FINANZ CHEF24

Pressemitteilung

# Hackerangriff – der 5 Schritte-Notfallplan für Unternehmer

**Cyber-Resilienz – potenzielle Bedrohungen proaktiv erkennen und Notfallplan vorbereiten. IT-Notfallkarten sollten angelegt und Sicherheitslücken fortlaufend gesucht werden.**

**(München, 23. Juli 2024.).** Abgesagte Operationen und Flüge, geschlossene Supermärkte, Millionenausfälle: Unternehmen sollten das fehlerhafte Crowdstrike-IT-Update zum Anlass nehmen, einen IT-Notfallplan zu erstellen und ihre Cyber-Resilienz zu prüfen. „Ob die Ursache für einen IT-Ausfall ein Updatefehler und ein Hackerangriff ist, spielt nicht nur bei kritischen Infrastrukturen eine unteregordnete Rolle. Das Ergebnis ist in beiden Fällen verheerend. Im Falle eines Cyberangriffs kommen Image- und Reputationsschäden hinzu“, sagt Payam Rezvanian, Mitglied der Geschäftsleitung bei Finanzchef24, dem Absicherungsspezialisten für Selbstständige und Unternehmer (www.finanzchef24.de). Fast jedes zweite Unternehmen in Deutschland ist heute bereits von einer Cyberattacke betroffen, doch nur etwa 40 Prozent der Unternehmen haben einen IT-Notfallplan.

Finanzchef24 rät Unternehmen zu einem gut entwickelten und regelmäßig getesteten IT-Notfallplan. Auch vor dem Hintergrund, dass eine bereits funktionierende IT-Sicherheit eine grundlegende Voraussetzung zum Abschluss einer Cyberversicherung gilt. Die zunehmend digitalen Bedrohungen und komplexer werdenden Risikoszenarien erfordern eine systematische Vorgehensweise bei einer unternehmenskritischen Notfallsituation.

### Die wichtigsten Punkte für einen Cyber-Notfallplan

1. **Effektive Kommunikation:** Ein Notfallkommunikationsplan, der sicherstellt, dass alle betroffenen Parteien schnell und klar informiert werden. Im Vorfeld: Stakeholder identifizieren, Kommunikationskanäle festlegen, Nachrichten für verschiedene Szenarien vorbereiten. Dabei sind Meldepflichten zu beachten. Zum Beispiel: Datenschutzbehörde, Bundesamt für Sicherheit in der Informationstechnik, Schadensmeldung an Versicherung.

2. **Umfassendes Notfallkontaktbuch:** Alle relevanten internen und externen Kontakte, die im Notfall benötigt werden. Das Kontaktbuch sollte regelmäßig aktualisiert und sowohl an einem anderen Ort separat digital als auch in physischer Form sicher aufbewahrt werden.

3. **Bereitstellung eines Notfallkoffers:** Ersatzrechner, -telefone, -server und wichtige Software, um den Geschäftsbetrieb aufrechtzuerhalten. Handbücher und Anweisungen in physischer Form für die schnelle Inbetriebnahme und Fehlerbehebung der Ersatzausrüstung.

4. **IT-Notfallkarte:** Hinweisschild in physischer Form sichtbar positioniert im Stil „Verhalten im Brandfall" bietet Beschäftigten wichtige Verhaltenshinweise bei IT-Notfällen. Die Notfallkarte soll an zentralen Orten platziert werden und erzeugt einen unmittelbaren Beitrag zur Security Awareness in der Organisation. Sie gibt Beschäftigten wichtige Verhaltenshinweisen bei IT-Notfällen, damit sie vom ersten Moment an richtige Entscheidungen treffen können. Die Karte beinhaltet die Ansprechpartner für IT-Notfälle und deren Erreichbarkeit, sowie die ersten Schritte zur Durchführung von Gegenmaßnahmen. Diese dürfen nur nach Absprache mit den Verantwortlichen durchgeführt werden.

5. **Regelmäßige Überprüfungen und Übungen:** Schulungen und Sensibilisierungs-maßnahmen im Unternehmen: Sicherstellen, dass der Notfallplan aktuell bleibt und alle Beteiligten wissen, was im Ernstfall zu tun ist.

## Cyber-Sicherheit: Führungskräfte in der Pflicht

Da Cybervorfälle die Existenz eines Unternehmens gefährden, ist Cyber-Sicherheit laut Finanzchef24 Chefsache. „Auch wenn die Aufstellung eines solchen Plans zunächst aufwendig erscheint, ist dies eine Investition in die Zukunftssicherheit des Unternehmens. Es geht nicht nur um die Wiederherstellung von Systemen und Daten, sondern um das Vertrauen von Kunden, Partnern und Mitarbeitern und die Unternehmenszukunft," betont Rezvanian. Die Vorbereitung sollte regelmäßig überprüft, getestet und aktualisiert werden. Schulungen und Weiterbildungen der Mitarbeiter seien essentiell, wodurch die Belegschaft zu einem wesentlichen Bestandteil der Cyber-Sicherheit wird.
Meist ist die Herausforderung die Kombination von technischen Lücken und Fehlverhalten der Mitarbeiter. „Die IT kann noch so gut sein, der Mensch bleibt auch im Jahr 2024 das Problem. Die Bedrohung durch Cyberkriminalität nimmt kontinuierlich zu, und Unternehmen jeder Größe müssen sich darauf einstellen", sagt Payam Rezvanian.

**Fehlende Updates sind potenzielle Einfallstore**

Das Problem: Gerade kleine und mittlere Unternehmen überschätzen oft ihre IT-Sicherheit und unterschätzen die Risiken eines Hackerangriffs. Die Basis sind meist Bugs in der Software und fehlerhafte oder fehlende Updates, die von Internet-Bots ausspioniert werden. „Hacker greifen die kleinen und mittleren Unternehmen in der Regel nicht gezielt an. Die Cyberkriminellen verwenden dazu besondere Software, die alle verfügbaren Rechner und Homepages auf bekannte Sicherheitslücken absuchen," sagt Rezvanian. Üblicherweise durchsuchen Bots das Internet wie eine Suchmaschine nach Lücken. Jeder Anschluss, der gerade online ist, wird geprüft. Es wird gesucht, wo das letzte Update noch nicht installiert wurde und welche Software Sicherheitslücken aufweist. Deswegen sollten Firmen auf aktuelle Updates und Systemsicherheit achten.

## 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