Mannheimer

Wer hilft Ihrem Unternehmen bei Hacker-Angriffen?

Firmen-Cyberversicherung mit
Soforthilfe und Krisenmanagement.

Ein falscher Klick und nichts geht mehr

Ein einziger gedankenloser Klick auf einen E-Mail-Anhang eines unbekannten Absenders – der Bildschirm wird schwarz und das gesamte IT-System steht still.

Viele Firmen unterschätzen die Gefahr eines Hacker-Angriffs. Fakt ist allerdings, dass bereits ein Drittel der kleinen und mittelständischen Unternehmen Opfer eines Cyberangriffs wurde. Und bei über der Hälfte der betroffenen Firmen kommt es dadurch zu einem Betriebsstillstand.

Ist Ihr Unternehmen bei einem Cyberangriff ausreichend geschützt?

Vermutlich sind Ihre Firewall und der Virenscanner auf dem neuesten Stand und Sie haben die Mitarbeiter sensibilisiert. Alle wissen, wie sie etwa mit E-Mail-Anhängen und Downloads umgehen sollen. Trotzdem kann ein Hacker erfolgreich sein und in Ihre Systeme eingreifen. Der Schaden kann schnell in die Zehntausende gehen.

Schützen Sie Ihr Unternehmen und damit Ihre Existenz mit der Firmen-Cyberversicherung der Mannheimer.

Das kann die Firmen-Cyberversicherung

Falls etwas passiert, ist schnelle Hilfe wichtig. Deshalb steht Ihnen unser **Krisenmanagement** rund um die Uhr zur Verfügung. Experten versuchen beispielsweise, die Ausbreitung des Virus zu stoppen und Ihre Systeme wieder zum Laufen zu bringen sowie Ihre Daten zu retten. **Kosten für Schäden**, die Ihnen selbst durch den Angriff entstehen, sind ebenfalls versichert. Genauso wie **berechtigte Forderungen auf Schadensersatz** – zum Beispiel von Ihren Kunden, wenn Sie nicht vertragsgemäß liefern können oder Kundendaten abgegriffen und missbraucht werden.

