Cybercrime, Cybersecurity, Cyberversicherung

Die Herausforderungen des Mittelstands im Bereich der Internetkriminalität und Möglichkeiten zur Absicherung

Handelsblatt RESEARCH INSTITUTE

R+V Versicherung

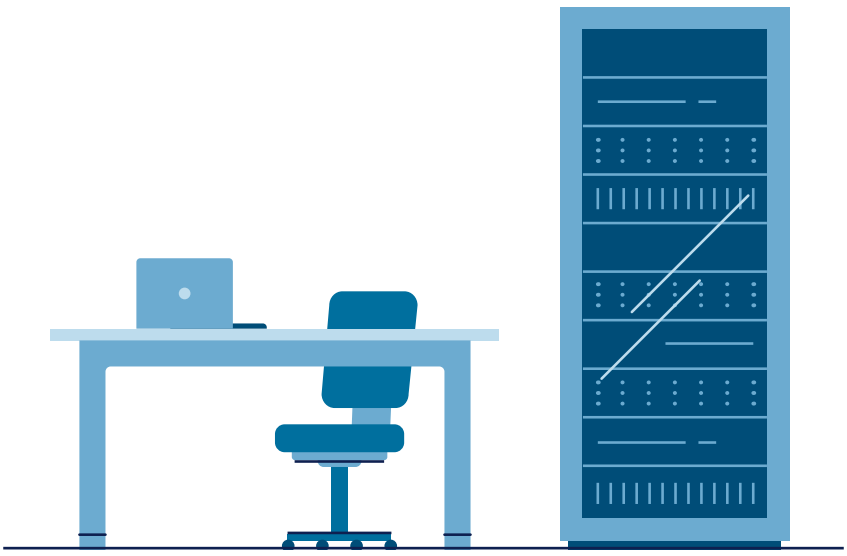
Einleitung

Die Cyberkriminalität ist eine wachsende Bedrohung, in Deutschland wie auf der ganzen Welt. Kriminelle versuchen, Geld zu erpressen oder zu stehlen. Unternehmen versuchen, ihre Konkurrenz auszuspionieren. Aktivistische Gruppen versuchen sich an gezieltem Vandalismus. Und autoritäre Regime versuchen, andere Länder lahmzulegen.

All dies geschieht heute vornehmlich im Internet. Zu den anvisierten Opfern können alle gehören: Privatpersonen und Organisationen, Behörden und Ministerien, große und kleine Unternehmen. Kundendaten, Geschäftsgeheimnisse, Kontoverbindungen – die Liste lukrativer Zielobjekte ist lang. Dabei geht es den Kriminellen meist gar nicht darum, die Informationen selbst zu verwerten, sondern ums Zerstören oder Schröpfen. Und die Schäden, die dadurch entstehen, wachsen stetig. Das Gleiche gilt für die Kosten, die Schutzmaßnahmen hervorrufen.

Zwischen Kriminellen auf der einen sowie Ermittlungsbehörden und Sicherheitsfachleuten auf der anderen Seite herrscht ein permanenter Innovationswettlauf. Die Täter:innen entwickeln fortlaufend neue Methoden und Betrugsmaschen. Und die Gegenseite antwortet mit neuen Gegen- und Schutzmaßnahmen, um diese neuen Geschäftsmodelle so schnell wie möglich zu bekämpfen. Sicherheit muss dabei ständig neu geschaffen werden. Denn mit jeder neuen Technologie und jedem neuen digitalen Angebot entstehen zugleich neue Ansatzpunkte für Angreifer:innen.

Während die Schlagkraft der Cyberkriminellen stetig zunimmt und durch die vielfältigen neuen Möglichkeiten der künstlichen Intelligenz (KI) einen zusätzlichen Schub erfährt, wächst auch der Cybersecurity-Markt. Tatsächlich ist eine Fülle von Angeboten entstanden, die insbesondere Angriffe auf Unternehmen abwehren sollen: Software- und Beratungsunternehmen helfen dabei, Systeme und Netzwerke vor Eindringlingen zu schützen und im Fall eines Angriffs Hilfe zu leisten. Versicherungen decken nicht nur mögliche Schäden ab, sondern bieten umfassende Sicherheitsdienstleistungen an. Und die Unternehmen selbst entwickeln alltägliche Sicherheitsroutinen und stellen Notfallpläne auf. Klar ist: Auch wenn die Gefahren groß sind, ist niemand schutzlos.



Cybercrime-Trends im globalen und nationalen Überblick

Tatsächlich unterliegt die Bedrohungslage einem ständigen Wandel. Klassische Computerviren, die sich selbstständig verbreiten und wahllos Systeme beeinträchtigen, stehen heute nicht mehr im Mittelpunkt. Andere Strategien der Cyberkriminalität hingegen haben in den vergangenen Jahren erheblich an Bedeutung gewonnen. Die folgende Übersicht gibt einen Überblick über die gängigsten Vorgehensweisen.

Die Angriffsstrategien der Kriminellen

Ausnutzen menschlicher Schwachstellen:

Phishing
Mit gefälschten E-Mails, SMS oder Websites wird versucht, an Passwörter oder Kreditkartennummern zu gelangen. Die Angreifer:innen tarnen sich als vertrauenswürdige Institutionen wie Banken oder Paketdienstleister und versuchen, Nutzer:innen zu unüberlegten Handlungen zu bewegen.

Man-in-the-Middle (MitM)
Angreifer:innen schalten sich heimlich in die Kommunikation zwischen zwei Parteien ein, um Daten mitzulesen oder zu manipulieren – etwa durch das Abfangen von Datenverkehr in ungesicherten WLAN-Netzwerken. Das Opfer glaubt, direkt mit der gewünschten Gegenseite zu kommunizieren.

Social Engineering
Hierbei geht es um die gezielte Manipulation von Mitarbeitenden. Angreifer:innen erschleichen sich deren Vertrauen, um an Informationen oder Geld zu kommen. Ein bekanntes Beispiel ist der CEO-Fraud, bei dem vermeintliche Chef:innen um Geldüberweisungen bitten.

Ausnutzen technischer Schwachstellen:

Ransomware (Erpressungstrojaner)
Durch ungesicherte Schnittstellen wird Schadsoftware in einem Computernetzwerk installiert. Diese verschlüsselt alle Daten, sodass kein Zugriff mehr möglich ist. Die Kriminellen fordern anschließend ein Lösegeld (meist in Kryptowährungen) für die Freigabe der Daten.

