IT-Abteilung

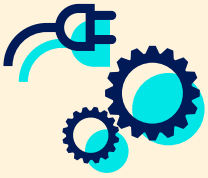
Managerhaftung bei Untätigkeit

Nach einem Gerichtsurteil[1] aus dem Jahr 2024 führt Unterversicherung trotz Einschaltung von Maklern zur Managerhaftung. Dies kann – und sollte – durch einen ausreichenden Versicherungsschutz verhindert werden.

Was brauchen Ihre Kunden eigentlich? Nur wer den Bedarf versteht, kann auch zielgenau beraten

Eine zentrale Frage in jeder Beratung: Kennen Ihre Kunden die Risiken und sind sie dagegen abgesichert? Um den Status Quo eines Unternehmens richtig zu analysieren, lässt sich Digitale Sicherheit in drei verschiedenen Bedarfsfeldern denken, die im Folgenden detailliert beschrieben werden.

Absicherung der Schäden durch Cyber-Kriminelle



Schutz vor den Folgen technischer Störungen

Abwehr von persönlichen Haftungsansprüchen

Risiken aufzeigen, Lösungen anbieten: Kundenbedarf im Detail

Nachvollziehbare und kundenfreundliche Beratung dank klarer Strukturen:
Sensibilisieren Sie Ihre Firmenkunden anhand dieser Themenfelder für die unterschiedlichen Risiken.

Foto: iStock/Skyneshe

Absicherung der Schäden durch Cyber-Kriminelle

Cyberkriminalität ist längst kein Randthema mehr, sondern zählt zu den größten Geschäftsrisiken für Unternehmen jeder Größe. Angreifer gehen zunehmend gezielt vor – etwa durch Phishing-Mails, Schadsoftware oder Social Engineering.
Ziel ist es, Zugang zu internen Systemen zu erhalten, Daten zu stehlen oder Zahlungsflüsse umzuleiten. Besonders heimtückisch: Viele Angriffe sind so professionell gestaltet, dass Mitarbeitende sie kaum erkennen können.

Folgen

- Betriebsunterbrechungen
- Datenverlust
- hohe Kosten für IT-Forensik
- Datenwiederherstellung
- Bußgelder nach Datenschutzverstößen
- Vermögensschäden nach betrügerischen Handlungen Dritter über das Internet (Social Engineering)

Produkte

- **R+V-CyberRisk & R+V-Vertrauensschadenversicherung (VSV)**
- **R+V-Wirtschaftsschutz-Police**

Tipp:

Prüfen Sie, ob das Unternehmen über eine ausreichende D&O- und Rechtsschutz-Deckung verfügt.

Kundenbedarf im Detail

Schutz vor den Folgen technischer Störungen

Nicht jeder digital verursachte Schaden entsteht durch Hacker oder Kriminelle – viele Gefahren entstehen innerhalb des Unternehmens selbst. Häufige Ursachen sind Hardwaredefekte, Softwarefehler, Stromausfälle oder menschliche Bedienfehler. Ein fehlerhaftes Update kann ganze Systeme lahmlegen, ein Serverausfall zu Datenverlust führen oder ein falsch konfiguriertes Backup wertvolle Unternehmensdaten vernichten oder gar Kundendaten veröffentlichen. Auch externe Faktoren wie Überspannung, Überhitzung oder Ausfälle von Cloud-Diensten können kritische Betriebsunterbrechungen verursachen.

Risiken und Folgen

- Produktionsstillstand
- Umsatzverluste
- Wiederherstellungskosten
- kostspielige Reparaturen
- Haftungs- oder Schmerzensgeldansprüche Dritter
- Strafen und Bußgelder wegen der Verletzung gesetzlicher Vorschriften

Produkte

- **R+V-CyberRisk, R+V-VSV, R+V-Wirtschaftsschutz Police**
- **R+V-Elektronikversicherung**
- **R+V-D&O-Versicherung**
- **R+V-Betriebshaftpflicht**

Kundenbedarf im Detail

Abwehr von persönlichen Haftungsansprüchen

Im digitalen Alltag genügt ein unbedachter Klick, um großen Schaden anzurichten. Mitarbeitende können durch Unachtsamkeit, Unwissen oder Stress Datenpannen verursachen – etwa durch versehentliches Löschen sensibler Dateien, falsche Empfänger bei E-Mails oder die Weitergabe von Zugangsdaten.

