# Cyberkriminalität: Die unterschätzte Bedrohung

Morgen kann kommen.
Wir machen den Weg frei.

## Risiken, Schäden & Schutz für Unternehmen

*„Wer in Sachen Cybersecurity zögert, spielt mit dem Feuer.“*

Michael Minth, Leiter Vertriebssteuerung bei der R+V Allgemeine Versicherung AG

Volksbanken
Raiffeisenbanken


## Cyberattacken als Unternehmensrisiko Nr. 1

Arbeitsschritte laufen immer häufiger automatisiert ab, firmenbezogene Daten sind in der Cloud zu finden und wir arbeiten von unterschiedlichen Orten aus: Die Digitalisierung erleichtert den Arbeitsalltag in vielerlei Hinsicht – aber nicht nur uns, sondern auch Cyberkriminellen.

**Der Mittelstand ist ein beliebtes Ziel**

102,9 Milliarden Euro – so hoch ist der Gesamtschaden, der sich für deutsche Unternehmen alleine im Jahr 2019 durch Cyberkriminalität ergeben hat. Das zeigt eine **Studie** von Deutschlands Digitalverband Bitkom. Im jährlichen **Risk Barometer der Allianz** waren Cyberrisiken bei den bedrohlichsten Unternehmensrisiken 2019 erstmals gleichauf mit Betriebsunterbrechungen.

Wer an dieser Stelle meint, all das betreffe vor allem größere Unternehmen, der irrt. Besonders kleine und mittelständische Unternehmen geraten nämlich zunehmend in das Visier von Kriminellen. Arztpraxen, Hotels, Restaurants, Einzelhändler und auch Handwerksbetriebe können zum Angriffsziel werden.

Deutschlandweit sind der Bitkom-Studie zufolge bereits 75% der Unternehmen Opfer von Cyberkriminalität geworden. Experten gehen allerdings davon aus, dass die Dunkelziffer der Angriffe deutlich höher ist und viele Attacken nicht gemeldet werden – weil sie lange unentdeckt geblieben sind, man sie nicht zweifelsfrei nachweisen kann oder aus Scham.

**Das Risiko ist groß, das Bewusstsein ist klein**

Problematisch ist: 92% der Unternehmen erkennen das generelle Risiko von Cyberattacken an, doch nur 50% meinen, dass auch der eigene Betrieb bedroht ist. Laut einer **Deloitte-Studie** gehen knapp 50% der Führungskräfte davon aus, nie oder nur selten Ziel eines Cyberangriffs zu werden. Und das, obwohl 5 von 6 Unternehmen gefährliche Lücken in ihrer IT-Sicherheit aufweisen, wie eine **Forsa-Umfrage** im Auftrag des GDV zeigt.

Fühlen Sie sich von diesen Informationen angesprochen? Glaubten Sie bisher auch, dass Ihr Unternehmen zu klein ist, Ihre Daten zu uninteressant sind und Ihr IT-Schutz ausreichend ist? Dann möchten wir Ihnen mit diesem Whitepaper zeigen, dass Sie Cyberkriminelle nicht unterschätzen sollten. Lassen Sie uns gemeinsam Risiken, erwartbare Schäden und Möglichkeiten, sich dagegen abzusichern, ansehen. Damit Sie wissen, wie Sie es potenziellen Angreifern in Zukunft schwerer machen können.

Volksbanken Raiffeisenbanken

## Begriffsdefinitionen

Von „Advanced Persistent Threats“ über „Phishing“ bis hin zu „Ransomware“: Jeder Cyberangriff hat seine eigene, gewiefte Vorgehensweise. Im Folgenden werden einige Methoden kurz erklärt – angesichts der rasanten Entwicklung im digitalen Raum jedoch ohne Anspruch auf Vollständigkeit.

### „Malware“ (Schadsoftware):

Zwei bekannte Formen von Schadsoftware sind Viren und Ransomware. Ein Virus ist ein Code, der sich an eine andere Datei hängt und vermehrt. Wird die betroffene Datei geöffnet, so führt auch der Code seine „Aufgaben“ aus. Je nach Auftrag kann er dann etwa Daten löschen, das Betriebssystem blockieren oder Hardware schädigen.

Ransomware hat die Bezahlung von Lösegeld zum Ziel. Um das zu erreichen, schränkt die Schadsoftware den Zugriff auf ein System zur Gänze ein. Nur wer bezahlt, bekommt – vermeintlich – wieder Zugang. Sicher ist das allerdings nicht.

