



Du bist nicht allein.



2026

ToolKit für Makler

Themenansprache Digitale Sicherheit

 **Gemeinsam
für Ihren Erfolg**



Das ToolKit für Makler

Gebündelte Vertriebspower – nur einen Klick entfernt

Gemeinsam startklar für neue Vertriebserefolge!

Auf den nachfolgenden Seiten haben wir Know-how, gebündeltes Fachwissen, schlagkräftige Argumente und zahlreiche Unterstützungen zusammengestellt, um Sie und Ihre Kunden umfassend rund um das Thema Digitale Sicherheit zu informieren.

Nutzen Sie dieses ToolKit für die intensive Beratung und Marktbearbeitung. Profitieren Sie von maßgeschneiderten Produktvorteilen und Neuerungen für das Beratungsgeschäft mit Ihren Kunden.

Wir wünschen Ihnen viel Erfolg!

ToolKit für Makler

Für Sie zur optimalen
Ansprache Ihrer Kunden



Dieses ToolKit ist
interaktiv aufgebaut.

Bitte navigieren Sie
mithilfe der Buttons.



Das ToolKit für Makler

In 4 Schritten zum Vertriebserfolg

1

Bedarfe kennen

„Ich habe das nötige Wissen aufgebaut.“

Branchendynamik

Bedarfe und Lösungen



2

Kunden überzeugen

„Ich kann den Bedürfnissen und Bedarfen meiner Kunden begegnen.“

Leistungsbeispiele

Produkthighlights

Reputation



3

Potenziale nutzen

„Ich kenne Potenziale und Verkaufschancen.“

Anspracheanlässe

Checklisten

Erfolgreich ansprechen



4

Kunden unterstützen

„Ich helfe meinen Kunden dabei, die richtige Entscheidung zu treffen.“

Verkaufsunterstützung

Cross-Selling





Bedarfe kennen

„Ich habe das nötige Wissen aufgebaut.“

Inhalte

Branchendynamik

Bedarfe und Lösungen

Nur wer sich auskennt, kann überzeugen!

In diesem Kapitel finden Sie alles Wissenswerte rund um das Thema Digitale Sicherheit, aktuelle Hintergründe sowie Informationen zu unseren Lösungen.

Klicken Sie sich durch und werden Sie zum überzeugenden Produktexperten.





Branchendynamik

Aktuelle Kennzahlen zur digitalen Sicherheit



87 % aller Unternehmen waren in den letzten 12 Monaten von **Diebstahl, Industriespionage oder Sabotage** betroffen.¹



80 % sehen Social Engineering (= Ausnutzung von Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität durch Kriminelle) als größte Cybergefahr.²



59 % der Betriebe sehen sich durch Cyberattacken in ihrer **Existenz bedroht**.¹



Cyberschäden steigen

Das Volumen aller Cyberschäden ist 2025 um 13 % gestiegen – von 178,6 Mrd. EUR in 2024 auf 202,4 Mrd. EUR¹

Achtung, Managerhaftung!

Nach einem Urteil des Oberlandesgerichts Schleswig-Holstein (OLG Schl.-Holst., Ur.t.v. 26.02.2024 – 16 U 93/23) führt Unterversicherung trotz Einschaltung von Maklern zur Managerhaftung.

Quellen: ¹ Bitkom Research (2025): Wirtschaftsschutz 2025, Berlin; ² Security Awareness Report des SANS Institute, 21.08.2025; ³ Hiscox Cyber Readiness Report 2025.

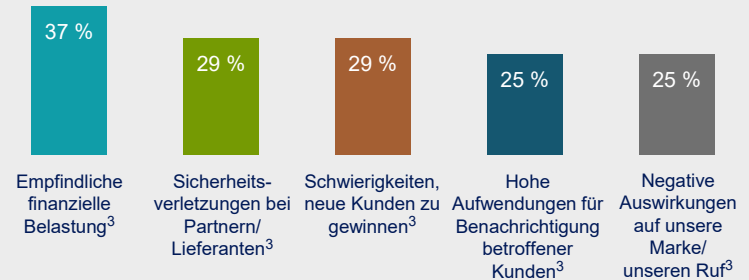
Mangelnde Absicherung gegen Cyberangriffe

67 % der kleinen und mittleren Unternehmen erlitten in den letzten 12 Monaten einen Cyberangriff³

60 % sind nicht angemessen gegen Cyberangriffe abgesichert³

34 % der Unternehmen planen, die Investitionen in Cybersicherheit signifikant zu erhöhen³

Auswirkungen der Cyber-Attacken auf das Unternehmen





Bedarfe und Lösungen

Thema Digitale Sicherheit

**Sie sprechen Cyber-Gefahren an.
Wir bremsen digitale Risiken aus.**

Digitalisierung macht Geschäftsprozesse schneller und effizienter – aber auch angreifbarer: Für Ihre Firmenkunden wachsen die Risiken. Von raffinierten Betrugsattacken über technische Ausfälle bis hin zur Haftung bei Datenschutzverstößen. Die finanziellen Folgen können das Aus bedeuten. Deshalb sprechen Sie mit Ihren Kunden über digitale Sicherheit. Und geben ihnen mit unseren Lösungen die Gewissheit, auch in einer vernetzten Welt geschützt zu sein.

Sie strukturieren Risiken, ordnen ein und machen Ihren Kunden komplexe Zusammenhänge verständlich. Wir unterstützen Sie dabei, dieses anspruchsvolle Thema souverän zu platzieren und Ihren Kunden tragfähige Lösungen aufzuzeigen, die Sicherheit und Orientierung geben.

Sprechen Sie Cyber-Gefahren aktiv bei Ihren Firmenkunden an
Geben Sie ihnen mit unseren Cyber- und Datenschutzlösungen die Gewissheit, auch bei Störungen in einer vernetzten Welt immer handlungsfähig zu bleiben.

MehrWerte für Makler

Wir bieten Ihnen umfangreiche MehrWerte und ein ausgezeichnetes Netzwerk: mit innovativen Produkten, zeitsparenden digitalen Services, breitem Experten-Know-how und einer Betreuung, die Sie und Ihre Kunden in den Mittelpunkt stellt.