Nach der DSGVO haftet das Unternehmen grundsätzlich für Datenschutzverstöße seiner Beschäftigten. Doch auch Führungskräfte tragen Verantwortung: Unterlassen sie angemessene Sicherheitsvorkehrungen oder Schulungen, können sie persönlich haftbar gemacht werden.

Risiken

- finanzielle Schäden
- Bußgelder
- Vertrauensverlust
- rechtliche Auseinandersetzungen

Produkte

- **R+V-D&O-Versicherung**
- **R+V-Spezial-Straf-Rechtsschutz**

➔ Zur digitalen Sicherheit gehört daher ein verlässlicher Haftungsschutz, der sowohl die Existenz des Unternehmens als auch das Privatvermögen der haftenden Personen schützt. Ergänzend ist ein Spezial-Straf-Rechtsschutz von Bedeutung, um die finanziellen Kosten einer optimalen Strafverteidigung zu tragen.

Der Ruf Ihrer Kunden steht auf dem Spiel

Zu allen hier genannten Folgen kommt auch das Risiko eines erheblichen Reputationsschadens – zu recht. Mal angenommen, Ihre Daten gelangen durch ein selbstverschuldetes Datenleck bei Ihrer Bank in die Hände von Kriminellen. Würden Sie dieser Bank noch weiterhin Ihr Vertrauen schenken? Sich gegen die hier benannten Risiken abzusichern ist dementsprechend nicht nur für das Unternehmen selbst wichtig, sondern auch für deren Kunden und Geschäftspartner.

Kein Science Fiction: Echte Schaden- und Leistungsbeispiele

Diese echten Fälle zeigen, wie raffiniert Cyber-Kriminelle vorgehen oder welche gravierenden Folgen IT-Fehler und Datenpannen nach sich ziehen können – aber auch, wie den Kunden geholfen wurde.

Foto: iStock/visualspace

Absicherung der Schäden durch Cyber-Kriminelle

Eingeschleuste Schadsoftware

Eine vermeintliche Kunden-E-Mail schleuste einen Virus in die Systeme eines Kleidungsherstellers. Über diese Schadsoftware konnten die Kriminellen eingehende E-Mails nun direkt im Postfach lesen und löschen. Reale Rechnungen wurden gelöscht und die erlangten Informationen genutzt, um dem Unternehmen gefälschte Rechnungen zu tatsächlich erhaltenen Warenlieferungen von einer täuschend ähnlich klingenden E-Mail-Adresse zu senden. Der Kleidungshersteller überwies daraufhin die Beträge auf Konten der Kriminellen und bemerkte den Fehler erst, als die ersten Zahlungserinnerungen der tatsächlichen Lieferanten eingingen.

Folgen und Ursache

Das gesamte System der Firma musste nun nicht nur überprüft und bereinigt, sondern auch die Rechnungsbeträge erneut überwiesen werden – dieses Mal an die richtigen Gläubiger. Bei Prüfung stellte sich heraus, dass der Virus in die Systeme eindringen konnte, da der zuständige IT-Vorstand Herr Berger aus Kostengründen an dem bisherigen Virenschutz-Programm noch sechs Monate festhalten wollte. Der Kleidungshersteller verlangte deshalb von ihm sämtliche Kosten ersetzt, die durch sein fahrlässiges Handeln entstanden sind.

Produkte

Die R+V kam mit der **R+V-CyberRisk Police** für alle Kosten zur Beseitigung der Schadsoftware auf, die **R+V-Vertrauensschadenversicherung** wiederum ersetzte den Schaden aus den fehlerhaften Überweisungen.

Die **R+V-D&O-Versicherung** von Herrn Berger übernahm neben den anfallenden Rechtsverteidigungs-/Abwehrkosten auch den finanziellen Schaden, den er der Firma durch seine Pflichtverletzung verursacht hat.

