FINANZ CHEF24

Pressemitteilung

IT-Hausaufgaben fürs Homeoffice: Wer remote arbeitet, riskiert andere Cybergefahren

Die Verlagerung der Arbeit ins Homeoffice erfordert starke Passwörter, VPNs und regelmäßige Updates zum Schutz vor Cyberangriffen. Menschliche Schwächen werden oft ausgenutzt.

(München, 20. August 2024). Die Zeitspanne zwischen dem Aufdecken von Sicherheitslücken und deren Ausnutzung durch Kriminelle wird immer kürzer. Die anhaltend hohe Homeoffice-Quote fordert die IT-Sicherheit bei Unternehmen zusätzlich heraus. „Wählen sich Mitarbeiter zu Hause mit unsicher abgesicherten Geräten in die Firmenstruktur ein, erhöht sich das Risiko von Cybervorfällen“, sagt Payam Rezvanian, Mitglied der Geschäftsleitung bei Finanzchef24, dem Absicherungsspezialisten für Selbstständige und Unternehmer.

Homeoffice: DSGVO stellt besondere Anforderungen an Unternehmer

Die Einhaltung der DSGVO (Datenschutz-Grundverordnung) stellt in Deutschland besondere Anforderungen an Unternehmen, die Homeoffice-Optionen anbieten. Laut DSGVO müssen Mitarbeiter mindestens einmal jährlich in IT-Sicherheit geschult werden, um deren Kenntnisse kontinuierlich zu verbessern. So sollen Sicherheitspraktiken auf den neuesten Stand gebracht und das Risiko von Datenschutzverletzungen minimiert werden. Werden Handy oder Laptop auch privat genutzt, schreibt die DSGVO eine Vereinbarung zwischen Unternehmen und Mitarbeiter vor. Der Unternehmer hat die Pflicht, die Daten seiner Kunden zu schützen und zu garantieren, dass diese ordnungsgemäß behandelt werden. Dürfen Mitarbeiter von privaten Geräten aus arbeiten, müssen sie sich DSGVO-konform verhalten.

Besondere Sorgfalt gilt, laut Finanzchef24, für das mobile Arbeiten. Sobald sich Mitarbeiter außerhalb der EU befinden, gilt die deutsche DSGVO nicht mehr. Werden E-Mails auf privaten Geräten eines Mitarbeiters gelesen oder bearbeitet, der berufliche Kalender auf privaten Geräten aufgerufen oder loggen sich Mitarbeiter in die Firma über öffentliches WLAN ein, stellt dies ein erhebliches Sicherheitsrisiko dar.

Personenbezogene Daten und DSGVO

Wenn es zu einem Cybervorfall kommt, kann ein DSGVO-Verstoß vorliegen. „Zum Beispiel im Fall eines Cyberangriffs, wenn auf Daten unberechtigt zugegriffen wird, sodass man die Kontrolle über die Verwendung dieser Daten verliert“, sagt Frank Gottheil, Senior Firmenkundenberater bei Finanzchef24, der auch auf Cyberversicherungen spezialisiert ist. Diese Daten könnten missbraucht werden, um Identitätsdiebstahl zu begehen oder vertrauliche Informationen zu veröffentlichen.

„Die Komplexität moderner Computer- und Netzwerkkonstellationen macht es IT-Abteilungen und Freiberuflern schwer, den Überblick über potenzielle Schwachstellen zu behalten“, erklärt der Experte. Es gelingt in der Regel binnen weniger Minuten, insbesondere private Abwehrsysteme zu überwinden. Eine einzige Schwachstelle genügt, um darüber Angreifern Zugang zur digitalen Infrastruktur eines Unternehmens zu ermöglichen. Ein Hauptfehler bleiben menschliche Schwächen. Wenn ein Mitarbeiter etwa den Namen seiner Katze in sozialen Netzwerken preisgibt und denselben als Passwort verwendet, öffnet das Tür und Tor für Cyberkriminelle.

Cybercrime auf Rekordhoch: Kleine und mittlere Unternehmen im Visier

Laut dem Lagebericht 2023 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist die Bedrohung durch Cybercrime so hoch wie nie zuvor. Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern vermehrt kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Jeder Angriff bei einem Geschäftspartner kann direkt auf alle verbundenen Unternehmen übergreifen. Im Vergleich zu großen Unternehmen mit automatisierten Prozessen müssen sich kleinere Firmen auf sich selbst oder auf ihre externen IT-Dienstleister verlassen, die Sicherheitsupdates durchzuführen.

Finanzchef24 empfiehlt, IT-Maßnahmen umzusetzen, um die Sicherheit im Homeoffice zu gewährleisten.

IT-Checkliste für sicheres Arbeiten im Homeoffice

1. **Verwendung von starken, einzigartigen Passwörtern** und Aktivierung der Zwei-Faktor-Authentifizierung (2FA).
2. **Software-Updates und Patches** umgehend installieren, um Sicherheitslücken zu schließen.
3. **Nutzung eines VPNs**, um eine sichere Verbindung zum Unternehmensnetzwerk zu gewährleisten.
4. **Sensibilisierung und Schulung der Mitarbeiter** im Erkennen von Phishing-Versuchen und anderen Cyberbedrohungen.
5. **Einsatz von Sicherheitssoftware** wie Antivirus- und Antimalware-Programmen auf allen Endgeräten, auch auf Smartphones.

6. **Sicherheitsrichtlinien für das Homeoffice** entwickeln und durchsetzen, um den sicheren Umgang mit Unternehmensdaten zu gewährleisten.
7. **Regelmäßige Backups** wichtiger Daten außerhalb der Cloud, um bei einem Angriff Datenverlust zu vermeiden.
8. **Beschränkung der Zugriffsrechte** auf das notwendige Minimum, um das Risiko von Datenlecks zu minimieren.
9. **Überwachung und Logging von Zugriffen** auf Unternehmensressourcen, um verdächtiges Verhalten frühzeitig zu erkennen.

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 Communications
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.de
Web: www.scrivo.de