### „Spam“:

Spam ist ein Überbegriff für Massen-E-Mails, die unaufgefordert an Millionen von Adressen gesendet werden. Neben werblichen E-Mail-Spams sind damit auch Kettenbriefe, Falschmeldungen („Hoaxes“) und durch Viren versandte Nachrichten gemeint. Auch Phishing-E-Mails (siehe nächste Begriffserklärung) fallen in diese Kategorie.

### „Phishing“ und „Spear Phishing“:

Eine E-Mail – vermeintlich von Ihrer Bank – trudelt in Ihr Firmen-Postfach ein. Wegen einer Sicherheitslücke werden Sie dazu aufgefordert, Ihr Passwort zu ändern. Der dazu notwendige Link ist direkt in der Mail zu finden. Wie reagieren Sie? Bei dieser Vorgehensweise handelt es sich um Phishing – einen Betrugsversuch, bei dem persönliche und finanzielle Daten erbeutet werden sollen. Cyberkriminelle verschicken dabei unzählige echt wirkende E-Mails und hoffen, dass ein Empfänger darauf reagiert.

Eine weitere Form dieser Methode ist das Spear Phishing. Dabei haben es die Angreifer auf bestimmte Personen oder Organisationen abgesehen und informieren sich vorab detailliert über diese, um die E-Mail noch glaubwürdiger zu gestalten.

### „Social Engineering“:

Sicherheitstechnisch relevante Daten erlangen, indem menschliches Verhalten ausgenutzt wird – so kann man die Taktik des Social Engineering zusammenfassen. Das vermeintlich „schwächste Glied“ eines Unternehmens in Sachen Sicherheit wird meist zum Ziel der Attacke: Cyberkriminelle geben sich dabei beispielsweise telefonisch als Systemadministrator aus. Um einen Systemfehler beheben zu können, bittet der Anrufer dringend um das Passwort des Opfers. Auch Phishing-E-Mails können auf diese Weise genutzt werden. In der Regel vermitteln die Angreifer das Gefühl, dass sie die Sicherheit einer bestimmten Angelegenheit erhöhen wollen, und machen sich dabei menschliche Eigenschaften wie Vertrauen, Hilfsbereitschaft oder Angst vor Autorität zunutze. Häufig wird tatsächlich die Identität einer bekannten Person – etwa des Vorgesetzten – in Form seiner E-Mail-Adresse gestohlen, um den Druck auf die Empfänger noch zu erhöhen.

### „Drive-by-Downloads“:

Bei Drive-by-Downloads müssen Nutzer nicht erst auf eine Fake-E-Mail oder Ähnliches reagieren: Schon beim Besuch einer infizierten Website wird Schadsoftware heruntergeladen. Weder die Website-Betreiber noch die Nutzer bemerken dies im Normalfall. Die Schadsoftware geht danach auf die Suche nach IT-Sicherheitslücken, um beispielsweise auf Firmensysteme zugreifen zu können.



Volksbanken
Raiffeisenbanken

**„DoS-“ und „DDoS“-Attacken:**

„DoS“ steht für „Denial of Service“. Der Zugang zu einem Server wird dabei blockiert. Häufig geschieht das, indem Server mit Unmengen an Anfragen konfrontiert werden, bis sie diese nicht mehr bearbeiten können und zusammenbrechen. „DDoS“ steht für „Distributed Denial of Service“. Bei diesem „verteilten“ Angriff führt eine Vielzahl von Systemen eine gemeinschaftlich koordinierte Attacke durch.

**„Advanced Persistant Threats“:**

Eine „hochentwickelte, hartnäckige Bedrohung“ ist eine ausgeklügelte Angriffstaktik, mit der Hacker über einen längeren Zeitraum und unbemerkt Zugang zu einem System erhalten. Ihr Fokus liegt meist auf dem Datendiebstahl. Auch kleinere Unternehmen sind nicht vor diesen Attacken gefeit: Häufig werden sie von Cyberkriminellen genutzt, um Zugriff zu ihrem eigentlichen Ziel, nämlich Großunternehmen, zu erhalten.

**„Man-in-the-Middle-Angriffe“:**

Bei Attacken dieser Art wird versucht, an der digitalen Kommunikation zweier oder mehrerer Personen teilzunehmen, ohne dass diese es merken. Cyberkriminelle begeben sich in die „Mitte“ der Unterhaltung und tarnen sich gegenüber dem Sender als Empfänger und umgekehrt. Auf diese Weise verschaffen sie sich Informationen und sind zugleich in der Lage, diese zu manipulieren.