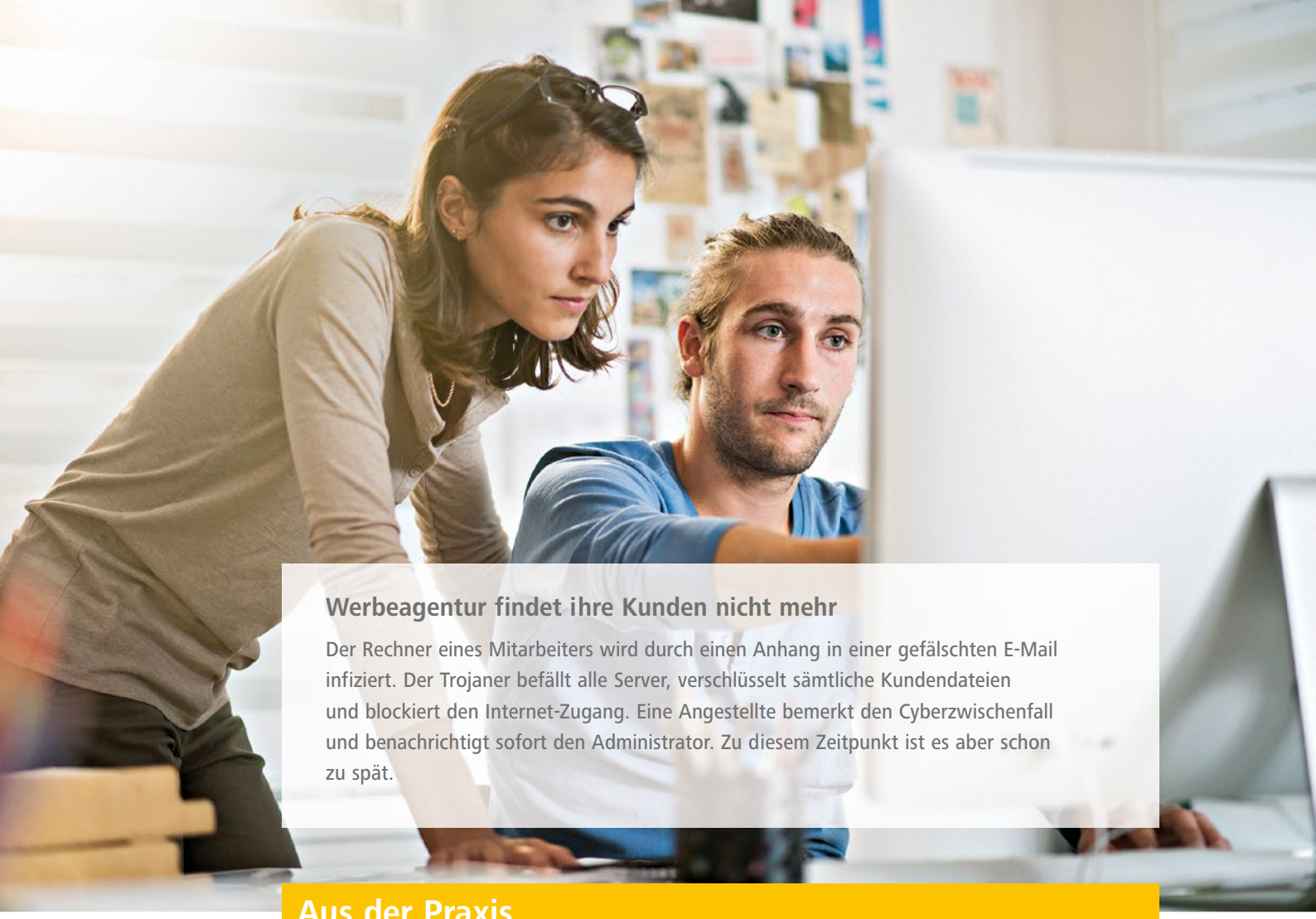
1 **Krisen-management & Soforthilfe**

2 **Übernahme der Kosten für eigene Schäden**

3 **Übernahme der Kosten für Schäden bei Dritten**

Abwehr von unberechtigten Ansprüchen

Damit am besten erst gar nichts passiert, enthält der Versicherungsschutz auch ein sogenanntes **Awareness-Training** (Awareness = Bewusstsein). Praxisnahe Beispiele von Cyberangriffen sorgen dafür, dass Sie und Ihre Mitarbeiter in Sachen „Früherkennung" regelmäßig sensibilisiert werden. Die Trainings sind kostenlos und rund um die Uhr online verfügbar – Sie und Ihre Mitarbeiter entscheiden individuell, wann und wo sie lernen.