SQL-Injection
Angreifer:innen schleusen bösartigen Code in Datenbankabfragen ein, um unbefugt Zugriff zu erhalten. Dadurch können sie sensible Daten auslesen, verändern oder sogar löschen. Diese Schwachstelle tritt vor allem bei schlecht gesicherten Web-Eingabefeldern oder Formularen auf.

Zero-Day-Exploits
Hierbei nutzen Angreifer:innen aus, dass es immer eine zeitliche Lücke zwischen der Entdeckung einer neuen Sicherheitslücke und ihrer Behebung durch neue Sicherheitsupdates gibt. Hinweise auf neu entdeckte Lücken werden auf dem Schwarzmarkt für viel Geld gehandelt.

Konzertiertes Angreifen:

Brute-Force-Angriffe
Ein Computerprogramm probiert Tausende Kombinationen aus Benutzernamen und Passwörtern aus, bis der Zugang geknackt ist. Besonders einfache oder kurze Passwörter sind innerhalb von Sekunden anfällig für diese Form des Durchprobierens.

DDoS-Angriffe (Distributed Denial of Service)
Hierbei wird ein Server oder ein Netzwerk gezielt mit einer riesigen Menge an automatisierten Anfragen überflutet, bis das System unter der Last zusammenbricht. Dies führt dazu, dass Internetseiten und Webshops nicht mehr für Kund:innen erreichbar sind und Umsatz verloren geht.

Welche Schäden durch Cybercrime entstehen

In den letzten Jahren sind die Schadenssummen, die auf Cyberkriminalität zurückzuführen sind, stark gewachsen. Längst machen sie den größten Teil jener Schäden aus, die Unternehmen in Deutschland durch Diebstahl, Spionage und Sabotage zu erleiden haben, wie Zahlen des Branchenverbands Bitkom zeigen. Demnach lagen die entsprechenden Verluste im Jahr 2025 bei insgesamt 289 Milliarden Euro, wovon 202 Milliarden auf den Bereich Cybercrime entfielen. Damit sind die Gesamtschäden seit 2021 um 29, die Cyberschäden allerdings um 53 Prozent angewachsen.

Weltweit sind die Schadenssummen im betrachteten Zeitraum sogar um 87 Prozent gestiegen, wie eine Schätzung von Statista Markets Insights zeigt. Demnach wurde die Marke von zehn Billionen US-Dollar bereits 2025 überschritten. Im Jahr 2029 dann könnten es knapp 16 Billionen sein.

Die Strategien der Angreifer:innen sind stets äußerst vielfältig. Eine Bitkom-Umfrage unter deutschen Unternehmen zeigt allerdings, dass Ransomware – also das Verschlüsseln sensibler Daten und das Erpressen von Lösegeldern – mittlerweile der häufigste Angriffsweg ist, gefolgt von DDoS und Phishing.

Wie heftig die Angriffswellen inzwischen sind, zeigt sich auch in der Polizeilichen Kriminalstatistik, die das Bundeskriminalamt herausgibt. Zwar ist die Zahl der registrierten Cyberstraftaten von Angreifer:innen aus Deutschland nach dem Höchststand von 145.000 im Jahr 2021 auf zuletzt 125.000 zurückgegangen. Gleichzeitig gab es aber mit rund 210.000 Fällen fast doppelt so viele Angriffe, die vom Ausland aus auf deutsche Ziele erfolgten.

Gerade bei diesen ist die Ausklärungsquote verschwindend gering: Während die deutsche Polizei immerhin fast jede dritte inländische Straftat aufklären konnte, ist es bei den ausländischen Fällen gerade einmal jede fünfzigste. Dies macht deutlich, wie zentral es für Unternehmen und Privatleute ist, sich selbst zu schützen. Einen kriminellen Angriff im Vorhinein zu vereiteln ist somit deutlich erfolgversprechender als die Strafverfolgung im Nachhinein.

Abb. 01

Deutschland: Wirtschaftliche Schäden durch Angriffe auf Unternehmen

(Diebstahl, Sabotage und Spionage), in Mrd. Euro

Quelle: Bitkom (2025a)[1]

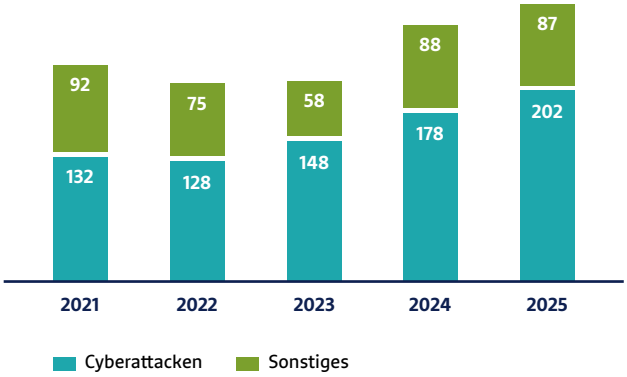


Abb. 02

Weltweit: Cybercrime-Kosten

in Billionen US-Dollar, Prognose

Quelle: Statista (2026)[2]

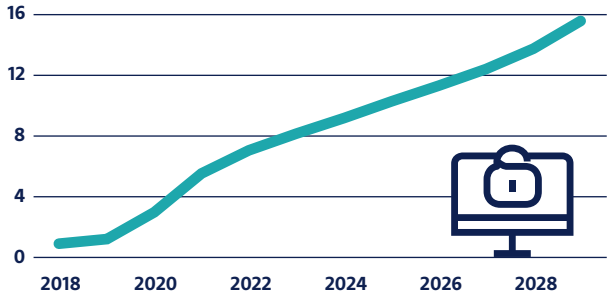
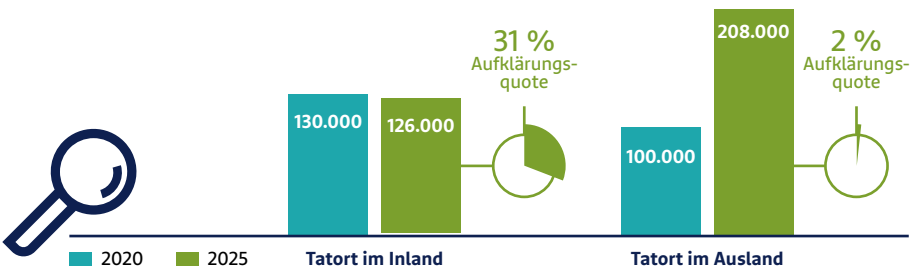


Abb. 03

Deutschland: Polizeilich erfasste Fälle von Cyberkriminalität

Quelle: BKA (2026a)[3]; BKA (2026b)[4]



Wie Unternehmen in mehr Sicherheit investieren

Der Markt für Cybersecurity-Angebote wächst derzeit rasant, gerade in Deutschland. Laut Zahlen des Beratungshauses PAC setzt die IT-Sicherheitsbranche hierzulande inzwischen mehr als zwölf Milliarden Euro pro anno um. Die jährlichen Wachstumsraten liegen dabei bei rund zehn Prozent. Den größten Anteil am Markt haben inzwischen – mit einem Umsatz von rund sechs Milliarden Euro – die Anbieter von IT-Services.