**Attacken auf Kennwörter:**

Wer das Passwort eines Nutzers entschlüsselt, hat nicht nur Zugriff zu Mailprogrammen, sondern im Firmenkontext häufig sogar zu ganzen Systemen des Unternehmens – sensible Daten inklusive. Eine Herangehensweise, um Kennwörter zu erbeuten, ist die Brute-Force-Methode. Dabei versucht ein automatisches Tool so lange unterschiedliche Passwort-Kombinationen, bis die richtige gefunden ist. Eine Form dieser Taktik ist der Wörterbuchangriff, bei dem sämtliche Begriffe des Wörterbuchs, ergänzt um Zahlen und Sonderzeichen, getestet werden.

## Risiken für Unternehmen

Laut einer **Bitkom-Studie** wurden bei 21% der Unternehmen bereits sensible digitale Daten gestohlen. Weitere 20% geben an, vermutlich davon betroffen gewesen zu sein. 17% berichten von digitaler Sabotage der Informations- und Produktionssysteme oder Betriebsabläufe, zusätzliche 20% waren vermutlich betroffen. Wenn es um das Ausspähen digitaler Kommunikation geht, vermuten 30%, Opfer gewesen zu sein – sicher sind sich 13%. Ein großer Risikofaktor ist auch der analoge Angriff: 32% der Firmen berichten von einem Diebstahl der IT- oder Telekommunikationsgeräte.

### Welche Fehler Firmen häufig begehen

Unverschlüsselte E-Mails; Nachrichten mit sensiblen Kundendaten, die an den falschen Verteiler gesendet werden; keine ausreichende Anti-Virus-Software; einfache Authentifizierung und Fahrlässigkeit in Sachen Datenschutz: All das öffnet Cyberkriminellen aktuell Tür und Tor in den deutschen Mittelstand.

Doch nicht immer liegt der Erfolg von Cyberkriminellen an mangelnder IT-Sicherheit: Die größte Sicherheitslücke jedes Unternehmens sind tatsächlich die eigenen Mitarbeiter. Das liegt einerseits daran, dass sie unbedacht mit IT-Systemen, E-Mails, Passwörtern und anderen Daten umgehen. Andererseits fehlt ihnen häufig schlichtweg die Kenntnis der Gefahren im digitalen Raum. Dieses Problem kommt nicht von ungefähr, denn laut dem **Versicherungskonzern** Allianz bieten lediglich 25% der Industrieunternehmen ihren Mitarbeitern Schulungen zur IT-Sicherheit an.

### Diese Geschäftsbereiche sind interessant

Innerhalb von Unternehmen passieren die häufigsten Cyberattacken laut **Bitkom** in der Sparte Marketing und Vertrieb. Besonders attraktiv für Hacker sind außerdem die Bereiche Lager/Logistik, Personalwesen/Human Resources sowie IT, Geschäftsführung/Management und Produktion/Fertigung.

Erschwerend hinzu kommt die ständig fortschreitende Professionalisierung der Cyberkriminellen. „Umfang und Qualität der Angriffe auf Unternehmen haben dramatisch zugenommen. Die Freizeithacker von früher haben sich zu gut ausgerüsteten und technologisch oft sehr versierten Cyberbanden weiterentwickelt – zuweilen mit Staatsressourcen im Rücken", wird Bitkom-Präsident Achim Berg in der Studie zitiert.

## Schäden, die durch Angriffe entstehen können

Die Folgen von Cyberattacken unterscheidet man in Eigenschäden sowie in Fremd- oder Drittschäden. Erstere treffen das Unternehmen direkt, Letztere können es in Form von Ansprüchen durch die Haftpflicht, Klagen etc. einholen.

### Häufige Schäden im Überblick

Eine **Forsa-Umfrage** zeigt, welche Schäden Cyberattacken für Unternehmen am häufigsten verursachen:

1. **Unterbrechung des Betriebsablaufs/der Produktion**
2. **Kosten für Aufklärung und Datenwiederherstellung**
3. **Diebstahl von unternehmenseigenen Daten/Betriebsgeheimnissen**
4. **Image-Schaden**
5. **Lösegeldzahlung**

Durch Betriebsunterbrechungen, die häufigste Folge von Cyberangriffen, stehen deutsche Firmen durchschnittlich 16 Stunden lang still, wie eine **Studie von McAfee** zeigt. Der dadurch entstehende Ertragsausfall kann enorme Ausmaße annehmen.