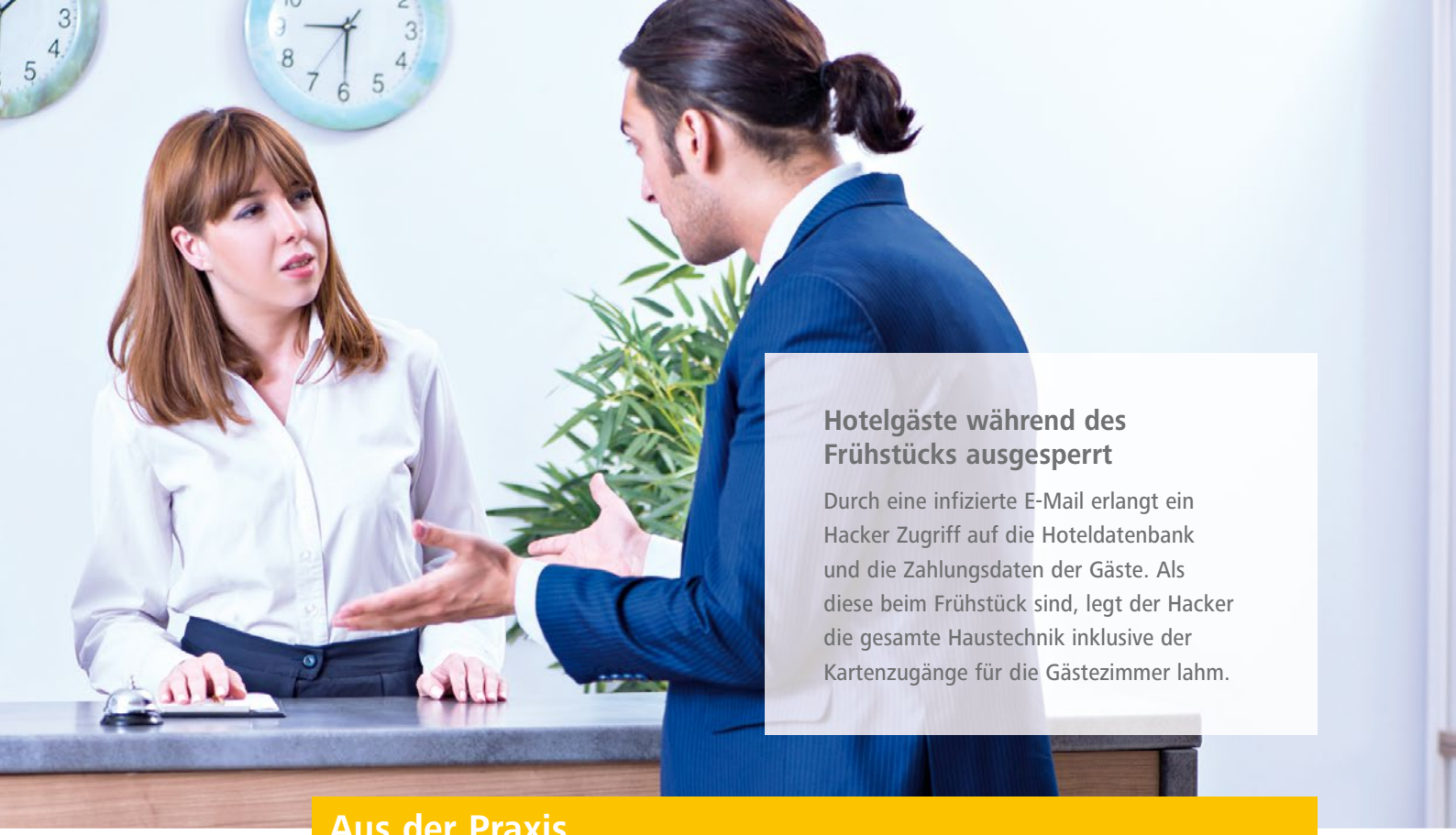
Werbeagentur findet ihre Kunden nicht mehr

Der Rechner eines Mitarbeiters wird durch einen Anhang in einer gefälschten E-Mail infiziert. Der Trojaner befällt alle Server, verschlüsselt sämtliche Kundendateien und blockiert den Internet-Zugang. Eine Angestellte bemerkt den Cyberzwischenfall und benachrichtigt sofort den Administrator. Zu diesem Zeitpunkt ist es aber schon zu spät.

Aus der Praxis

Die Folgen	Die Leistungen	Kosten
■ Die Mitarbeiter können nicht mehr auf Dateien zugreifen. Ein Großauftrag kann nicht erledigt werden.	■ Erste telefonische Notfall- und Krisenunterstützung mit Empfehlungen für Sofortmaßnahmen.	**5.000 Euro**
	■ Beauftragung eines externen Spezialisten, der die Werbeagentur unterstützt und gemeinsam mit dem Administrator den Trojaner unschädlich macht.	**29.000 Euro**
■ Es dauert sieben Tage, bis die Werbeagentur wieder auf alle Daten zugreifen und die Kundenaufträge bearbeiten kann.	■ Ein PR-Berater wird eingeschaltet, weil sich der Vorgang herumspricht. Die Geschäftspartner werden informiert und beruhigt.	**3.000 Euro**
	■ Die Firmen-Cyberversicherung übernimmt die Kosten für die Wiederherstellung der Daten in Höhe von	**7.500 Euro**
	■ Der entstandene Ertragsausfall wird erstattet, das heißt, die fortlaufenden Kosten und der entgangene Betriebsgewinn werden übernommen.	**100.000 Euro**

Versicherungsschutz inklusive aller Deckungserweiterungen.