**Gemeinsam für
Ihren Erfolg**



Bedarfe und Lösungen

Zielgruppe mit hohem Bedarf



Die Hürden für einen erfolgreichen Cyberangriff auf ein gut geschütztes Unternehmen sind mittlerweile deutlich höher. Natürlich sind auch gut aufgestellte Unternehmen nicht immun, aber sie sind schwerer zu „knacken“.

Deshalb haben sich **die Schwerpunkte der Cyber-Kriminellen verlagert** – weg von Großunternehmen und **hin zu kleinen und mittleren Unternehmen**, deren digitale Sicherheit häufig lückenhaft ist.

Für Ihre Kunden ist eine Frage zentral:



**„Kenne ich die vielfältigen Risiken
und bin ich ausreichend versichert?“**



Bedarfe und Lösungen

Einteilung in Themenfelder

Um die zentrale Frage „**Kenne ich die vielfältigen Risiken und bin ich ausreichend versichert?**“ zu beantworten, werden die Bedarfe Ihrer Firmenkunden in verschiedene Themenfelder eingeteilt, für die wir die jeweils passenden Lösungen haben.

Bitte klicken Sie auf eines der Themenfelder für vertiefende Informationen.



Absicherung der Schäden durch Cyber-Kriminelle



Schutz vor den Folgen technischer Störungen



Abwehr von persönlichen Haftungsansprüchen





Bedarfe im Detail

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.**

Die Folgen sind vielfältig:

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

Hinzu kommt das Risiko eines erheblichen Reputationsschadens. **Für Firmenkunden ist es daher essenziell, sich gegen diese Risiken abzusichern.** Eine CyberRisk-Versicherung übernimmt Kosten für die Schadenbewältigung, Wiederherstellung und Haftungsansprüche Dritter. Gleichzeitig schützt eine Vertrauensschadenversicherung im Paket mit separaten Versicherungssummen vor Schäden durch Täuschung oder betrügerische Handlungen Dritter.

Unsere Lösungen:



**R+V-CyberRisk
Police und R+V-
Vertrauensschaden-
versicherung**



**R+V-
Wirtschaftsschutz
Police**



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



Bei Betrieben mit einem Jahresumsatz ≤ 25 Mio. EUR bieten die R+V-CyberRisk Police und R+V-Vertrauensschadenversicherung innerhalb der **R+V-MultiLine Police** einen umfassenden Schutz bei gezielten Angriffen durch Dritte über das Internet.



Die **R+V-CyberRisk Police** ersetzt Vermögens-, Sach- und Drittschäden sowie versicherte Kosten, die auf eine Informationssicherheitsverletzung zurückzuführen sind, und bietet zusätzlich umfangreiche Assistance-Dienstleistungen. Lediglich vier Sicherheitsvoraussetzungen müssen Kunden bis 25 Mio. EUR Jahresumsatz erfüllen:

1. Lizenz-Management für Software
2. Funktionierendes Back-up-Management/Datensicherung
3. Aktuelle Antivirensoftware und Firewall
4. Keine Nutzung von Administratorenrechten für die normale tägliche Arbeit

Diese Sicherheitsvoraussetzungen werden durch vier Risikofragen abgefragt. Im Versicherungsschutz enthalten ist zudem ein Rechtsschutz-Baustein zur Durchsetzung von Schadenersatzansprüchen gegen den Schadenstifter.

R+V-Vertrauensschadenversicherung

Vertrauen wird oft in betrügerischer Absicht missbraucht – zunehmend auch mithilfe des Internets. Nicht selten sind dann existenzielle Schadenhöhen die Folge von Hackerangriffen.

Die R+V-Vertrauensschadenversicherung schützt Ihre Kunden vor den Folgen krimineller Straftaten im Geschäftsverkehr.

Sie ersetzt Vermögensschäden, die im Geschäftsverkehr u.a. über das Internet als Tatmittel und als Folge wirtschaftskrimineller Handlungen durch Dritte oder Vertrauenspersonen im laufenden (oft digitalen) Geschäftsverkehr entstehen.

R+V-MultiLine Police

- › für Betriebe mit Jahresumsatz ≤ 25 Mio.
- › Versicherungssumme VSV ≤ 1 Mio. EUR
- › VSU Cyber ≤ 2 Mio. EUR

Mehr erfahren

Info: Unternehmen mit einem Umsatz über 25 Mio. können Sie über die **R+V-WirtschaftsschutzPolice** absichern.



R+V-Wirtschaftsschutz Police

Für Unternehmen ab 25 Mio. EUR Jahresumsatz bietet die R+V-Wirtschaftsschutz Police maximalen Schutz mit einer einzigen Police. Sie kombiniert die Absicherung vor den Folgen aus Cyber-Risiken und wirtschaftskriminellen Handlungen über einen Versicherungsschein überschneidungsfrei.

Sie ersetzt Vermögens-, Sach- und Drittschäden sowie versicherte Kosten, die auf eine Informationssicherheitsverletzung zurückzuführen sind, und bietet zusätzlich umfangreiche Assistance-Dienstleistungen. Zudem sind Vermögensschäden, die im Geschäftsverkehr u.a. über das Internet als Tatmittel und als Folge wirtschaftskrimineller Handlungen durch Dritte oder Vertrauenspersonen im laufenden (oft digitalen) Geschäftsverkehr entstehen, abgesichert.

R+V-Wirtschaftsschutz Police

- › für Betriebe mit Jahresumsatz > 25 Mio. EUR bis ≤ 250 Mio.
- › Versicherungssumme VSV ≤ 3 Mio. EUR
- › VSU Cyber ≤ 5 Mio. EUR

[Mehr erfahren](#)

Info: Unternehmen mit einem Umsatz unter 25 Mio. EUR können Sie über die MultiLine Policen (z. B. UNP) absichern.

Bei einem Umsatz über 250 Mio. EUR senden Sie uns bitte eine individuelle Anfrage.



Bedarfe 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.