Echte Schaden- und Leistungsbeispiele

Foto: iStock/Organic Media

Schutz vor den Folgen technischer Störungen

Regelmäßiges System-Update versäumt

Bei einem Hersteller von Getreideprodukten wird es nach einem Wechsel in der Geschäftsleitung versäumt, den Nachfolger eines längerfristig erkrankten Mitarbeiters für die technische Wartung der Produktionsanlage einzuarbeiten. Das wöchentliche Systemupdate der Anlage wird daher nicht mehr verlässlich technisch angestoßen und durchgeführt.

Folgen und Kosten

Nach einiger Zeit klagen drei Kunden nach dem Verzehr der Produkte über Unwohlsein und allergische Beschwerden. Bei der Überprüfung der Mischanlage wird entdeckt, dass sie inzwischen mit einem Schimmelpilz (Toxin) befallen ist, der sich auch in den Cerealien wiederfindet. Die Anlage steht über mehrere Tage still, denn ein zusätzlicher Spezialfilter muss für 80.000 Euro beschafft werden.

➔ **Schmerzensgeld und ärztliche Behandlungskosten: weitere 60.000 Euro**

Produkte

Die R+V kam über die **Sachversicherung** für die versicherten Kosten aus der Betriebsunterbrechung auf und ersetzte über die **R+V-Betriebshaftpflicht** auch die Heilbehandlungskosten sowie die Schmerzensgeldforderungen der erkrankten Personen.

Die **R+V-D&O-Versicherung** des Unternehmens übernahm unter anderem auch den finanziellen Schaden für den neuen Filter, den die neue Geschäftsführerin der Firma durch ihre Pflichtverletzung verursacht hat.

Echte Schaden- und Leistungsbeispiele

Es muss nicht immer ein Angriff sein: Das folgende Beispiel zeigt,
wie prekär das Thema Haftung im Bereich der digitalen Sicherheit sein kann.

Abwehr von persönlichen Haftungsansprüchen

Datenpanne alarmiert Staatsanwaltschaft

Ein mittelständisches IT-Dienstleistungsunternehmen mit 80 Mitarbeitenden betreut sensible Kundendaten (z. B. Vertrags- und Bankinformationen). Ein Mitarbeiter verschickt versehentlich eine Excel-Datei mit personenbezogenen Daten von rund 1.200 Kunden an einen falschen externen Empfänger. Der Fehler wird zu spät bemerkt – die Datei wurde zwischenzeitlich geöffnet und teilweise weitergeleitet. Die Staatsanwaltschaft untersucht wegen der Geschäftsbeziehung des Versicherungsnehmers zu dem Dritten ein aus ihrer Sicht hinreichend indiziertes absichtliches gewerbsmäßiges Handeln des VN. Sie leitet dafür ein Ermittlungsverfahren gegen die Geschäftsführung ein.

Folgen der Datenpanne

- Meldepflicht an die Datenschutzbehörde (nach Art. 33 DSGVO) innerhalb von 72 Stunden
- Benachrichtigungspflicht gegenüber allen betroffenen Personen (Art. 34 DSGVO)
- Bußgeld der Datenschutzbehörde in Höhe von 80.000 Euro wegen unzureichender interner Kontrollprozesse und Schulungsmaßnahmen
- Rechtsberatung und Krisenkommunikation verursachen zusätzliche Kosten von 20.000 Euro
- Schadenersatzforderungen einzelner Kunden (wegen immaterieller Schäden) summieren sich auf 15.000 Euro
- Ermittlungsverfahren nach § 42 BDSG gegen die Geschäftsführer, für das jedoch unter Einschaltung eines Strafverteidigers die Einstellung des Verfahrens erwirkt wird. Kosten rund 25.000 Euro

➔ **Gesamtschaden: 140.000 Euro**

Produkte

Die **R+V-D&O-Versicherung** schützt die Geschäftsführerin in diesem Fall vor den finanziellen Folgen der persönlichen Haftung. Sie übernimmt die Prüfung der Haftungsansprüche, Abwehr unberechtigter Forderungen sowie ggf. Zahlung von Schadenersatz, wenn eine Pflichtverletzung nachgewiesen wird. In diesem Beispiel wurden 30.000 Euro Anwalts- und Gutachterkosten als Rechtsverteidigungskosten übernommen, 50.000 Euro Schadenersatzforderungen aus der Organhaftung reguliert sowie 10.000 Euro interne Aufwandskosten für Kommunikation und Krisenmanagement erstattet.

