AUS SCHADEN LERNEN

Von der Bedrohung zur Resilienz: Cyberrisiken gezielt managen

Ausgabe 2/2025

Cyberangriffe sind Alltag – und treffen in starkem Maße auch kleine und mittlere Unternehmen (KMU). Egal welche Branche, egal wie groß: Wer mit sensiblen Daten oder digitalen Prozessen arbeitet, steht im Visier von Cyberkriminellen. Gerade KMU sind oft nicht ausreichend geschützt. Die Folgen eines Angriffs können drastisch sein: Betriebsstillstand, Imageschäden, hohe Kosten. Viele Firmen unterschätzen das Risiko oder sind im Ernstfall überfordert.
Gut, wenn Ihre Kunden dann auf die Firmen-Cyberversicherung der Mannheimer zählen können: Experten sind im Schadenfall schnell zur Stelle, handeln professionell und helfen, Vermögensschäden zu minimieren.

Fall 1 – Ransomware-Angriff

Ein mittelständisches Fertigungsunternehmen aus dem High-Tech-Bereich wurde gezielt mit einer infizierten E-Mail attackiert. Ein Klick – und sogenannte Ransomware legte zentrale Produktionssysteme lahm. Die Folge: Produktionsstopp, Datenverlust drohte.

Der Schaden wurde direkt über die Hotline gemeldet. Unser Partner Allysca übernahm sofort die Koordination der nächsten Schritte. Gemeinsam mit der IT des Kunden und externen Forensikern wurden Gegenmaßnahmen eingeleitet – etwa das Isolieren infizierter Systeme vom Netzwerk, das Zurücksetzen kompromittierter Benutzerkonten sowie das Einspielen sauberer Backups. Schnell, professionell und eng abgestimmt.

Dank dieser Unterstützung und aktueller Backups konnte die Ausbreitung gestoppt und die Produktion neu gestartet werden.

Schadenhöhe: 360.000 Euro

Entschädigung Cyber-Firmenversicherung:

- 240.000 Euro **Betriebsunterbrechung** (Stillstand der Produktionsanlagen, Vertragsstrafen und Verzögerungen in der Lieferkette)
- 120.000 Euro für **IT-Notfallmaßnahmen und Systemreparatur** (Einsatz externer IT-Forensiker, Analyse der Schadsoftware zur Vermeidung weiterer Schäden, Validierung wiederhergestellter Daten auf Integrität)

Erstmaßnahmen im Schadenfall und Serviceleistungen

- Cyber-Experten unseres **Assistance-Dienstleisters Allysca** sind rund um die Uhr einsatzbereit. Sie erfassen alle relevanten Informationen, klären Fragen und geben erste Empfehlungen zur Schadenbegrenzung.
- In enger Abstimmung mit dem Kunden und seinen internen IT-Team übernimmt Allysca die weitere Koordination, damit Ihr Kunde schnellstmöglich wieder handlungsfähig wird.

Für eine zügige Schadenbearbeitung bitten wir Sie, Ihre Kunden darauf hinzuweisen, Schadenmeldungen **ausschließlich** telefonisch über die **0621. 457 55 55** vorzunehmen – E-Mail-Meldungen können zu Verzögerungen führen.

Fall 2 – Angriff über einen unsicheren VPN-Zugang

Unser Kunde – eine Rechtsanwaltskanzlei – wurde über ein veraltetes VPN-System Ziel eines Cyberangriffs. Die Angreifer nutzten gestohlene Zugangsdaten, um sich unbemerkt ins interne Netzwerk einzuschleusen und vertrauliche Mandantendaten zu kopieren.

Wenige Tage später tauchten sensible Dokumente auf einer Leak-Plattform im Darknet auf – darunter laufende Vertragsverhandlungen mit einem internationalen Mandanten.

Die Folgen waren gravierend: Der Mandant beendete die Zusammenarbeit, weitere Geschäftspartner forderten Auskunft über die Datenschutzmaßnahmen der Kanzlei. In der Folge musste die Kanzlei kurzfristig einen externen Datenschutzexperten hinzuziehen und ihre IT-Sicherheitsstruktur umfassend prüfen lassen.

Schadenhöhe: 180.000 Euro

Entschädigung Cyber-Firmenversicherung:

- 20.000 Euro **IT-Notfallmaßnahmen und Ursachenanalyse** (48 Stunden durchgehende Arbeit der externen IT-Dienstleister)
- 50.000 Euro **Betriebsunterbrechung** (verschobene Mandate und ausgefallene Honorareinnahmen während der Wiederherstellung der IT-Systeme)
- 25.000 Euro **Datenschutz und rechtliche Pflichten** (Meldepflicht nach DS-GVO, Mandantenbenachrichtigung, Rechtsberatung durch externe Experten)
- 40.000 Euro **PR- und Reputationsschutz** (Krisenkommunikation, Mandantenbindung und Wiederherstellung des Vertrauens durch externe Berater)
- 45.000 Euro **Sicherheitsmaßnahmen und IT-Optimierung** (Härtung der IT-Systeme, Implementierung neuer Sicherheitsrichtlinien, externe Beratung)