Spiegelbildlich dazu geben die Unternehmen mehr Geld für Cybersicherheit aus. Machten entsprechende Ausgaben im Jahr 2022 noch durchschnittlich neun Prozent der IT-Budgets aus, so waren es 2025 bereits 18 Prozent, wie eine Bitkom-Umfrage zeigt.

Auch Versicherungen spielen für Unternehmen eine immer wichtigere Rolle. Laut Zahlen der Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) und des Gesamtverbands der Versicherer (GDV) lag das Beitragsvolumen von privaten Cyberversicherungen zuletzt grob bei einer Milliarde Euro pro Jahr. Seither dürfte es weiter gestiegen sein.

Abb. 04
Deutschland: Umsatz mit IT-Sicherheit
in Mrd. Euro
Quelle: Bitkom (2025b)[5]

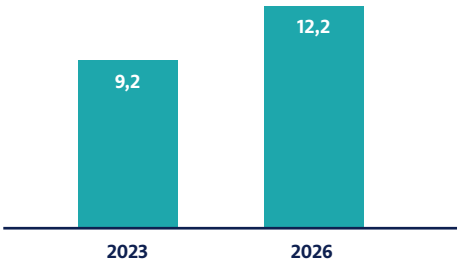
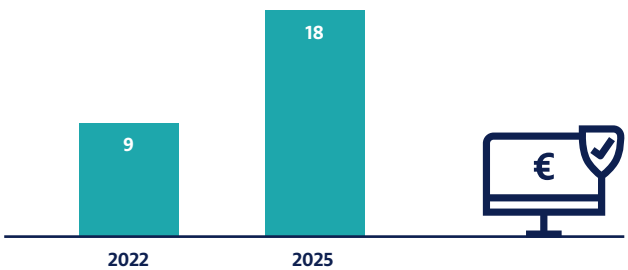
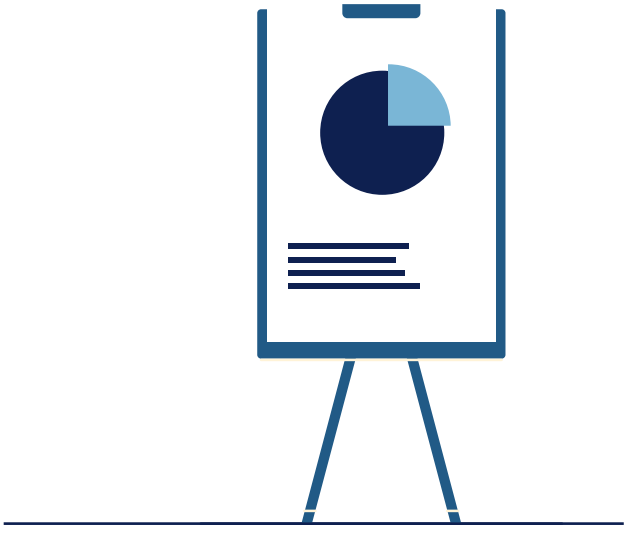


Abb. 05
Unternehmen in Deutschland: Anteil der IT-Sicherheit am gesamten IT-Budget
in Prozent
Quelle: Bitkom (2025b)[5]





EXKURS

Business Email Compromise:
Typischer Ablauf eines – versicherten! – Schadensfalls

Es kann so schnell passieren im hektischen Unternehmensalltag! Im E-Mail-Postfach des Unternehmens taucht eine Rechnung auf. Sie wirkt normal, sie klingt sinnvoll – und schon hat die Buchhaltung das Geld überwiesen. Doch schon kurz danach stellt man fest: Die Rechnung war gefälscht. Das Geld ist auf dem Konto von Kriminellen gelandet.

Business Email Compromise, wie es im Fachjargon heißt, ist eine der häufigsten Maschen, die Cyberkriminelle anwenden. Der Aufwand ist überschaubar, die möglichen Gewinnchancen sind enorm. Selbst wenn nur jeder hundertste Angriff Erfolg hat, kann die Marge beträchtlich sein.

Ist das betroffene Unternehmen versichert, so beginnt nach dem Schadensfall ein umfassender Prozess. Je nach Police übernehmen Versicherungen beispielsweise Kosten für die anwaltliche Begleitung oder für die Forensik.

Von zentraler Bedeutung ist die technische Überprüfung des Tathergangs. Die entscheidende Frage dabei: Was wurde wo manipuliert? War es ein klassischer Betrugsversuch, bei der Kriminelle eine gefälschte, aber echt wirkende Rechnung mit ihrer eigenen Kontonummer drauf geschickt haben? Dann ist es ein Fall für die Vertrauensschadenversicherungen. Diese erstatten dann den mittelbaren Vermögensschaden, hier also den irrtümlich überwiesenen Rechnungsbetrag.

Basiert der Fall dagegen auf einer Manipulation innerhalb des Systems des Unternehmens, wird der Vorgang komplexer. Dann muss geprüft werden, wie umfassend die Kriminellen in die Netzwerke eindringen konnten. Wurden bei dem Sicherheitsvorfall auch sensible Daten entwendet? Haben die Kriminellen weiterhin Zugang zum System? Besteht möglicherweise eine Meldepflicht im Sinne der Datenschutzgrundverordnung? Für solche Situationen sind Cyberversicherungen zuständig. Je nach Police übernehmen sie auch Kosten, die durch Betriebsunterbrechungen, Datenwiederherstellungen oder Schäden bei Dritten entstehen.