Und die Liste an Schäden setzt sich noch weiter fort. Dazu gehören unter anderem: Kosten für Anwälte und Beratungshonorare, der Missbrauch ausgespähter Kundendaten und darauf folgende Schadensersatzansprüche, Haftpflichtschäden, Krisenbewältigungskosten, Informationskosten, Vertragsstrafen und vieles mehr.

Das alles zeigt eindrucksvoll, wie groß die Nachwirkungen einer Cyberattacke sind und wie stark die wirtschaftliche Existenz eines Betriebes dadurch gefährdet wird. Expertenschätzungen zufolge müssen selbst kleinere Unternehmen mit einem fünfstelligen Schadensbetrag rechnen.

**Wer haftet für die Schäden?**

Seit 2015 gibt es für die IT-Sicherheit von Betrieben strenge Richtlinien. Betreiber einer kritischen Infrastruktur, Telekommunikationsunternehmen sowie Betreiber von Webangeboten müssen ihre IT demnach am aktuellen Stand der Technik absichern und alle zwei Jahre überprüfen. Maßnahmen müssen sowohl für den Schutz personenbezogener Daten als auch für den Schutz vor unerlaubten Eingriffen in die Infrastruktur getroffen werden. Kommt es trotz aktueller und umfassender Sicherheitsmaßnahmen zu einem Cyberangriff, handelt das Unternehmen nicht schuldhaft.

## Experteninterview zum Thema Cybersecurity

Michael Minth ist Leiter der Vertriebssteuerung bei der R+V Allgemeine Versicherung AG

Michael Minth, Leiter Vertriebssteuerung bei der R+V Allgemeine Versicherung AG, im Gespräch über das unterstützte Risiko und Möglichkeiten, Unternehmen zu schützen.

In Deutschland werden immer mehr Unternehmen zum Ziel von Cyberangriffen. Führungskräfte kennen das Risiko, glauben aber, dass die Gefahr für den eigenen Betrieb nicht so groß ist. Warum?
Manche Unternehmen wiegen sich mittels Firewalls und Anti-Viren-Programmen schlichtweg in falscher Sicherheit. Dazu kommt, dass die möglichen Folgen und Kosten schwer abschätzbar sind. Und viele unterschätzen den Aufwand, den es bedeutet, nach einem erfolgreichen Angriff das Herzstück der Unternehmens-IT wieder aufzubauen. Nach unserer Erfahrung braucht das zwischen drei und zwölf Wochen. Zeit, in der ein Unternehmen nur begrenzt oder gar nicht arbeiten kann.

Vor allem mittelständische Unternehmen treten in den Fokus von Cyberkriminellen. Was macht sie zur beliebten Angriffsfläche?
Der Mittelstand ist ein attraktives Ziel für Kriminelle, weil sich hier mit vergleichbar geringem Aufwand leicht Geld verdienen lässt. Gerade der Erfolg, die Innovationsfähigkeit und Leistungsstärke des Mittelstands sind ein Garant für die Werthaltigkeit der entwendeten Daten. Für ihre Auslösung sind die Unternehmen bereit, hohe Summen zu zahlen. Gleichzeitig ist die IT-Infrastruktur oft schlecht geschützt. Hier haben Kriminelle leichtes Spiel.

Was mache ich als Unternehmer konkret, wenn ich Opfer einer Cyberattacke wurde?
Dann heißt es vor allem, schnell und richtig handeln, damit der Schaden nicht noch größer wird. Ich empfehle jedem, sich im Vorfeld einen Notfallplan zu schreiben – welche Maßnahmen muss ich treffen, wen informieren, was dokumentieren? Im Idealfall hat das Unternehmen eine CyberRisk-Versicherung. In diesem Fall ist der erste und wichtigste Schritt, die Notfall-Hotline der Versicherung anzurufen. Sie stellt den Betroffenen unmittelbar einen Experten zur Seite, der erste Hilfe leistet und hilft, den Schaden zu begrenzen.

Was würden Sie Unternehmen sagen, die sich in Sachen Cybersecurity zögerlich geben?
Die Gefahr, Opfer eines Cyberangriffs zu werden, ist heute leider groß, die Folgen können für Unternehmen schnell existenzbedrohend sein. Denn es gibt kaum Daten, die Cyberkriminelle nicht zu Geld machen können – entweder indem sie sie ausspionieren und weiterverkaufen oder den Zugriff darauf blockieren und Lösegeld fordern. Dazu kommt: Sobald Kunden oder Geschäftspartnern durch den Datendiebstahl ein Schaden entsteht, muss das Unternehmen dafür haften. Wer in Sachen Cybersecurity zögert, spielt also mit dem Feuer.