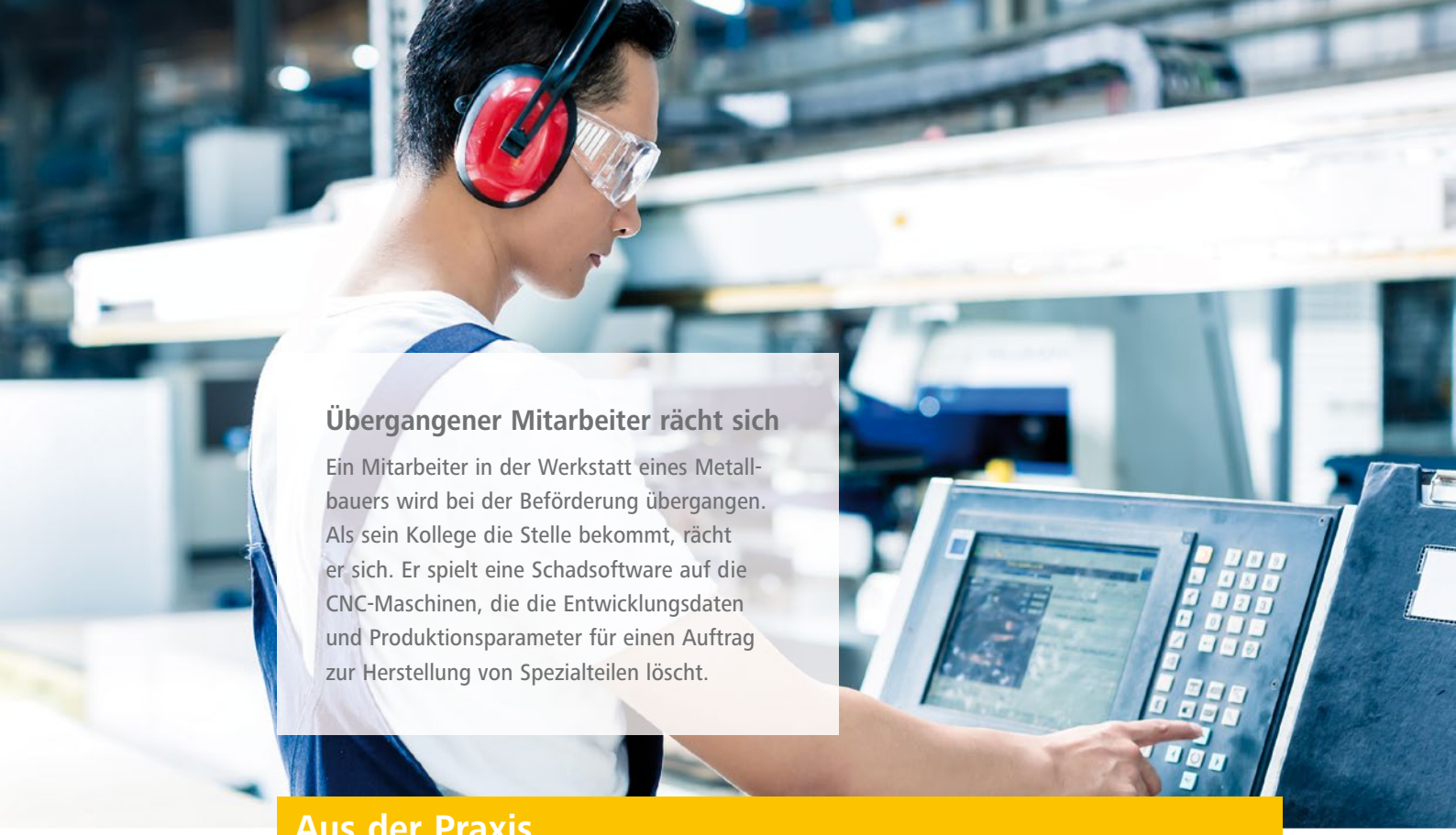
Hotelgäste während des Frühstücks ausgesperrt

Durch eine infizierte E-Mail erlangt ein Hacker Zugriff auf die Hoteldatenbank und die Zahlungsdaten der Gäste. Als diese beim Frühstück sind, legt der Hacker die gesamte Haustechnik inklusive der Kartenzugänge für die Gästezimmer lahm.