Blick
auf den deutschen Mittelstand

Obwohl die Zahl der Cyberangriffe in den zurückliegenden Jahren massiv gestiegen ist, sieht sich die Mehrheit der kleinen und mittleren Unternehmen (KMU) in Deutschland derzeit keiner großen Gefahr ausgesetzt. Dies ist das Ergebnis einer Umfrage unter 255 Entscheider:innen aus dem deutschen Mittelstand, die das Meinungsforschungsinstitut YouGov im Mai 2026 durchgeführt hat. Rund die Hälfte der befragten Unternehmen hat weniger als 50 Mitarbeitende, die andere Hälfte 50 bis 250.

Mit 37 Prozent hält es zwar ein gutes Drittel der Unternehmen für wahrscheinlich oder sogar sehr wahrscheinlich, dass man in den kommenden zwölf Monaten einen gezielten Cyberangriff erleben wird. Allerdings erachten dies 55 Prozent der Befragten als eher oder sogar sehr unwahrscheinlich. Die große Mehrheit der Firmen sieht auch keine wachsenden Gefahren: So sind lediglich 27 Prozent der Unternehmen der Meinung, dass die Wahrscheinlichkeit eines Angriffs zugenommen hat.

Abb. 06

Für wie wahrscheinlich halten Sie einen gezielten Cyberangriff auf Ihr Unternehmen in den nächsten zwölf Monaten?

Anteil der Befragten in Prozent

Quelle: Umfrage des Handelsblatt Research Institute in Zusammenarbeit mit YouGov im Auftrag der R+V Allgemeine Versicherung AG (siehe Text oben)

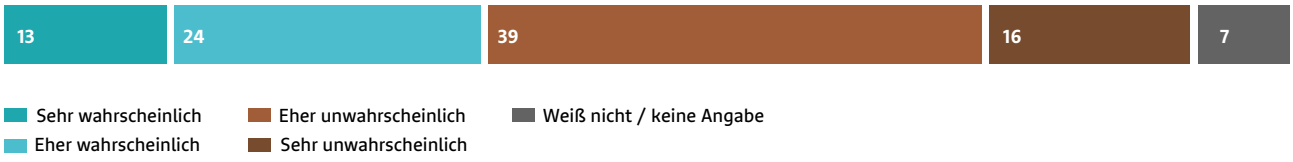
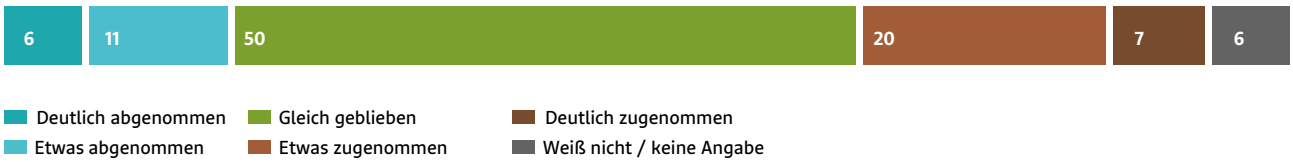


Abb. 07

Wie hat sich die Wahrscheinlichkeit eines gezielten Cyberangriffs auf Ihr Unternehmen in den vergangenen zwölf Monaten entwickelt?

Anteil der Befragten in Prozent

Quelle: Umfrage des Handelsblatt Research Institute in Zusammenarbeit mit YouGov im Auftrag der R+V Allgemeine Versicherung AG (siehe Text oben)



Ein ähnlich großes Ausmaß an Optimismus zeigen die Unternehmen, wenn sie gefragt werden, wie gut sie – ihrer eigenen Einschätzung nach – auf etwaige Angriffe vorbereitet sind. So bewerten mit 65 Prozent knapp zwei Drittel der Befragten das Sicherheitsniveau ihres Unternehmens als gut oder sogar ausgezeichnet.

Dies überrascht, da mit 31 Prozent nur ein knappes Drittel der Unternehmen in den vergangenen zwölf Monaten zusätzliche Investitionen in die eigene Cybersicherheit vorgenommen hat. Allerdings hat auch kaum jemand gekürzt: Nur zwölf Prozent der Befragten geben an, die Investitionen zurückgefahren zu haben.

Abb. 08

Wie beurteilen Sie das Niveau der Cybersicherheit Ihres Unternehmens?

Anteil der Befragten in Prozent

Quelle: Umfrage des Handelsblatt Research Institute in Zusammenarbeit mit YouGov im Auftrag der R+V Allgemeine Versicherung AG (siehe Text auf Seite 7)

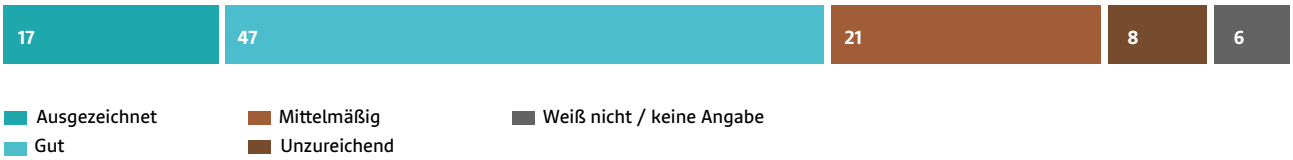
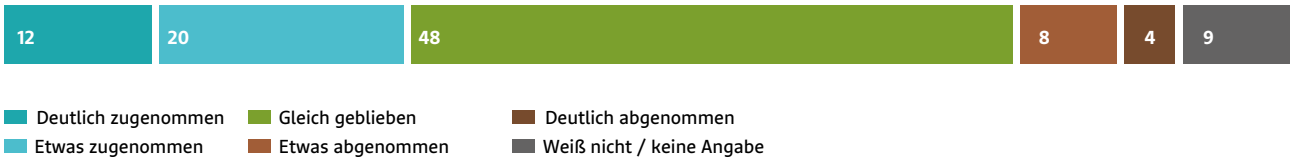


Abb. 09

Wie haben sich die Investitionen in die Cybersicherheit in Ihrem Unternehmen über die letzten zwölf Monate entwickelt?

Anteil der Befragten in Prozent

Quelle: Umfrage des Handelsblatt Research Institute in Zusammenarbeit mit YouGov im Auftrag der R+V Allgemeine Versicherung AG (siehe Text auf Seite 7)



Überdies geben sich die meisten Unternehmen recht selbstbewusst, was das eigene Know-how in Bezug auf das Thema angeht. Befragt nach den Bereichen Cyberkriminalität, Cybersicherheit und Cyberversicherungen, beurteilen jeweils mehr als 60 Prozent den Wissensstand ihres Unternehmens als gut oder sogar ausgezeichnet. Mit 69 Prozent ist dieser Wert beim Thema Cybersicherheit am höchsten. Nur jeweils weniger als ein Zehntel der Befragten bezeichnen ihre Kenntnisse aus unzureichend.