Wenn ich mich dazu entscheide, meinen Betrieb umfangreich vor Cyberattacken zu schützen, wie gehe ich am besten vor?
Cybersecurity ist eine komplexe Angelegenheit, sie muss ganzheitlich und systematisch eingeführt und betrieben werden. Da ist fachliche Expertise gefordert. Es gibt externe Security-Berater, die gemeinsam mit Unternehmen in Workshops erarbeiten, wie diese ihren Cyberschutz verbessern können. Solche Workshops bietet etwa die VdS Schadenverhütung als Tochterfirma des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) an. Ich empfehle Unternehmen darüber hinaus, einen Informationssicherheitsbeauftragten zu etablieren.

Wie sinnvoll sind Cyberversicherungen und wie unterstützen sie Unternehmen?
Eine Cyberversicherung ist für alle Unternehmen sinnvoll, die mit sensiblen Daten arbeiten – vom Handwerksbetrieb über die Rechtsanwaltskanzlei bis zur Arztpraxis. Sie sichert Schäden im Unternehmen selbst, aber auch bei Partnern und Kunden ab. Und: Sie beinhaltet wichtige Services und Dienstleistungen, stellt zum Beispiel im Schadenfall ihren Kunden unmittelbar einen Experten und mit ihm ein komplettes IT-Notfall-Sicherheitsmanagement zur Seite. Nicht zu vergessen: das Thema Compliance. Es nimmt bei mittelständischen Unternehmen einen immer wichtigeren Stellenwert ein. Damit die Compliance, die immer eine zentrale Aufgabe des Managements ist, in Unternehmen auch nachhaltig betrieben werden kann, müssen die Prozesse in der IT darauf abgestimmt sein.



## Prävention: Das können Sie tun

Das Wichtigste zuerst: Kein Sicherheitskonzept bietet 100-prozentigen Schutz vor Cyberattacken. Doch es gibt viele Schrauben, an denen Unternehmen drehen können, um das Risiko eines Angriffes einzugrenzen.

**Technischer Schutz**

Passwortschutz auf sämtlichen Geräten, Firewalls, Virenscanner und regelmäßige Backups: Der technische Basisschutz ist laut **Bitkom-Studie** so gut wie flächendeckend etabliert. Aber: Er reicht nicht mehr aus. Weitere wichtige Vorkehrungen sind:

- **Regelmäßige Überprüfung der Netzwerke & Schwachstellenanalysen**
- **Einsatz von Penetrationstests & Intrusion Detection Systemen**
- **Verschlüsselung von Netzwerkverbindungen & E-Mails**
- **Erweiterte Verfahren zur Benutzeridentifikation**
- **Elektronische Zugangskontrollen zu Gebäuden und Maschinen**
- **Protokollierung von Zugriffen & erweiterte Verfahren zur Benutzeridentifikation**
- **Verschlüsselung von Datenträgern**
- **Absicherung gegen Datenabfluss von innen**

Um bestmöglich auf den Ernstfall vorbereitet zu sein, sollten Betriebe zudem einen Notfallmanagement-Plan ausarbeiten.

Volksbanken
Raiffeisenbanken

### Organisatorischer Schutz

Neben technischen Methoden zur Senkung der Cyberrisiken gibt es auch organisatorische Faktoren, die dabei helfen, Ihr Unternehmen zu schützen:

- **Festlegung von Zugriffsrechten auf bestimmte Informationen**
- **Regeln für den Umgang mit schützenswerten Informationen**
- **Regeln für die Mitnahme von IT-Geräten auf Dienstreisen**
- **Klare Klassifizierung von Betriebsgeheimnissen**
- **Sicherheitszertifizierungen durch externe Experten**
- **Einführung von Informationssicherheits-Managementsystemen**
- **Regelmäßige Sicherheitsaudits**

Um bestmöglich auf den Ernstfall vorbereitet zu sein, sollten Betriebe zudem einen Notfallmanagement-Plan ausarbeiten.