AUS SCHADEN LERNEN

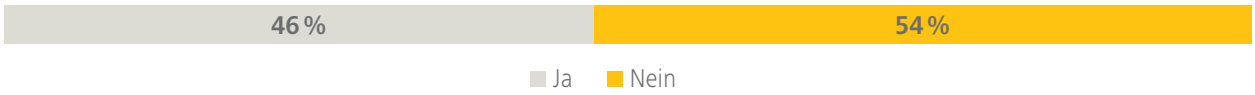
Von der Bedrohung zur Resilienz: Cyberrisiken gezielt managen

Cyber-Risiken im Blick – ein Leitfaden für kleine und mittlere Unternehmen

Ein effektives Risikomanagement in Unternehmen erhöht die Widerstandsfähigkeit gegenüber Cybergefahren.

- **IT-Abhängigkeiten erkennen:** wichtige IT-Systeme und Daten identifizieren
- **Cyberbedrohungen kennen:** Risiken wie Ransomware oder Rechnungsbetrug verstehen. Unser Outside-in-Scan informiert Firmen über Schwachstellen ihrer IT-Infrastruktur. Das Tool unseres Dienstleisters cysmo nutzt nur öffentlich zugängliche Informationen und greift niemals das IT-System des Kunden an. Den Scan führen wir nur durch, wenn wir den Kunden im Vorfeld darüber informiert haben. Erkenntnisse daraus können sowohl für Ihre Beratung und noch mehr für Ihren Kunden hilfreich sein.
- **Ausfallauswirkungen bewerten:** betriebliche Abläufe ohne IT analysieren
- **Schadenszenarien durchspielen:** potenzielle Kosten für Krisenmanagement und Ertragsausfälle einschätzen
- **Präventive Maßnahmen umsetzen:** Sicherheitsrichtlinien, regelmäßige Backups und Mitarbeiterschulungen etablieren. Über unsere Firmen-Cyberversicherung haben Unternehmen kostenlosen Zugang zu einem Awareness-Training (Awareness = Bewusstsein) mit Praxisbeispielen. Der vereinbarte Selbstbehalt kann sich im Schadenfall um 250 Euro reduzieren, wenn mindestens 70 % der Mitarbeiter das Training mit einem Zertifikat abgeschlossen haben.
- **Updates und Sicherheitspatches:** Regelmäßige Aktualisierungen sorgen dafür, dass bekannte Sicherheitslücken geschlossen werden
- **Sichere Zugänge:** VPNs und Multi-Faktor-Authentifizierung nutzen.
- **Netzwerksegmentierung und Zero Trust:** Netzwerk in Sicherheitszonen aufteilen und Zugriffe stets überprüfen

Hat das Unternehmen einen schriftlichen Notfallplan oder eine vertragliche Vereinbarung mit dem IT-Dienstleister für den Fall eines IT-Ausfalls?



Quelle: repräsentative Forsa-Umfrage unter 300 mittelständischen Unternehmen 2024

- **Backup- und Notfallpläne:** regelmäßige Backups und klare Notfallstrategien implementieren. Unser digitaler Cyber-Dialog mit Underwritern unterstützt Unternehmen bei vertiefenden Fragestellungen sowie der Erarbeitung und Einführung eines Notfallplans. Wir unterstützen Sie dabei, Ihren Kunden eine strukturierte Herangehensweise zur Entwicklung ihrer Cyber-Resilienz und zur Kontrolle von Cyberrisiken aufzuzeigen.

Hinweise für den Vertrieb

Stellen Sie Ihren Kunden die drei Bausteine der Cyberversicherung vor:

- Krisenmanagement und Soforthilfe
- Übernahme der Kosten für eigene Schäden
- Übernahme der Kosten für Schäden bei Dritten. Abwehr von unberechtigten Ansprüchen

Bei Fragen rund um das Thema Cyberversicherung und den enthaltenen Serviceleistungen, sprechen Sie Ihren Maklerberater an.

AUS SCHADEN LERNEN

Von der Bedrohung zur Resilienz: Cyberrisiken gezielt managen

Weitere Informationen

- Wie gut ist die IT-Sicherheit Ihres Kunden? Empfehlen Sie den Check.
- Merkblatt zum Verhalten bei einer Cyber-Attacke
- Broschüre Cybersicherheit für KMU vom Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Die Transferstelle Cybersicherheit im Mittelstand unterstützt kleine und mittlere Unternehmen, Handwerksbetriebe und Start-ups kostenfrei bei der Prävention, Detektion und Reaktion auf Cyberangriffe.

Die dargestellten Schadenfälle sind nicht allgemeingültig. Art und Höhe der erbrachten Leistungen sind abhängig von schadenrelevanten Gegebenheiten und den jeweiligen vertraglichen Vereinbarungen.

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

ASL 0625 EV