Diese internen Fehler oder technischen Störungen haben oft ähnliche wirtschaftliche Folgen wie ein Angriff von außen:

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

Unsere Lösungen:



R+V-CyberRisk /
R+V-VSV / R+V-
Wirtschaftsschutz
Police



R+V-Elektronik-
versicherung



R+V-D&O-
Versicherung



R+V-
Betriebshaftpflicht





R+V-CyberRisk / R+V-Wirtschaftsschutz Police

Cyber-Risiken lediglich auf kriminelle Handlungen zu beziehen, wird dem tatsächlichen Umfang nicht gerecht.

Technische Defekte und menschliches Versagen können ebenso – ungeachtet der überwiegenden Vorteile – die Gefahren einer großen Abhängigkeit von Technik und Digitalisierung aufzeigen.

- › Das können beispielsweise sein:
- › Verletzung von Geheimhaltungspflichten
- › rechtswidrige Kommunikation
- › Urheberrechtsverletzungen

Sind diese auf eine Informationssicherheitsverletzung zurückzuführen, besteht Versicherungsschutz im Rahmen der R+V-CyberRisk Versicherung.

[Mehr erfahren](#)

Abhängig vom Jahresumsatz des Betriebes erfolgt die Absicherung über

- › die R+V-MultiLine Policen (z.B. UNP) bei ≤ 25 Mio. EUR Jahresumsatz

oder

- › die R+V-Wirtschaftsschutz Police bei einem Jahresumsatz > 25 Mio. EUR bis ≤ 250 Mio. EUR



R+V-Elektronikversicherung

Eine große Abhängigkeit von Informationstechnologien bringt zwangsläufig auch eine **Abhängigkeit von den datenverarbeitenden Geräten mit sich. Ohne funktionierende Hardware, keine Software.**

Über eine Elektronikversicherung **können sämtliche elektrotechnischen und elektronischen Anlagen und Geräte** eines Unternehmens **versichert werden.** Von Daten-, Informations- und Kommunikationstechnik sowie Bürogeräten, über Mess-, Prüf- und Sicherungstechnik, Materialprüf- und Labortechnik, Bild- und Tontechnik, bis hin zu Medizintechnik.

Versicherungsschutz besteht im Rahmen einer Allgefahrendeckung, das heißt, dass alle Gefahren versichert gelten, sofern diese nicht ausdrücklich ausgeschlossen gelten.

[Mehr erfahren](#)



R+V-D&O-Versicherung



Die Gefahren, die sich aus der Digitalisierung ergeben, sind vielfältig, die potenziellen Schäden können existenziell sein. **Zur Vorbeugung ist ein professionelles Risikomanagement-System unverzichtbar – und zwar unabhängig von der Unternehmensgröße.**

Dieses Risikomanagement-System, seine Einrichtung, Dokumentation und Kontrolle müssen laufend an sich verändernde Herausforderungen angepasst werden. Das ist originäre Pflicht (sog. Kardinalpflicht!) jeder Unternehmensleitung und kann grundsätzlich nicht delegiert werden.

Zu dieser Kardinalpflicht gehört nicht nur die Auswahl **geeigneter Soft- und Hardware sowie externer und interner IT-Dienstleister** bzw. Mitarbeiter. Genauso wichtig sind die **regelmäßige Schulung der Mitarbeiter, die Ausarbeitung von Notfallplänen und deren regelmäßige(!) Überprüfung bzw. Anpassung.**

Die Geschäftsleitung kann sich bei IT- und Cyber-Risiken nicht darauf beschränken, einen IT-Fachmann mit der Eingrenzung IT-spezifischer Risiken zu beauftragen. Vielmehr muss das Leitungsorgan (GF / Vorstand) die unternehmensspezifischen Risiken selbst bewerten und nachvollziehen.

[Zu den Urteilen und Gesetzen](#)[Mehr erfahren](#)



Urteile und Gesetze zur D&O-Versicherung

Ein funktionierendes
Risikomanagement-System ist
**unabhängig von der
Unternehmensgröße essenziell.**

Vgl. §§ 43 GmbHG
iVm. 91 II AktG

**Aktualität des
Risikomanagement-Systems** ist
Kardinalpflicht jeder
Unternehmensleitung.

BGH, Ur. v. 06.11.2018

**Die Geschäftsleitung muss die
Bestandsaufnahme** der
unternehmensspezifischen Risiken
**selbst bewerten und
nachvollziehen.**

Vgl. LG München I, NZG
2008, 319 (320)



R+V-Betriebshaftpflicht

Die Betriebshaftpflichtversicherung deckt **nicht nur Ansprüche Dritter wegen Personen- und Sachschäden, sondern auch mitversicherte Vermögensschäden im Rahmen der betrieblichen Tätigkeit**. Sie bietet Schutz vor finanziellen Risiken, letztlich also auch mehr unternehmerische Freiheit.

Egal, ob Handwerker oder Industrieunternehmen: Erbrachte Gewerke, selbst hergestellte oder gehandelte Produkte und Dienstleistungen können zu berechtigten, aber auch unberechtigten Schadenersatzforderungen Geschädigter in großer Höhe führen.

Führt ein Installations- und Programmierungsfehler eines Technikers dazu, dass die Maschine eines Kunden dessen eingesetzten Rohstoffe mit Öl verunreinigt, würde die Betriebshaftpflichtversicherung Schadenersatz leisten.

[Mehr erfahren](#)



Bedarfe 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.

Beispiel:

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.

Die Risiken sind vielfältig:

- › finanzielle Schäden
- › Bußgelder
- › Vertrauensverlust
- › rechtliche Auseinandersetzungen

Unterläuft Mitarbeitenden oder dem Management ein Fehler, der zu einem Schaden führt, können Haftungsansprüche auf Geschäftsführer und Management zukommen. 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.

Unsere Lösungen:



R+V-D&O-
Versicherung



R+V-Spezial-Straf-
Rechtsschutz





R+V-D&O-Versicherung

Risiko-Früherkennungssysteme sollen nicht nur Schäden **vermeiden**, sondern auch den Anstoß geben, Schäden und Haftungsrisiken durch einen geeigneten Versicherungsschutz abzusichern – ein integraler Bestandteil jedes Risikomanagement-Systems.