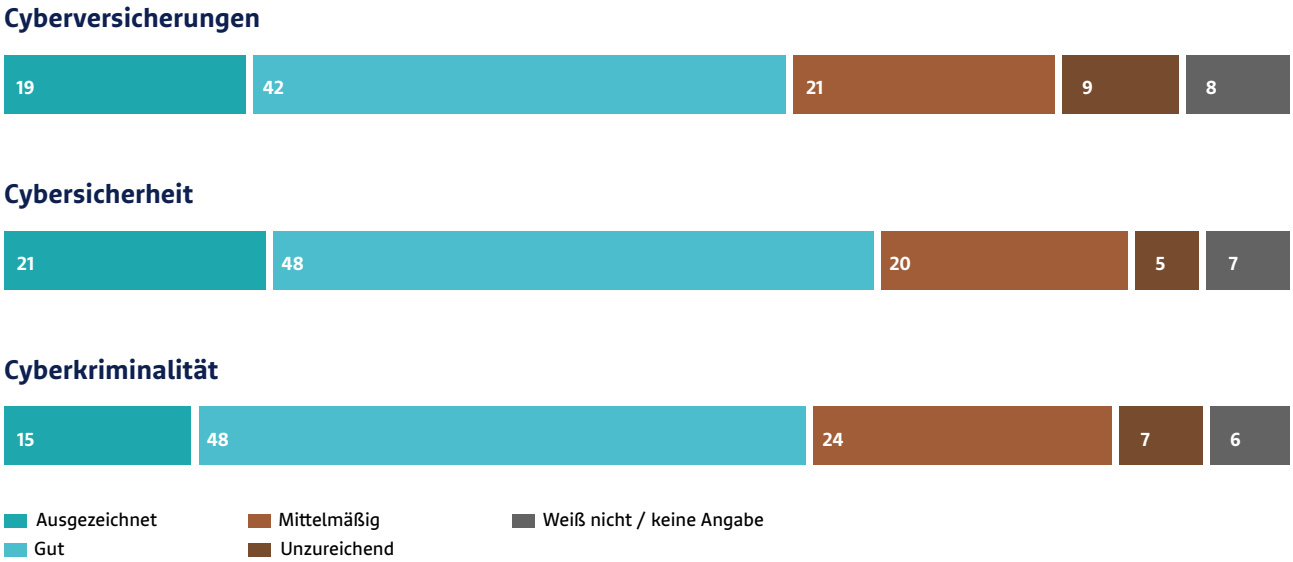
Insgesamt zeigt sich in der Umfrage eine große Diskrepanz zwischen der Zuversichtlichkeit der befragten Unternehmen – und den tatsächlich von ihnen genutzten Sicherheitsvorkehrungen. Dies lässt sich aus den Antworten auf die Frage schließen, welche Maßnahmen konkret von den Unternehmen ergriffen werden, um sich vor Cyberangriffen zu schützen oder um den Schaden bei erfolgreichen Angriffen zu reduzieren.

Abb. 10

Wie beurteilen Sie den Wissenstand in Ihrem Unternehmen im Bereich ...

Anteil der Befragten in Prozent

Quelle: Umfrage des Handelsblatt Research Institute in Zusammenarbeit mit YouGov im Auftrag der R+V Allgemeine Versicherung AG (siehe Text auf Seite 7)



Viele Maßnahmen, die Fachleute heutzutage als zwingenden Bestandteil einer guten Sicherheitsarchitektur ansehen, werden nur von einer Minderheit der Befragten umgesetzt. Dazu gehören beispielsweise das Patchmanagement und die regelmäßigen Update-Routinen, was nur bei 21 Prozent der Befragten vorgesehen ist. Notfallpläne für Cyberangriffe sind lediglich bei 29 Prozent der Unternehmen vorhanden. Und selbst die Multi-Faktor-Authentifizierung nutzt mit 35 Prozent nur ein gutes Drittel.

Regelmäßige Back-ups gehören immerhin für 45 Prozent der Firmen zur Routine. Über eine Firewall verfügen 52 Prozent. Dies ist der einzige Punkt in der Liste, der einen Wert von mehr als 50 Prozent erreicht.