### Der Faktor Mensch in Sachen Sicherheit

Wie bereits erwähnt gehören Mitarbeiter zu den größten Sicherheitsschwachstellen von Unternehmen. Gleichzeitig sind sie es auch, die eine rasche Aufdeckung eines Angriffs ermöglichen. Firmen sollten daher unbedingt IT-Sicherheitsschulungen der Mitarbeiter forcieren. Sicherheit gehört aber auch in die Chefetage. Das Management ist gefragt, wenn es darum geht, das Bewusstsein für Cyberrisiken zu fördern – idealerweise wird ein Sicherheitsbeauftragter ernannt (Hintergrundprüfungen der Person sind natürlich ein Muss). Um die IT-Sicherheit zu erhöhen, lohnt es sich zudem, auf das Know-how von externen Spezialisten zu setzen.

## Was kann eine Cyberversicherung?

Neben den präventiven Maßnahmen im Betrieb zählen zur Rundum-Absicherung auch die Unterstützung durch Experten im Ernstfall sowie der finanzielle Schutz. Beide Bereiche werden von sogenannten Cyberversicherungen abgedeckt. Laut Deloitte hat aktuell ein Viertel der deutschen Unternehmen eine solche Versicherung abgeschlossen. Der Bedarf dieses Sicherheitsnetzes ist bei jedem Unternehmen gegeben: Das zeigt auch ein Blick auf die Hilfeleistungen, die diese Versicherungen – je nach Anbieter – erbringen.



Volksbanken Raiffeisenbanken

**Soforthilfe im Notfall**

Es ist das Worst-Case-Szenario: Trotz getroffener technischer und organisatorischer Vorkehrungen ist Ihr Unternehmen Opfer von Cyberkriminalität geworden. Der Link in einer echt erscheinenden E-Mail wurde geöffnet und Schadsoftware in Ihr System eingeschleust, oder ein gezielter Angriff auf eine Schwachstelle Ihres IT-Systems wurde ausgenutzt. Ob es sich nun um Datendiebstahl handelt oder Sie keinen Zugriff mehr zu Ihren Systemen haben und der gesamte Betrieb stillsteht: Soforthilfe ist gefragt.

Cyberversicherungen stellen diese in Form der Unterstützung durch Profis zur Verfügung. So sind etwa Cyberspezialisten rund um die Uhr und an sieben Tagen die Woche für Sie erreichbar. Im Schadensfall erhalten Sie zudem gezielte Hilfe von IT-Experten und IT-Forensikern. Auch Experten für die Krisenkommunikation sowie Fachanwälte sind im Ernstfall zur Stelle.

**Finanzieller Schutz**

Steht der Betrieb still oder geraten sensible Daten in die falschen Hände, entsteht schnell ein enormer finanzieller Schaden: Verträge können nicht eingehalten werden, Rechnungen können nicht gestellt werden, ein Nachteil im Wettbewerb stellt sich ein, die Reputation des Unternehmens ist massiv geschädigt, etc.

Cyberversicherungen ersetzen finanzielle Eigen- und Drittschäden, die durch Cyberangriffe verursacht werden. Wird der Geschäftsbetrieb durch eine Attacke unterbrochen, ist es auch möglich, den dadurch entstandenen Ertragsausfall abzusichern. Häufig werden auch Vermögensschäden ersetzt – etwa wenn eine firmeninterne Vertrauensperson unerlaubt und vorsätzlich handelt und dem Unternehmen auf diese Weise schadet.

Welche Schadensfälle Sie für Ihr Unternehmen absichern können, hängt unter anderem von der Branche und vom Jahresumsatz ab. Je nach Bedarf decken zudem Zusatzprodukte Leistungen und Bedürfnisse ab, die über vordefinierte Pakete hinausgehen.

## Die Volksbanken Raiffeisenbanken beraten Sie individuell

Ohne digitale Abläufe geht es in der modernen Geschäftswelt nicht mehr – und das muss es auch nicht. Wichtig ist, Ihr Unternehmen rundum gegen Risiken abzusichern. Das bedeutet zum einen, umfassende Prävention zu betreiben, und zum anderen, für den Ernstfall vorzusorgen und dadurch sofort Unterstützung durch Experten und finanziellen Schutz zu haben.

### Jetzt beraten lassen

**Die Versicherungs-Experten Ihrer Volksbank Raiffeisenbank sind Ihr erster Ansprechpartner zum Thema Cybersicherheit. Wir helfen Ihnen zu analysieren, welche Risiken sich für Ihr Unternehmen ergeben, und stellen sicher, dass Ihre Cyberversicherung alle für Sie notwendigen Fälle abdeckt.**

Volksbanken
Raiffeisenbanken