Dazu gehören zum einen die Absicherung als solches, zum anderen aber auch die Auswahl geeigneter Produkte sowie die regelmäßige Überprüfung und Anpassung von Deckungsumfang und Versicherungssummen. **Diese Pflicht ist nicht vollständig übertragbar** (OLG Schl.-Holst., Urt. V. 26.02.2024 - 16 U 93/23), auch dann nicht, wenn ein Versicherungsvermittler eingeschaltet wird.

Kommt die Unternehmensleitung dieser Pflicht nicht im erforderlichen Umfang nach, macht sie sich selbst dem Unternehmen oder Dritten gegenüber schadenersatzpflichtig. Neben der Absicherung des Unternehmens gegen IT- und Cyber-Risiken ist deshalb auch die **Absicherung des Managements** über eine D&O-Versicherung (Unternehmens-D&O od. Persönliche D&O) essenziell. Denn sowohl die verursachten Schäden als auch die Kosten der Abwehr unbegründeter Ansprüche übersteigen oft das Privatvermögen der Verantwortungsträger um ein Vielfaches.

Dieser weltweite Versicherungsschutz umfasst alle Vorstands-, Geschäftsführungs-, Aufsichtsrat-/Beirats-Mitglieder sowie leitende Angestellte von Kapital-, Personengesellschaften und Non-Profit-Organisationen. Versichert sind Ansprüche des Unternehmens sowie Schadenersatzansprüche Dritter.

Als einer der führenden D&O-Versicherer in Deutschland bietet die R+V diesen für Führungskräfte **essenziellen Versicherungsschutz in drei Varianten an:**

- › Unternehmens-Deckung (für alle potenziell betroffenen Personen)
- › Persönliche D&O (individueller Schutz für den einzelnen Manager)
- › Vereins-D&O (wie Unternehmens-Deckung, aber zu Sonderkonditionen)

Sonderfall gesetzlicher Pflicht-Selbstbehalt (insbes. Aktiengesellschaften):

Bitte sprechen Sie Ihren Maklerbetreuer oder zuständigen Direktionsbevollmächtigten an.

[Mehr erfahren](#)[Tarifrechner](#)



Persönliche D&O



Anders als bei der Unternehmens-Variante kann der Versicherungsschutz bei der Persönlichen D&O von der jeweiligen Person individuell, für mehrere Mandate und unabhängig von einer eventuell bestehenden Unternehmens-D&O abgeschlossen werden.

Zum Beispiel:

- › Um nicht in Abhängigkeit von Unternehmensentscheidungen zu stehen.
- › Weil eine Kollektiv-Versicherung die Gefahr des Abschmelzens der VSU bedeutet.
- › Wenn die Person die Deckungsinhalte der Unternehmens-D&O nicht kennt.
- › Falls das Ausscheiden aus dem Unternehmen die eigenen Einflussnahme-Möglichkeiten beendet, die Haftung mit langen Verjährungsfristen aber fort dauert.
- › Weil Obliegenheitsverletzungen Dritter ggfs. den eigenen Versicherungsschutz gefährden.
- › Wenn Probleme durch Nachfolger drohen (Kündigung, Reduzierung der VSU, Zahlungsverzug etc.).

Zielgruppe der Persönlichen D&O sind Prokuristen und leitende Angestellte, Unternehmensberater, die als Interimsmanager agieren, oder Anwälte, die in ein Kontrollgremium berufen werden. Daneben ist sie aber auch für Organpersonen interessant, die bei ihrem D&O-Schutz nicht von Unternehmensentscheidungen (Vertragsaufhebung, Reduzierung oder Verbrauch der Versicherungssumme etc.) abhängig sein wollen.

Mehr erfahren

Tarifrechner



R+V-Spezial-Straf-Rechtsschutz



Der R+V-Spezial-Straf-Rechtsschutz ist auf die Bedürfnisse von Firmen und Selbstständigen ausgerichtet.

Er bietet eine **Absicherung bei der Verteidigung gegen strafrechtliche Vorwürfe** (Straftaten einschließlich Verbrechen und Ordnungswidrigkeiten) **und übernimmt neben der Vergütung von Anwälten in angemessener Höhe (Honorarvereinbarungen)** auch Zeugenentschädigungen, Gerichtsgebühren, Sachverständigenkosten und vieles mehr. Versichert ist die Unternehmensleitung genauso wie die Mitarbeitenden in Ausübung ihrer beruflichen Tätigkeit.

Mehr erfahren

Tarifrechner

Persönlicher Spezial-Straf-Rechtsschutz (SSR)

Als Geschäftsführer, Vorstandsmitglied oder gesetzlicher Vertreter von juristischen Personen kann man den Persönlichen Spezial-Straf-Rechtsschutz für sich selbst abschließen.

Die Absicherung ist besonders interessant für Top-Manager in verantwortlichen Positionen, die ihren Versicherungsschutz individuell kombinieren möchten.

Versichert ist die namentlich genannte Person als gesetzlicher Vertreter des/der im Versicherungsschein genannten Unternehmen/s.

Mehr erfahren

Tarifrechner



2

Kunden überzeugen

„Ich kann den Bedürfnissen und Bedarfen meiner Kunden begegnen.“

Inhalte

Leistungsbeispiele
Produkthighlights
Reputation

Digitale Risiken ansprechen und ausbremsen.

Zeigen Sie Ihren Kunden, welche Expertise die R+V bereithält. Mit umfangreichen Leistungsbeispielen, starken Produkten sowie exzellenten Ratings liefern wir die beste Basis für erfolgreiche Beratungsgespräche.





Leistungsbeispiele

Ganz praktisch überzeugen

Konkret, verständlich und direkt aus der Praxis: Mit diesen Leistungsbeispielen haben Sie gute Argumente an der Hand.