Aus der Praxis

Die Folgen	Die Leistungen	Kosten
■ Die Online-Datenbank mit 1.000 Gästedaten und über 400 Zahlungsvorgängen inklusive Kredit- und Bankkartennummern wird an den Hacker übermittelt.	■ Alle 1.000 Kunden müssen per Brief über den Datenmissbrauch informiert werden. Dies sieht Artikel 34 DSGVO vor. Für die Gestaltung, Konfektionierung und Porto entstehen Kosten in Höhe von 1.000 x 5 Euro =	**5.000 Euro**
■ Viele Betroffene rufen im Hotel an und wollen weitere Informationen.	■ Um die Hotelmitarbeiter zu entlasten, wird ein Callcenter mit der Entgegennahme der Anrufe beauftragt. Die Kosten werden von der Firmen-Cyberversicherung übernommen.	**3.800 Euro**
■ Betroffene fordern Schadensersatz, weil sie z. B. die Konten auflösen und weitere Personen informieren müssen.	■ Die Firmen-Cyberversicherung prüft, ob die Ansprüche gerechtfertigt sind. Sollte dies der Fall sein, werden die Betroffenen entschädigt.	
■ Die Hotelgäste können erst zwei Stunden später wieder in ihre Zimmer – nachfolgende Gäste müssen lange auf den Check-in warten. Oder anderweitig untergebracht werden.	■ Der Mehraufwand, den die Gäste haben, zum Beispiel für eine weitere Taxi- oder Bahnfahrt, wird übernommen.	**1.800 Euro**
■ Über den Cyberangriff im Hotel wird in der Presse berichtet. Daraufhin gibt es Zimmerstornierungen.	■ PR-Maßnahmen werden notwendig, um den Ruf des Hotels wiederherzustellen. Kosten für Gestaltung und Schaltung der Anzeige:	**1.500 Euro**

Versicherungsschutz inklusive aller Deckungserweiterungen.



Übergangener Mitarbeiter rächt sich

Ein Mitarbeiter in der Werkstatt eines Metallbauers wird bei der Beförderung übergangen. Als sein Kollege die Stelle bekommt, rächt er sich. Er spielt eine Schadsoftware auf die CNC-Maschinen, die die Entwicklungsdaten und Produktionsparameter für einen Auftrag zur Herstellung von Spezialteilen löscht.

Aus der Praxis

Die Folgen	Die Leistungen	Kosten
■ Die Maschinen arbeiten durch die Schadsoftware nicht mehr und stehen drei Tage still.	■ Bis zur vollständigen Wiederherstellung der Funktionsfähigkeit entstehen eine Betriebsunterbrechung und ein konkreter Ertragsausfall, der von der Firmen-Cyberversicherung übernommen wird.	**16.500 Euro**
■ Die Geschäftsführung vermutet einen Sabotageakt und will wissen, von welchem Rechner die Schadsoftware aufgespielt wurde.	■ Die für die Ermittlung des Täters entstehenden Kosten werden übernommen.	**2.000 Euro**
■ Der Vorfall spricht sich in der Branche herum; weitere Kunden befürchten eine verspätete oder fehlerhafte Lieferung.	■ Um den Ruf des Betriebs zu schützen, werden PR-Maßnahmen getroffen wie Anzeigenschaltungen, positive, klarstellende Berichterstattung.	**5.000 Euro**
■ Ein Kunde erhält seine bestellten Spezialteile nicht rechtzeitig und kann seinen Auftrag nicht wie geplant ausführen.	■ Der Kunde verlangt Schadensersatz wegen vergeblicher Aufwendungen. Er kann einen zur Verladung der Maschinen benötigten Kran nicht mehr rechtzeitig abbestellen und muss den Mietpreis bezahlen.	**1.000 Euro**
■ Ein Kunde kann nicht mehr auf seine Daten in der Cloud zugreifen.	■ Der Kunde hat einen Ausfallschaden, da er seine Produktion einstellen muss.	**5.000 Euro**
■ Der Angriff führt zu einem Schaden an der Hardware.	■ Die Kosten der Wiederherstellung werden übernommen.	**3.000 Euro**

Versicherungsschutz inklusive aller Deckungserweiterungen.

So bekommen Sie Cyber-Risiken in den Griff

Digitale Risiken sind reale Bedrohungen für Ihr Unternehmen. Schützen Sie sich jetzt und warten Sie nicht auf einen Angriff.