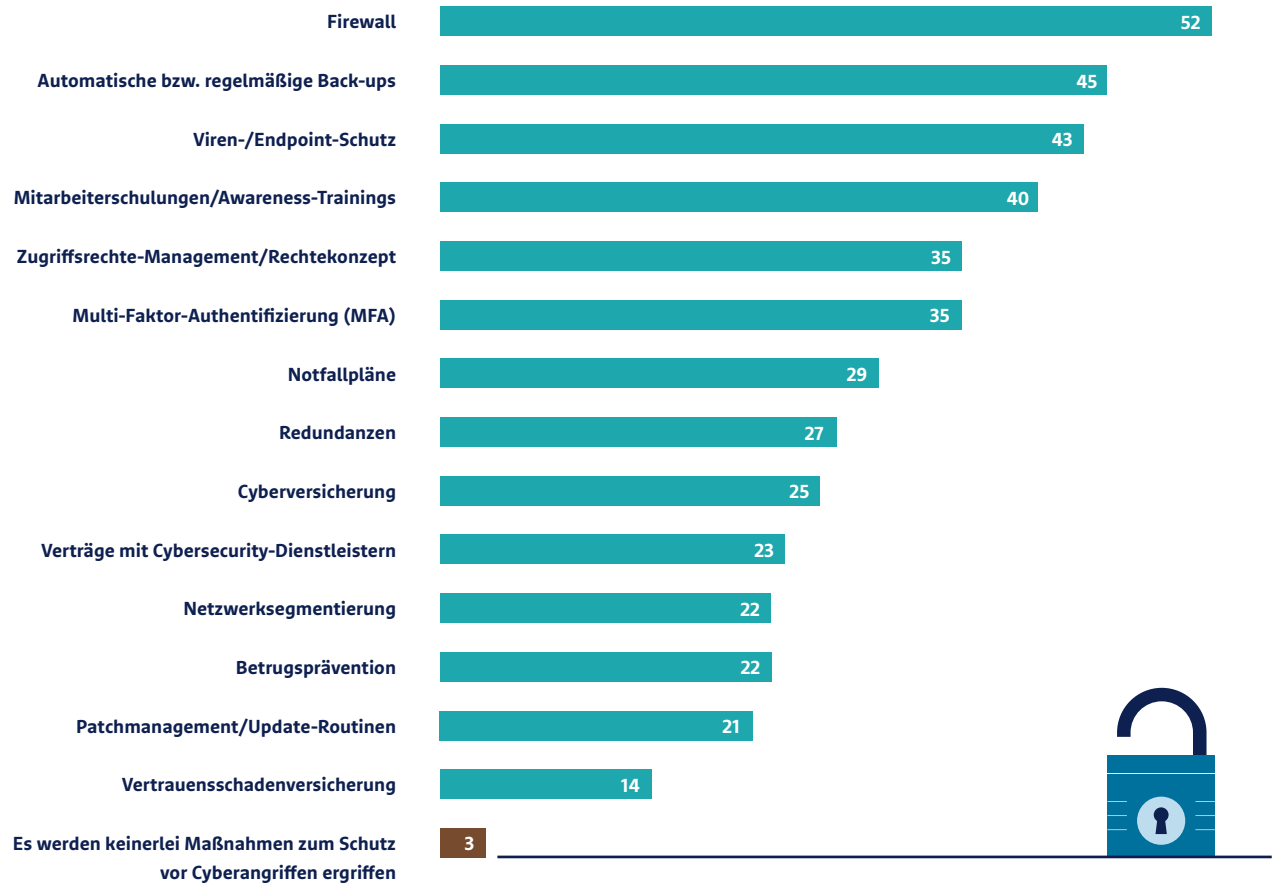
Hinzu kommt, dass nur eine Minderheit der Unternehmen im Schadensfall externe Hilfe in der Hinterhand hat. Lediglich 23 Prozent haben Verträge mit Cybersecurity-Anbietern abgeschlossen. Über eine Cyberversicherung verfügt mit 25 Prozent gerade einmal ein Viertel der Befragten. Bei der Vertrauensschadenversicherung liegt der Anteil sogar nur bei 14 Prozent.

Abb. 11

Welche Maßnahmen werden in Ihrem Unternehmen ergriffen, um sich vor einem Cyberangriff zu schützen beziehungsweise den Schaden bei Angriffen zu verringern?

Anteil der Befragten in Prozent; Mehrfachnennung möglich

Quelle: Umfrage des Handelsblatt Research Institute in Zusammenarbeit mit YouGov im Auftrag der R+V Allgemeine Versicherung AG (siehe Text auf Seite 7)



Maßnahmen für den Umgang mit Cyberangriffen

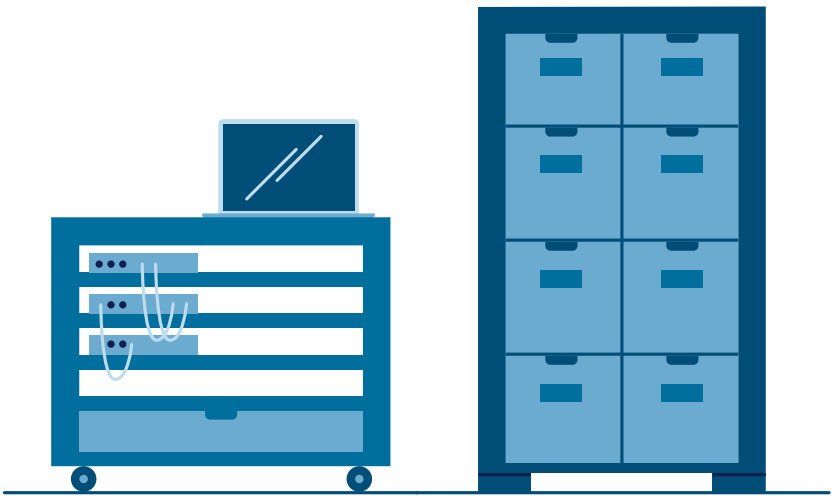
Cyberangriffe gehören heute zu den wichtigsten geschäftlichen Risiken für Unternehmen. Neben klassischen Bedrohungen wie Malware, Phishing oder Ransomware nehmen vor allem Betrugsmaschen wie der CEO-Fraud deutlich zu. Kleine und mittelgroße Unternehmen sind dabei besonders attraktive Ziele für Angreifer:innen: Sie verfügen über wertvolle Daten, agieren mit durchaus hohen Geldbeträgen, sind aber häufig weniger umfassend abgesichert als Großkonzerne.

Umso wichtiger ist ein ganzheitlicher Ansatz aus Prävention, klaren Routinen, professioneller Vorbereitung und finanzieller Absicherung. Die Grundlage eines wirksamen Schutzes für Mittelständler bildet eine klare Liste aus soliden Schutzmaßnahmen. Dazu zählen regelmäßige Software-Updates und ein konsequentes Patchmanagement, starke und individuelle Passwörter sowie die flächendeckende Nutzung der Multi-Faktor-Authentifizierung.

Technisch sinnvoll sind zudem strukturierte Zugriffsrechte, segmentierte Netzwerke und ein wirksamer Schutz der sogenannten Endpoints – also von Laptops, Smartphones und ähnlichen Geräten. Ein besonderes Augenmerk sollte auf die Datensicherung gelegt werden: Back-ups müssen regelmäßig erstellt, getrennt vom Produktivsystem aufbewahrt, idealerweise unveränderbar gespeichert sowie regelmäßig auf Wiederherstellbarkeit geprüft werden.

Da viele Angriffe darauf abzielen, die Unaufmerksamkeit oder Leichtgläubigkeit von Menschen auszunutzen, ist die Sensibilisierung der Mitarbeitenden ein zentraler Baustein für den wirksamen Schutz vor Cyberangriffen. Regelmäßige, praxisnahe Schulungen zu Phishing, Social Engineering und sicherem Arbeiten im digitalen Alltag senken das Risiko erheblich. Klare Prozesse erschweren mögliche Betrügereien zusätzlich: So sollten Zahlungsanweisungen immer von mindestens zwei Personen freigegeben werden müssen. Gleichzeitig sollte die Echtheit hoher Rechnungen immer per Telefon überprüft werden.