Absicherung der Schäden durch Cyber-Kriminelle

➤➤➤ Schadsoftware



Schutz vor den Folgen technischer Störungen

➤➤➤ IT-System lahmgelegt



➤➤➤ Regelmäßiges System-Update versäumt



Abwehr von persönlichen Haftungsansprüchen

➤➤➤ Datenpanne alarmiert Staatsanwaltschaft





Absicherung der Schäden durch Cyber-Kriminelle

Leistungsbeispiel: 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. 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.



R+V-CyberRisk Police & R+V- Vertrauensschadenversicherung (VSV):

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.

R+V-D&O-Versicherung:

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.



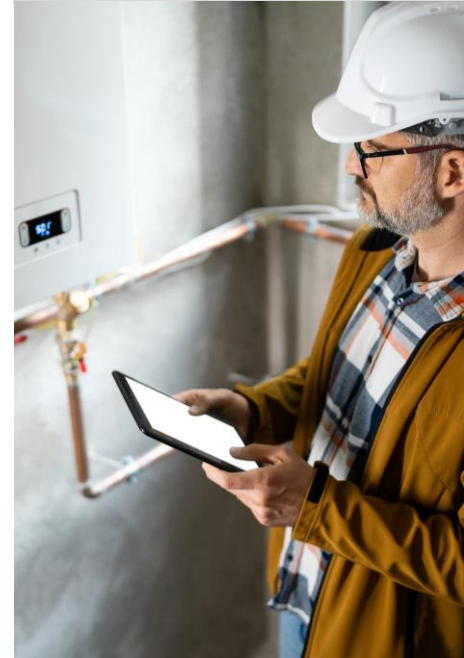


Schutz vor den Folgen technischer Störungen

Leistungsbeispiel: IT-System lahmgelegt

CyberRisk-Versicherung: Zero-Day-Sicherheitslücke

Eine schwerwiegende Sicherheitslücke, die nicht geschlossen werden konnte, hat Tausende von IT-Systemen (Exchange-Server) für Angriffe verwundbar gemacht. Unser Versicherungsnehmer, ein Heizungsinstallationsbetrieb, musste bis zur Klärung des Vorfalls seine IT-Systeme vom Netz nehmen. Es konnten in der Zwischenzeit E-Mails weder empfangen noch gesendet, weitere Systeme nicht normal betrieben und keiner forensischen Prüfung unterzogen werden. Das hatte zur Folge, dass alle Systeme in der Windows-Domäne (gesamtes Netzwerk) neu aufgesetzt werden mussten. **Leistungshöhe: 140.000 EUR.**



R+V-CyberRisk Police

Die R+V kam mit der R+V-CyberRisk Police für alle Kosten zur Beseitigung auf.





Schutz vor den Folgen technischer Störungen

Leistungsbeispiel: 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. 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 EUR beschafft werden.

Schmerzensgeld und ärztliche Behandlungskosten: weitere 60.000 EUR.



R+V-Betriebshaftpflicht:

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

R+V-D&O-Versicherung:

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





Abwehr von persönlichen Haftungsansprüchen

Leistungsbeispiel 1/2: 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 VN 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 EUR wegen unzureichender interner Kontrollprozesse und Schulungsmaßnahmen
- › Rechtsberatung und Krisenkommunikation verursachen zusätzliche Kosten von 20.000 EUR
- › Schadenersatzforderungen einzelner Kunden (wegen immaterieller Schäden) summieren sich auf 15.000 EUR
- › Ermittlungsverfahren nach § 42 BDSG gegen die Geschäftsführer, für das jedoch unter Einschaltung eines Strafverteidigers die Einstellung des Verfahrens erwirkt wird. Kosten rund 25.000 EUR





Abwehr von persönlichen Haftungsansprüchen

Leistungsbeispiel 2/2: Datenpanne alarmiert Staatsanwaltschaft

Gesamtschaden: 140.000 EUR

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).



Lösung:

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 EUR Anwalts- und Gutachterkosten als Rechtsverteidigungskosten übernommen, 50.000 EUR Schadenersatzforderungen aus der Organhaftung reguliert, 10.000 EUR 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 EUR.





Produkthighlights

Digitale Sicherheit

R+V-CyberRisk Police (MultiLine)

- ✓ All-Risk-Deckung
- ✓ Telefonischer Notdienst (24/7) und umfangreiche Assistance-Leistungen vor sowie nach Eintritt des Versicherungsfalls
- ✓ Versicherungssummen bis 2 Mio. EUR, auf Wunsch 2-fach maximiert

R+V-CyberRisk Police

R+V-Elektronik- versicherung

- ✓ Weltweiter Versicherungsschutz für mobile Geräte
- ✓ Auf Wunsch Mitversicherung Homeoffice
- ✓ Optionale Daten- und Mehrkostenversicherung

R+V-Elektronikversicherung

R+V-Vertrauensschaden- versicherung (MultiLine)

- ✓ Volle – bedarfsgerecht auswählbare – Versicherungssumme bei Schäden durch Betrug (abzgl. SB)
- ✓ Schadenermittlungs- und Rechtsverfolgungskosten sind bis zur Höhe der vollen Versicherungssumme versichert

R+V-Vertrauensschadenversicherung

R+V-Wirtschaftsschutz Police

- ✓ Vereint die Vorteile der R+V-CyberRisk Police und der R+V-Vertrauensschadenversicherung
- ✓ Bündelung zweier vollständiger Produkte in einer Police
- ✓ Versicherungssummen in Cyber bis 5 Mio. EUR (auf Wunsch 2-fach maximiert) und in VSV bis 3 Mio. EUR (2-fach maximiert)

R+V-Wirtschaftsschutz Police



Produkthighlights

Digitale Sicherheit

R+V-Betriebshaftpflicht

- ✓ Für die meisten Branchen überwiegend einheitliches Deckungskonzept mit kompakten Bedingungen für einfache Handhabung bei maximaler Flexibilität
- ✓ Innovative Produktlösungen für weitere attraktive Branchen, u. a. Baugewerbe, Handelsbetriebe, Heil- und Heilnebenberufe, herstellende Betriebe, IT-Betriebe, Alten- und Pflegeheime, erneuerbare Energien, Haus- und Grundbesitzer
- ✓ Schaden-Hotline rund um die Uhr: 0800 533-1205

