FINANZ CHEF24

Pressemitteilung

Cyber-Security: Neues Gesetz ab Herbst treibt IT-Mindestvorgaben

(München, 09. April 2024) Obwohl auch kleine Unternehmen zunehmend unter Hackerangriffen leiden, haben sie grundsätzlich bessere Chancen, überhaupt eine Police zu erhalten. Bei Unternehmen mit über 10 Millionen Euro Umsatz wird mittlerweile rund jeder zweite Antrag wegen unzureichender IT-Sicherheit abgelehnt. Ab Oktober 2024 wird der Abschluss einer Cyberversicherung für Unternehmen möglicherweise noch schwieriger, weil dann die zweite Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) in Kraft tritt. Darauf weist der Gewerbeversicherungsmakler Finanzchef24 (www.finanzchef24.de) hin.

Vielen nicht bewusst: CEO und IT-Leiter können persönlich haften

„Jedes Unternehmen sollte regelmäßig Stresstests durchführen und einen Notfallplan aufstellen“, rät Payam Rezvanian, Mitglied der Geschäftsleitung bei Finanzchef24. Nach seinen Erfahrungen ist das Bewusstsein für das Thema grundsätzlich vorhanden – aber vielen kleinen Unternehmen fällt der erste Schritt schwer. Unternehmen sollten daher zunächst kritische Prozesse und Risiken im Kerngeschäft quantifizieren. „Zudem müssen gerade Geschäftsführer von kleineren Unternehmen begreifen, dass Informationssicherheit nicht nur eine Aufgabe der IT-Abteilung ist, sondern des Geschäftsführers“, sagt Rezvanian. CEO und IT-Leiter können persönlich haftbar gemacht werden, wenn es zu ernsthaften Schäden kommt – und wenn das Unternehmen weder eine Cyberversicherung abgeschlossen, noch sich adäquat geschützt hat.

Tägliche Datensicherung und sinnvolle Rechteverwaltung sind Pflichtprogramm

Finanzchef24 rät Kleinst- und Kleinunternehmen, einen Angebotsprozess für IT-Cyberversicherungen zu durchlaufen – um im Zuge dessen die Mindestanforderungen ins eigene Unternehmen zu übertragen. Einige Versicherer bieten sogenannte Antragsmodelle an: Dort können Unternehmer Angaben zur eigenen IT-Sicherheit machen und prüfen, ob sie eine Versicherung erhalten würden. So wird einerseits verhindert, dass Anträge abgelehnt werden und andererseits erhält das Unternehmen Hinweise auf wesentliche IT-Schwachstellen. Das ebnet den Weg für einen neuen Antrag mit verbesserter IT-Sicherheit. Als Mindestvoraussetzung werden meist Kriterien gefordert wie die Frequenz der Datensicherung, Sicherheitstrainings für Mitarbeiter, 2-Faktor-Authentifizierung und ein angemessenes Konzept der

Rechtevergabe. „Im Prinzip geht es beim Thema Cybersicherheit darum, den Schadenfall durch technische und organisatorische Lösungen so weit wie möglich in die Zukunft zu verschieben und das Restrisiko an eine Cyberversicherung abzugeben“, erklärt Frank Gottheil, Senior Firmenkundenberater bei Finanzchef24.

Cybersicherheit kein einmaliges Projekt, sondern fortlaufender Prozess

Versicherer setzen wegen der steigenden Schadenfälle Firewalls ebenso voraus wie einen aktuellen Stand der IT-Technik. Darüber hinaus passen Versicherer fortlaufend ihre Konditionen an. Neben oft steigenden Prämien, und niedrigeren Deckungssummen erhöhen sie sukzessive die generellen Anforderungen an die IT-Sicherheit. Spätestens ab Oktober 2024 ist mit einer weiteren Verschärfung zu rechnen. Dann tritt in Deutschland die NIS-2-Richtlinie in Kraft. Bei Verstößen drohen Bußgelder bis zu 10 Millionen Euro oder zwei Prozent des Jahresumsatzes. „Zwar gilt die Richtlinie nur für Unternehmen, die mehr als 50 Mitarbeiter beschäftigen, mehr als 10 Millionen Euro Umsatz erwirtschaften und in kritischen Wirtschaftsbereichen tätig sind. Allerdings kommen gesetzliche Vorgaben früher oder später in den Verträgen an“, weiß Gottheil.

Kosten durch Betriebsunterbrechung sind nicht zu unterschätzen

Eine Cyberversicherung zu prüfen, lohnt laut Finanzchef24 nicht nur als erster Stresstest, sondern vor allem in Ernstfall. Sie übernimmt im anerkannten Schadenfall die Kosten für die IT-Wiederherstellung, die Kundenkommunikation, Benachrichtigung der Kunden, Interessenten und Zulieferer sowie die Betriebsunterbrechung. „Im Schnitt dauert eine Betriebsunterbrechung nach einem schweren Hackerangriff drei bis sechs Wochen. In dieser Zeit fällt einerseits das Geschäft aus, anderseits laufen weiterhin die Fixkosten etwa für die Gehälter“, sagt Gottheil. Die Wiederherstellung der IT-Daten wird in der Regel mit 30 bis 50 Prozent des IT-Wertes angesetzt. Nicht zu unterschätzen sind die Benachrichtigungskosten: Laut DSGVO sind Unternehmen nach einem Cyberangriff verpflichtet, alle betroffenen Personen zu benachrichtigen. Die Kosten dafür liegen bei 20 bis 40 Euro je personenbezogenem Datensatz. Hinzu kommen Kosten für die weitere Kommunikation wie Öffentlichkeitsarbeit, um mögliche Reputationsschäden zu minimieren. Immer weniger Versicherer sind indes bereit, für Lösegeldforderungen aufzukommen.

Grundsätzlich rät Finanzchef24 zur eigenen Cyberversicherung, in der sich Risiken modular versichern lassen. Deutlich günstiger und ebenfalls eine einfache Option können Schutzbriefe darstellen, die im Ernstfall vor allem beratend unterstützen. Weniger ratsam seien an die Betriebshaftplicht gekoppelte Zusatzverträge. Grundsätzlich empfehle sich der Gang zum Makler, der einen breiten Marktüberblick habe und mit Fachwissen beraten könne.

Über Finanzchef24

Finanzchef24 definiert den Markt der Gewerbeversicherungen für Einzel- und Kleinunternehmer (SME) neu. Das Münchener Insurtech vereint digitale Kommunikation und Prozesse mit der Kompetenz des Versicherungsspezialisten und der

Unabhängigkeit einer Plattform. Unternehmer erhalten so die für sie optimale Absicherung und können sich voll auf ihr Geschäft konzentrieren. Über 40 Versicherer machen ihre Lösungen effizient und zielgenau den richtigen Kunden zugänglich. Das Konzept von Finanzchef24 hat bereits 50.000 aktive Kunden überzeugt. Mehr unter www.finanzchef24.de

Unternehmenskontakt
Finanzchef24 GmbH
Hohenlindener Str. 1
81677 München
Tel.: +49 89 716 772 700
Fax: +49 89 716 772 800
E-Mail: presse@finanzchef24.de

Pressekontakt
SCRIVO PUBLIC RELATIONS
Ansprechpartnerin: Katja Kraus
Lachnerstraße 33
80639 München
Tel.: +49 89 45 23 508 13
Fax: +49 89 45 23 508 20
E-Mail: katja.kraus@scrivo-pr.de
Web: www.scrivo-pr.de