Hier ein Überblick über die Leistungen

Service-Kosten	
Soforthilfe – telefonische Notfall- und Krisenunterstützung, Empfehlungen zur Begrenzung des Schadens und technische Sofortmaßnahmen	✓
Ermitteln der Ursache und Feststellen des Schadens durch Sachverständige nach Rücksprache mit dem Versicherer	✓
Prüfung und Erfüllung gesetzlicher Informationspflichten	✓
Maßnahmen zur Erhaltung und Wiederherstellung der öffentlichen Reputation nach einem Angriff durch gezielte Werbung und Krisenkommunikation	✓
Beauftragung eines Callcenters zur Erfüllung gesetzlicher Informationspflichten im Zusammenhang mit der Verletzung von datenschutzrechtlichen Vorschriften	✓
Aufwendungen für erforderliche Maßnahmen zur Vermeidung eines unmittelbar bevorstehenden Schadens	✓
Maßnahmen zur Abwehr oder Minderung eines möglichen Reputationsschadens nach einem öffentlich nur angedrohten Angriff	✓
Überwachung von Kreditkarten- oder Bankdaten Ihrer Kunden bei einem vermuteten Missbrauch und Benachrichtigung der Betroffenen	✓

Eigenschaden	
Betriebsunterbrechung/Ertragsausfall und Mehrkosten	✓
Wiederherstellen von Daten	✓
Analyse eigener Systeme und konkrete Vorschläge zur Verbesserung der Sicherheit nach einem Schadensfall	✓
Übernahme der Aufwendungen zur Minderung des Schadens	✓
Wiederherstellung einer gekappten internen Telefonverbindung oder Übernahme von erhöhten Telefongebühren	✓

Drittschaden	
Erfüllung und Abwehr von Haftpflichtansprüchen Dritter wegen Vermögensschäden	✓
Verletzung von Datenschutzgesetzen – wie Persönlichkeits-, Namens-, Urheber-, Patent-, Kartell-, Wettbewerbsrechts- und Markenrechtsverletzungen	✓
Haftungsfreistellung von Vertragspartnern. Zum Beispiel bei der Verarbeitung von Daten durch externe Dienstleister, die gehackt wurden	✓
Schadensersatzansprüche von Vertragspartnern wegen vergeblicher oder erhöhter Aufwendungen	✓
Abwehrkosten bei behördlichen Verfahren in Verbindung mit einer Informationssicherheitsverletzung	✓

Deckungserweiterungen, die Sie zusätzlich vereinbaren können	
Täterermittlung Ermittlung, von welcher Stelle im Betrieb die „Infektion" ausgegangen ist, und konkrete Empfehlungen zur Sicherheitsverbesserung	
Cyber-Erpressung Krisenmanagement im Falle einer Erpressung	
Cyber-Betrug/Cyber-Diebstahl Ersatz des Geldverlusts, der durch Manipulationen von zum Beispiel Webseiten, Programmen, Online-Banking oder Zahlungssystemen entstanden ist	✓
Versand von Waren Ersatz von Aufwendungen oder Verlusten, weil Waren oder Vorräte aufgrund einer Informationssicherheitsverletzung falsch bestellt, ausgeliefert oder umgeleitet wurden	
Betriebsunterbrechung durch Cloud-Ausfall Ersatz von Schäden, die infolge des Ausfalls externer Dienstleister entstehen	✓
Betriebsunterbrechung durch technische Probleme Ersatz von Schäden, die aus Fehlfunktionen der eigenen EDV-Systeme resultieren	✓
Sachschäden an der Hardware der IT-Systeme Ersatz notwendiger Aufwendungen zur Wiederherstellung der Hardware	✓
E-Payment Vertragsstrafen wegen Verletzung von Sicherheitsstandards beim Zahlungsverkehr mit Kreditkarten/E-Payment	✓

Diese Darstellung gibt einen ersten Überblick über die möglichen Leistungen. Der konkrete Leistungsumfang ergibt sich jeweils aus dem Versicherungsschein und den Versicherungsbedingungen.

Mannheimer Versicherung AG

Augustaanlage 66
68165 Mannheim
Telefon 06 21. 4 57 80 00
Telefax 06 21. 4 57 80 08
service@mannheimer.de
mannheimer.de

Ein Unternehmen des Continentale
Versicherungsverbundes auf Gegenseitigkeit.

HF_056 0124