R+V-Betriebshaftpflicht

R+V-D&O-Versicherung

- ✓ Doppelte Versicherungssumme (1 x Abwehr-/Kostenschutz + 1 x Schadenersatzleistungen)
- ✓ Nachmeldefrist unbegrenzt & unverfallbar für Inanspruchnahmen nach Vertragsende, auch bei Versichererwechsel, inkl. Retirement-Cover
- ✓ Volle Versicherungssumme für Kosten vor Inanspruchnahme (und nicht nur „Abwehrkosten-Zusatzlimit“)

R+V-D&O-Versicherung

R+V-Spezial-Straf-Rechtsschutz

- ✓ Verteidigung gegen den Vorwurf von Straftaten (inklusive Verbrechen) und Ordnungswidrigkeiten
- ✓ Übernahme von angemessenen Vergütungen (Honorarvereinbarungen)
- ✓ Versicherungsschutz auch bei Ermittlung gegen unbekannt/Firmenstellungnahmen

R+V-Spezial-Straf-Rechtsschutz



Top-10-Argumente

Für die Absicherung digitaler Risiken

1. Jedes Unternehmen ist betroffen – nicht nur Konzerne

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

2. Ein einziger Angriff kann existenzbedrohend sein

Durchschnittlicher Schaden nach Ransomware-Angriff:
1,2 Mio. EUR.*

3. Datenschutzverstöße sind kein Kavaliersdelikt

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

4. Die Haftung trifft die Geschäftsleitung persönlich

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

5. Wiederherstellung von Daten und Systemen ist teuer und zeitaufwendig

Datenwiederherstellung, forensische IT-Analysen und Neuinstallation von Systemen kosten schnell fünfstellende Beträge.

6. Ohne IT-Sicherheit kann der Betrieb stillstehen

Produktionsausfall, gesperrte Systeme, kein Zugriff auf Kundendaten – der Betrieb kann tage- oder wochenlang lahmgelegt sein.

7. Kunden und Geschäftspartner erwarten Sicherheit

Viele Auftraggeber verlangen inzwischen Sicherheits- oder Versicherungsnachweise (z. B. bei IT-, Handwerks- oder Beratungsfirmen).

8. Rechtliche Unterstützung ist im Schadensfall entscheidend

Bei Cyberfällen kommen IT-, Datenschutz- und Haftungsfragen zusammen.

9. Umfangreiche Absicherung benötigt Prävention und Versicherung

Immenses Schadenpotenzial vs. verhältnismäßig günstigen Beitrag.

10. Absicherung schafft Vertrauen bei Kunden und Mitarbeitenden

Unternehmen, die professionell mit Risiken umgehen, stärken ihr Image als verlässlicher Partner.



R+V-Tarifrechner

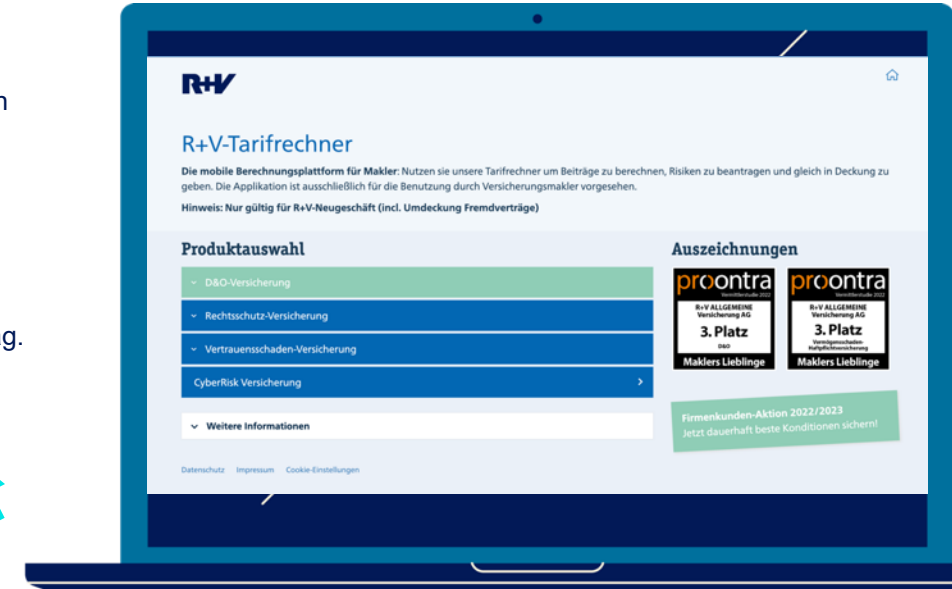
www.do-rechner.de

Einfach clever: Mit nur wenigen Klicks können Sie mit unserem R+V-Tarifrechner nicht nur die für Ihre Kunden passenden Tarife berechnen, sondern den gewünschten Versicherungsschutz auch gleich abschließen – ohne lange Wartezeiten, komplizierte Eingaben und mit direkter Bestätigungsmail samt Deckungsbestätigung.

Das benutzerfreundliche Interface leitet Sie intuitiv durch alle notwendigen Schritte, sodass Sie ohne großen Aufwand zu präzisen Ergebnissen gelangen. Nutzen Sie den Tarifrechner und profitieren Sie von einer effizienten und zeitsparenden Lösung für Ihren Beratungsalltag.



R+V-Tarifrechner





Reputation

Gemeinsam für Ihren Erfolg



Nutzen Sie das Thema Digitale Sicherheit als Einstieg in die vertrauensvolle Beratung mit Ihren Kunden.



Finanzstärke

Wir können in jeder Situation halten, was wir versprechen, und das tun wir auch.



Weitblick

Mit Ihnen und Ihren Kunden entwickeln wir Perspektiven für die Zukunft.



Flexibilität

Genau wie Sie und Ihre Kunden reagieren wir auf Marktentwicklungen und finden schnell und flexibel passgenaue Lösungen.