Die Kosten, die bei der Beauftragung eines Strafverteidigers anfallen, werden durch den **R+V-Spezial-Straf-RS** abgedeckt und übernommen.

➔ **Gesamterstattete Summe durch die R+V-D&O-Versicherung und den R+V-Spezial-Straf-Rechtsschutz: 115.000 Euro**

Rechtlicher Rahmen

Nach DSGVO haftet das Unternehmen grundsätzlich für Datenschutzverstöße, die durch Mitarbeitende verursacht wurden. Die Aufsichtsbehörde stellt fest, dass die Geschäftsführung ihre Aufsichtspflicht verletzt hat: Es gab keine ausreichende Schulung der Mitarbeitenden im Umgang mit personenbezogenen Daten. Interne Prüfprozesse für Versand und Freigabe sensibler Dateien fehlten. Daher werden persönliche Haftungsansprüche gegen die Geschäftsführerin geprüft (Organhaftung nach § 43 GmbHG).

Top-Argumente für Ihre Beratung

Warum sollten sich Ihre Kunden unbedingt gegen digitale Risiken absichern?

Jedes Unternehmen ist betroffen – nicht nur große Konzerne

Kleine und mittlere Unternehmen (KMU) machen laut BKA rund 80% der von Ransomware betroffenen Unternehmen aus.

Ein einziger Angriff kann existenzbedrohend sein

Der durchschnittliche Schaden nach einem Ransomware-Angriff: bis zu 1,2 Mio. Euro.

Quelle: Global Ransomware Trends 2024 Report von ExtraHop

Datenschutzverstöße sind kein Kavaliersdelikt

DSGVO-Bußgelder liegen oft zwischen 10.000 Euro und 100.000 Euro bis zu 20 Mio. Euro oder 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr (höherer Wert gilt).

Die Haftung trifft die Geschäftsleitung persönlich

Die Geschäftsleitung (und gegebenenfalls auch leitende Angestellte) haften persönlich und unbegrenzt für Organisations-und Überwachungsfehler.

Mehr Argumente und Gesprächsanlässe finden Sie in unserem ToolKit für Makler – jetzt kostenlos downloaden

Besuchen Sie uns gleich im R+V-Maklerportal und holen Sie sich alle weiterführenden Informationen zum Thema Digitale Sicherheit:

https://online.ruv.de/makler/vertriebsinfos/themenansprache/digitale-sicherheit

Checkliste:

Wie steht es um die Digitale Sicherheit Ihrer Kunden?

Machen Sie im Beratungsgespräch doch einfach einen schnellen Test. Bleiben Felder blank, ist Handeln angesagt. Die folgenden Punkte sollen dabei nur einen ersten Anhaltspunkt für die Digitale Sicherheit eines Unternehmens bieten. Welche (weiteren) Maßnahmen notwendig sein können, muss stets individuell geprüft werden.

- regelmäßige Backups – extern und offline gespeichert
- Originaldaten und Datensicherung (Backup) dürfen nicht durch dieselbe Ursache manipuliert, beschädigt oder unbrauchbar gemacht werden (Backup-Management)
- Mitarbeiterschulungen – Erkennen von Phishing und Social Engineering
- Zugriffsrechte beschränken – „Need-to-know“-Prinzip
- Mehrfaktor-Authentifizierung (MFA) aktivieren
- Updates & Patches konsequent durchführen
- Passwort-Richtlinie implementieren
- Hinreichende Passwortkomplexität sowie nach z.B. fünf Fehlversuchen das Konto sperren
- Notfallplan (Incident Response Plan) entwickeln – wer macht was im Ernstfall?
- Datenschutzprozesse dokumentieren (DSGVO-konform)
- D&O-Deckung prüfen, falls Organisationspflichten verletzt werden könnten

Wichtig: Selbst die beste Police ersetzt keine solide IT- und Organisationssicherheit

Kontaktieren Sie bei Fragen gern Ihren bekannten R+V-Ansprechpartner. Hier finden Sie weitere Kontaktoptionen: makler.ruv.de/kontakt