Wichtig sind auch Vorkehrungen für Schadensfälle. Ein klar definierter Notfall- oder Krisenplan sollte Zuständigkeiten und Aufgaben festlegen – und regelmäßig aktualisiert und geprüft werden. Dieser Plan muss auch dann verfügbar sein, wenn IT-Systeme nur eingeschränkt arbeiten können. Tatsächlich kann sogar ein Ausdruck auf Papier hilfreich sein.



Angriffe verhindern, Schäden verringern

Neben diesen Basismaßnahmen ist es sinnvoll, die eigenen Systeme im Alltag permanent zu überwachen. Wer sich kein eigenes Security-Team leisten will, kann entsprechende Dienstleistungen an externe Anbieter auslagern – an sogenannte Managed Security Service Provider. Für viele Mittelständler ist dies ein effizienter Weg, mit begrenztem finanziellem Aufwand moderne Sicherheitsstandards umzusetzen.

Ein Beispiel für entsprechende Tätigkeiten ist das sogenannte Security Monitoring: Dabei werden Protokolle von Servern, Firewalls oder Anwendungen regelmäßig auf verdächtige Aktivitäten analysiert – etwa auf ungewöhnliche Log-ins, Datenabflüsse oder verdächtige neue Softwareprogramme.

Von ebenso zentraler Bedeutung ist es, im Schadensfall auf Expert:innen zurückgreifen zu können, die sich auf das sogenannte Incident-Response spezialisiert haben, also die Behebung und Begrenzung von Schäden durch erfolgreiche Cyberangriffe. Entsprechende Dienstleister dämmen Angriffe ein, koordinieren die technischen Maßnahmen und helfen bei der Systemwiederherstellung. Digital-Forensics-Experten analysieren den Angriff, sichern Beweise und klären, ob und welche Daten abgeflossen sind – ein wichtiger Aspekt, wenn es um rechtliche Schritte oder Meldepflichten geht.

Dabei ist Schnelligkeit gefragt, schließlich erfolgen viele Attacken nachts, am Wochenende oder an Feiertagen. So zügig wie möglich sollten Angriffe gestoppt und betroffene Systeme isoliert werden, um eine weitere Ausbreitung zu verhindern. Parallel dazu müssen Beweise gesichert und rechtliche Verantwortlichkeiten fristgerecht erfüllt werden – beispielsweise jene Meldepflichten, die die Datenschutzgrundverordnung (DSGVO) erforderlich macht.

Versicherungen bieten auch Dienstleistungen an

Als Bausteine zur finanziellen Absicherung haben sich auch spezielle Versicherungen etabliert. Zu nennen sind einerseits die Vertrauensschadenversicherungen, die durch Betrug, Diebstahl und Untreue entstandene Schäden abdecken. Dies können eigene Mitarbeiter:innen sein, aber auch externe Geschäftspartner:innen oder Kund:innen – oder unbekannte Dritte. Vertrauensschadenversicherungen sind für typische Cybercrime-Fälle relevant, bei denen gezielt menschliche Schwachstellen ausgenutzt wurden – wie beim Social Engeneering, beim Phishing oder bei Man-in-the-Middle-Angriffen. Meist sind sie nicht auf Cyberkriminalität beschränkt.

Angeboten werden darüber hinaus auch spezielle Cyberversicherungen. Je nachdem, wie umfassend der Leistungskatalog der einzelnen Police ausgestaltet ist, umfasst die Abdeckung die Kosten für IT-Forensik, Systemwiederherstellung, Betriebsunterbrechung, Rechtsberatung, Krisenkommunikation und Haftpflichtansprüche. Für mittelständische Unternehmen liegen die Deckungssummen häufig zwischen einigen Hunderttausend und mehreren Millionen Euro.

Viele Versicherer bieten zusätzlich zur finanziellen Entschädigung eigene Serviceleistungen an, die sie selbst bereitstellen oder vermitteln. Mit in den Policen inbegriffen können beispielsweise 24/7-Notfall-Hotlines, Notfall- und Incident-Response-Teams sowie präventive Sicherheitschecks sein.

Interview mit Torsten Töllner
Geschäftsführer der CyCo Cyber Competence Center GmbH

Herr Töllner, sind die mittelständischen Unternehmen in Deutschland gut geschützt vor Cyberangriffen?

Viele ja, aber die allermeisten nicht. Einen Notfallplan für einen Hackerangriff beispielsweise hat kaum ein Unternehmen in der Schublade liegen. Dabei gehört der zu jeder Sicherheitsstrategie dazu. Es hängt immer davon ab, ob die Unternehmerin oder der Unternehmer eine Affinität zu dem Thema haben – und viele haben die eben nicht. Klar, wenn ein Sanitär-Meister so viel zu tun hat, dass für das Schreiben von Rechnungen nur noch die Samstagabende bleiben, dann hat er wenig Zeit und Lust, obendrein auch noch eine Cybersicherheitsschulung zu organisieren und in den Kalender zu quetschen. Aber sie ist nötig.

Welche Fehler sind besonders typisch?

Viele Unternehmen verlassen sich darauf, dass ihr IT-Dienstleister schon alles für sie regeln wird. Aber es gibt nun einmal gute Gründe für die Regel, dass man IT-Betrieb und IT-Sicherheit organisatorisch voneinander trennen sollte. Ein Handwerker überprüft ja auch nicht selbst, ob er gut gearbeitet hat. Dazu kommen noch allerlei Nachlässigkeiten: Viele fertigen zwar hin und wieder Back-ups an, überprüfen aber nie, ob die überhaupt funktionsfähig sind. Oder sie lassen nur einmal im Monat Software-Updates laufen. Das ist viel zu selten, wenn man bedenkt, dass bei den großen Betriebs- und Softwaresystemen jeden Tag mehr als hundert neue Schwachstellen aufgedeckt werden.

Welche Tricks nutzen Kriminelle besonders häufig?

Zum einen die Erpressungen mit Verschlüsselungen: In Tausenden kleinen Unternehmen in Deutschland brauchen die Mitarbeiterinnen und Mitarbeiter noch immer keinen VPN-Client, um sich vom Homeoffice aus mit den Firmenservern zu verbinden. Genau das ist ein Einfallstor für Kriminelle: Die hacken sich in das System, verschlüsseln die Daten und saugen sie ab. Dann veröffentlichen sie einen Teil davon im Netz, um zu beweisen, dass sie sie besitzen. Und dann schicken sie ein Erpressungsschreiben. Für die betroffenen Unternehmen kommt dann oft noch ein Bußgeld dazu, weil sie die Anforderungen der Datenschutzgrundverordnung nach Sicherheit bei der Verarbeitung nicht erfüllt haben.