Makler Mehrwert

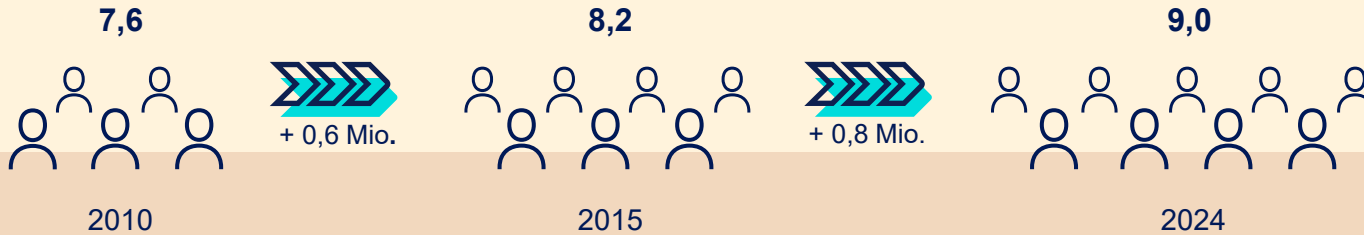
Mit vielen zusätzlichen Services stärken wir Ihnen für nachhaltige Erfolge den Rücken.



Solide, stark, erfolgreich – die R+V im Markt

Auf Wachstumskurs bei Kunden, Verträgen und Beiträgen

Kunden der R+V in Deutschland¹ in Mio. EUR



Versicherte Risiken
in Deutschland in Mio. EUR

+ 3,3 Mio.

20,8

23,6

26,9

2010

2015

2024

Beiträge in Deutschland
in Mrd. EUR (HGB)

+ 25,0 %

9,7

12,8

16,0

2010

2015

2024

Insgesamt
20,9 Mrd.
EUR²

¹ Nach konzernweiter Kundendefinition aus 2024.

² Gesamte R+V Gruppe (HGB) inklusive Rückversicherung und Ausland.



Reputation

Die Vorteile der R+V als Partner für Sie



Wir handeln **miteinander** und füreinander.



Wir bieten finanzielle **Stabilität**:
26,9 Mio. versicherte Risiken für 9,0 Mio. Kunden.



Wir sind einer der größten deutschen **Versicherer**
mit langjähriger Expertise speziell für Firmenkunden.



Die R+V ist traditionell eng verbunden mit **mittelständischen Unternehmen**
aus Industrie, Handel, Handwerk, Gewerbe und Landwirtschaft.



Es gibt ein flächendeckendes Netz an engagierten Betreuern
mit Entscheidungskompetenz **vor Ort**.



Wir sind **aktuell größter Kreditversicherer** in Deutschland und **langjähriger Marktführer** in der Kautionsversicherung.



Reputation

Ausgezeichnet bei Kundenvertrauen und Finanzstärke

Überzeugt
als sichtbarer
Beweis



Exzellenter Service, exzellente Ratings!



Ihr Vertriebsansatz:

Profitieren Sie von diesen starken Bewertungen und überzeugen Sie Ihre Kunden von unserer Qualität. Setzen Sie die Siegel gern auch in Ihrer Kommunikation ein.



Potenziale nutzen

„Ich kenne Potenziale und Verkaufschancen.“

Inhalte

Anspracheanlässe

Checklisten

Erfolgreich ansprechen

Mit dem richtigen Argument zur richtigen Zeit.

Überzeugen Sie Ihre Kunden mit unserem Rundumpaket: Wir liefern Ihnen die passende Ansprache für jede Zielgruppe sowie starke Argumente, um die Produkte in jeder Situation bestmöglich zu präsentieren.





Anspracheanlässe

Wann und wie können Sie zur digitalen Sicherheit ins Gespräch kommen?

- › Aktive Kundenansprache im Rahmen einer ganzheitlichen Beratung
- › Im Rahmen der Firmenanalyse bzw. Jahresdurchsprache
- › In der Bestandskundenansprache: Bieten Sie Rundumschutz für Unternehmen
- › Vor dem Hintergrund aktueller Pressemeldungen (bei R+V-D&O-Versicherung und R+V-CyberRisk Police finden Sie beinahe täglich frischen Input)



„Wie lange hält Ihr Betrieb finanziell durch, wenn die Produktion nach einem Cyberangriff tagelang nicht läuft?“



„Wissen Sie, wer in Ihrem Unternehmen im Falle eines Datenvorfalles haftet – Sie persönlich, Ihre Mitarbeitenden oder das Unternehmen?“



„Was tun Sie, wenn die Bildschirme schwarz bleiben und plötzlich Lösegeld für Ihre Daten verlangt wird?“



„Werden Ihre Mitarbeitenden im Umgang mit digitalen Bedrohungen regelmäßig geschult – und wissen sie, wie sie im Ernstfall reagieren sollen?“



„Welche Maßnahmen haben Sie bisher getroffen, um sich vor Datenverlust oder Systemausfällen zu schützen – und was würde passieren, wenn Ihre IT morgen ausfällt?“



„Wie abhängig ist Ihr Unternehmen heute von funktionierender IT und digitaler Kommunikation?“



Checkliste

Vorsorgemaßnahmen für Unternehmen

Selbst die **beste Police** ersetzt keine solide IT- und Organisationssicherheit.
Unternehmen sollten auf Folgendes achten:

- ✓ 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?

R+V-Notfallkarte

- ✓ Datenschutzprozesse dokumentieren (DSGVO-konform)
- ✓ D&O-Deckung prüfen, falls Organisationspflichten verletzt werden könnten

Auf Folie 48
zum
Ausdrucken
und Abhaken



Argumentationshilfe für das Kundengespräch

Kunde: **Wir sind noch nie gehackt worden.**

Vermittler: „Prima, dass Sie bisher davon verschont geblieben sind. Aber wie können Sie sicher sein, dass das auch künftig so bleibt?“

Kunde: **Wer soll uns denn schon hacken?**

Vermittler: „So wie Sie denken viele unserer Kunden. Tagtäglich werden etwa 6.200 Unternehmen erfolgreich gehackt. Wie können Sie sicherstellen, dass dies bei Ihnen nicht passiert?“

Kunde: **Ich habe einen guten IT-Spezialisten.**

Vermittler: „Eine weise Entscheidung. Deshalb sollte Ihr IT-Spezialist bei dem Termin unbedingt dabei sein, denn ...“

Kunde: **Wir arbeiten mit DATEV, sind bestens geschützt, die interne IT hat keine Internet-Anbindung.**

Vermittler: „Können Sie garantieren, dass betrügerische E-Mails in Ihrem Unternehmen jederzeit erkannt werden?“

Vermittler: „Viele Cyberangriffe nutzen menschliche Fehler als Einstieg. Nicht aus böser Absicht, sondern durch Unachtsamkeit oder Täuschung.“

Mittlerweile wurde **jedes Unternehmen** schon mal gehackt!






Erfolgreich ansprechen. Im Gespräch mit Ihren Kunden

Gesprächseinstiege, mit denen Sie Interesse und die Aufmerksamkeit wecken

Mit diesen Themen und Fragen können Sie bei Ihren Firmenkunden in das Gespräch einsteigen.



Laut dem Bundeskriminalamt lag die Zahl der offiziell erfassten **Cybercrime-Fälle in Deutschland im Jahr 2024 bei über 330.000 Fällen.**¹

Neue Erkenntnisse zeigen: Phishing-Mails werden durch den Einsatz von KI sprachlich gesehen professioneller und persönlicher. Dadurch **steigt das Risiko**, dass die Empfänger sie **nicht als schadhafte Phishing-Mail erkennen.**²

Quellen: ¹ BKA; ² BKA; ³ pwc; ⁴ haufe.

Die Geschäftsleitung ist verpflichtet, ein **angemessenes Schutzniveau gegen Cyber Risiken sicherzustellen.**

Insbesondere:

- › technische Maßnahmen (z. B. Schwachstellenanalyse)
- › organisatorische Maßnahmen (z. B. Vier-Augen-Prinzip bei Zahlungsanweisungen)
- › Mitarbeiterschulung
- › Notfallmanagement³

Kleine und mittlere Unternehmen (KMU) machen laut BKA **rund 80 % der von Ransomware betroffenen Unternehmen** aus.⁴





Kunden unterstützen

„Ich helfe meinen Kunden dabei, die richtige Entscheidung zu treffen.“

Inhalte

Verkaufsunterstützung

Cross-Selling

Sind Ihre Kunden erfolgreich – sind Sie es auch!

Wir unterstützen Sie und machen Sie fit für das Thema Digitale Sicherheit. Von der Kampagne über die passgenaue Verkaufsunterstützung bis zur fachlichen Veranstaltung – hier finden Sie alles übersichtlich zusammengefasst.





Verkaufsunterstützung für Ihre Beratung

Auf diesen Seiten finden Sie verkaufsunterstützende Unterlagen zum Download:

R+V-CyberRisk Police

R+V-D&O-Versicherung

R+V-Vertrauensschadenversicherung

R+V-Spezial-Straf-Rechtsschutz

R+V-Wirtschaftsschutz Police

R+V-Betriebshaftpflicht

R+V-Elektronikversicherung

Informationen zu weiteren Produkten und Lösungen finden Sie hier:

Maklerportal



Maklerakademie

Ihre Weiterbildungen und Online-Seminare

Profitieren Sie von den vielfältigen Möglichkeiten unserer Online-Seminare und erweitern Sie Ihr Wissen zu verschiedensten Themenbereichen.

So können Sie flexibel von zu Hause aus lernen und sich die Zeit selbst einteilen.

[Zur Maklerakademie](#)





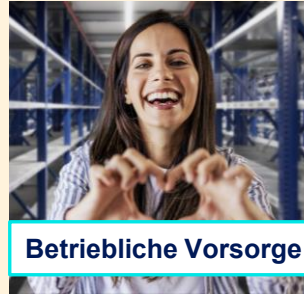
Cross-Selling

Für jedes Bedarfsfeld die passende Lösung



Wir sind nicht nur bei der Absicherung von digitaler Sicherheit der starke Partner an Ihrer Seite. Nutzen Sie unser vielfältiges Portfolio deshalb jetzt auch, um Ihre Kunden mit ganzheitlichen Lösungen für jeden Bedarf zu überzeugen.

Klicken Sie am besten gleich auf die jeweiligen Kacheln und erfahren Sie mehr.



Betriebliche Vorsorge



Energie



Liquidität



Mobilität



Gesundheit



Haftungsrisiken managen



VERSICHERN STATT VERSPRECHEN

Sie geben immer alles.**Wir versichern volle Unterstützung.**

Haken dran, wir haben genau verstanden, was Sie brauchen. Denn als einer von Deutschlands führenden Versicherern unterstützen wir Sie mit attraktiven MehrWerten und liefern Ihnen regelmäßig die besten Services.



Praktische
ToolKits
für Ihre neuen
Vertriebsserfolge



Am Puls der Zeit mit
Speaker Events
zu aktuellen Themen
und unserem Weiter-
bildungsangebot



Reichweite aufbauen,
Marktposition stärken:
**Social Media
inkl. digidor**



**KI/ChatGPT
für Makler** zur
Prozessoptimierung
mit Künstlicher
Intelligenz



Mit dem Leitfaden
„Empfehlungs-
marketing“ den
**Empfehlungs-
Effekt** nutzen



Immer up to date
durch unseren
MaklerTicker

Jetzt abonnieren!

Ausgezeichnet:
Beurteilungen durch
Rating-Agenturen und
die Fachpresse



Umfangreiche Tipps
und Tricks in unseren
Factsheets



Jetzt informieren und gleich profitieren.

makler.ruv.de/mehrwert



Du bist nicht allein.

Checkliste

Vorsorgemaßnahmen für Unternehmen

Selbst die **beste Police** ersetzt keine solide IT- und Organisationssicherheit.

Unternehmen sollten auf Folgendes achten:

- 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
- Multifaktor-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?

R+V-Notfallkarte
- Datenschutzprozesse dokumentieren (DSGVO-konform)
- D&O-Deckung prüfen, falls Organisationspflichten verletzt werden könnten