Und zum anderen?

Oft müssen die Kriminellen die Tür gar nicht aufbrechen, sondern werden freiwillig eingelassen. Eine gefälschte Rechnung kommt per Mail – und weil sie echt aussieht, wird sie eben beglichen, leider auf das Konto einer Hackerbande. Hier haben wir kein technisches Problem, sondern ein organisatorisches. Abhilfe bringen schlichte Sicherheitsroutinen, so etwa das Vier-Augen-Prinzip für größere Rechnungen. Und wenn ein Geschäftspartner die Änderung seiner Kontonummer per Mail durchgibt, dann muss das immer mit einem telefonischen Rückruf gecheckt werden. Solche Regeln sind übrigens überhaupt nichts Neues.

Es wirkt, als würde es für kleine Unternehmen immer komplexer und teurer, sich vor Cyberangriffen zu schützen …

Nein, das stimmt nicht. Klar, die Zahl der Angriffe nimmt zu, die Risiken wachsen. Trotzdem ist es heute einfacher als früher, sich abzusichern: Es gibt immer bessere Dienstleistungen am Markt, die die Unternehmen kaufen können. Und die Cyberversicherungen decken heute sehr viel ab. Dazu zählen Hilfestellungen verschiedenster Art – wie Risikoanalysen, Beratungen oder Incident-Response-Hotlines. Ja, die Pflege der eigenen Sicherheitsarchitektur kostet Unternehmerinnen und Unternehmer ein paar Tage Arbeit im Jahr. Aber mehr ist es nicht.

Welche Rolle spielt KI heutzutage? Macht sie das Leben von Kriminellen nicht noch einfacher?

Auf der einen Seiten ja: Wer heute Lösegeldangriffe starten will, muss sich nicht mehr ein Hackerheer buchen, das den Code für die entsprechende Schadsoftware schreibt, sondern kann das eine KI machen lassen. Und die früher so typischen Rechtschreibfehler findet man in betrügerischen Mails auch nicht mehr. Auf der anderen Seite profitieren aber auch wir – also die Verteidigung – von der KI. Wir können damit vieles automatisieren, zum Beispiel die Suche nach Schwachstellen in einem System oder die Berücksichtigung neu gefundener Sicherheitslücken. Und auch Schulungsinhalte lassen sich mit KI schnell auf die speziellen Anforderungen eines Unternehmens anpassen.

Endnoten

[1] Bitkom (2025a): Wirtschaftsschutz 2025 - Lagebild der deutschen Wirtschaft. Publikation von Bitkom e.V., Berlin.

[2] Statista (2026): Cybersecurity. Market Insights, online verfügbar unter: https://de.statista.com/outlook/tmo/cybersecurity/weltweit?currency=USD#umsatz, zuletzt abgerufen am 01.09.2026.

[3] BKA (2026a): Polizeiliche Kriminalstatistik - Grundtabelle. Bundeskriminalamt, online verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2025/Bund/Faelle/BU-F-01-T01-Faelle_xls.xlsx?__blob=publicationFile&v=4, zuletzt abgerufen am 01.09.2026.

[4] BKA (2026b): Polizeiliche Kriminalstatistik - Auslandstaten Grundtabelle. Bundeskriminalamt, online verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2025/Bund/Ausland/Faelle/BU-F-01-T01-A-Faelle-Auslandstaten_xlsx.xlsx?__blob=publicationFile&v=3, zuletzt abgerufen am 01.09.2026.

[5] Bitkom (2025b): Deutscher Markt für IT-Sicherheit wächst zweistellig. Pressemitteilung von Bitkom e.V. vom 07.10.2026, online verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Deutscher-Markt-IT-Sicherheit-waechst-zweistellig#ll_unterlagen_pk_cybercrime_2025, zuletzt abgerufen am 01.09.2026.

Impressum

Die Studie wurde im Auftrag der R+V Versicherung erstellt. Die R+V Versicherung hat die Untersuchung fachlich begleitet und die erforderlichen Informationen und Materialien bereitgestellt. Die Verantwortung für Konzeption, Analyse und redaktionelle Aufbereitung der Studie liegt beim Handelsblatt Research Institute.

Handelsblatt
RESEARCH INSTITUTE

Das **Handelsblatt Research Institute (HRI)** ist ein unabhängiges Forschungsinstitut unter dem Dach der Handelsblatt Media Group. Es erstellt wissenschaftliche Studien im Auftrag von Kunden wie Unternehmen, Finanzinvestoren, Verbänden, Stiftungen und staatlichen Stellen. Dabei verbindet es die wissenschaftliche Kompetenz des 20-köpfigen Teams aus Ökonom:innen, Sozial- und Naturwissenschaftler:innen, Informationswissenschaftler:innen sowie Historiker:innen mit journalistischer Kompetenz in der Aufbereitung der Ergebnisse. Es arbeitet mit einem Netzwerk von Partner:innen und Spezialist:innen zusammen. Daneben bietet das Handelsblatt Research Institute Desk-Research, Wettbewerbsanalysen und Marktforschung an.

Konzept, Analyse und Gestaltung
Handelsblatt GmbH
Handelsblatt Research Institute
Toulouser Allee 27, 40211 Düsseldorf
+49 (0)211/887-1100
www.handelsblatt-research.com

Autor: Dr. Hans Christian Müller

Layout: Yasmin Karim, Kristine Reimann

Bilder: R+V

Stand: August 2026

Gendern im Text: Sofern das generische Maskulinum verwendet wird (insbesondere bei Komposita), dient dies allein der besseren Lesbarkeit; grundsätzlich sind alle Geschlechter einbezogen.

R+V

Die R+V Versicherung zählt mit rund 9 Millionen Kundinnen und Kunden zu den größten Versicherern Deutschlands. Als Teil der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken bietet die R+V ihren Kundinnen und Kunden Versicherungslösungen für private und geschäftliche Risiken. Die Produktpalette der R+V-Gesellschaften umfasst Versicherungen für Privat- und Firmenkunden. Die R+V Gruppe erzielte im Jahr 2024 Beitragseinnahmen von fast 21 Milliarden Euro und beschäftigte bundesweit rund 18.000 Mitarbeitende. An ihrem Direktionsstandort in Wiesbaden ist die R+V mit rund 8.000 Beschäftigten der größte private Arbeitgeber.