17.11.2020 – 08:21 Uhr

Zurück im Home Office: 5 Tipps für Unternehmen zur Vermeidung von Sicherheitslücken beim mobilen Arbeiten

Zürich (ots) -

Lockdown 2.0: Nach dem erneuten Verschärfen der Maßnahmen zum Eindämmen der Corona-Pandemie ist ein großer Teil der Büromitarbeiter bereits wieder im Home Office - falls sie nach Ende des ersten Lockdowns überhaupt an ihren regulären Arbeitsplatz zurückgekehrt waren. Dies hat die Entwicklung des mobilen Arbeitens in den Unternehmen maßgeblich beschleunigt. Ein Problem bei der rasanten Umstellung hin zur Heimarbeit: In den letzten Monaten hat sich die Zahl der Cyberangriffe stark erhöht. Laut einer aktuellen Studie von IDC, für die im August IT- und Fachentscheider aus 210 Unternehmen mit mehr als 100 Mitarbeitern befragt wurden, gaben 78 Prozent der Befragten an, in den vergangenen Monaten erfolgreich attackiert worden zu sein. Besonders die fehlende Vorbereitungszeit und fehlendes Fachwissen im IT-Bereich können hier für Unternehmen zur Hürde werden. Diese Zahl zeigt, dass durch den schnellen Wechsel ins Home Office Anfang des Jahres Sicherheitslücken entstanden sind. Die folgenden fünf Tipps helfen, Schwachstellen zu beheben.

1. Mitarbeiter über IT-Sicherheitsrisiken informieren

Die eigenen Mitarbeiter können sich erst dann sinnvoll mit dem Schutz der Unternehmensdaten auseinandersetzen, wenn sie verstehen, welchen potenziellen Bedrohungen sie gegenüberstehen und wie sie ihnen begegnen. Oftmals bestehen allerdings auf diesem Gebiet bei Angestellten ohne speziellen IT-Background Wissenslücken - die dann zu Sicherheitsrisiken werden. Es ist deshalb von zentraler Bedeutung, seine Mitarbeiter sorgfältig über die Gefahren aufzuklären und ihnen mögliche Folgen verständlich zu machen. Oftmals werden die Folgen eines Cyberangriffs stark unterschätzt und Sicherheitsmaßnahmen daher vernachlässigt. Die Sensibilisierung gerade für aktuelle Gefahren, wie Phishing-Angriffe oder Ransomware-Attacken, ist hierbei besonders wichtig. Allen Mitarbeitern sollte beispielsweise klar sein: Schon ein Klick auf einen E-Mail-Anhang eines Angreifers kann zu großen Schäden führen. Zusätzlich sollten unternehmensweit einheitliche Regeln geschaffen werden. So bleibt es nicht den Mitarbeitern selbst überlassen, ihre Informationen auf beliebige Art und Weise zu schützen - wodurch Unsicherheiten und eventuell Schwierigkeiten bei der Zusammenarbeit, beispielsweise beim sicheren Austausch von Dateien - vermieden werden.

2. Private Geräte schützen - oder vermeiden

Unternehmen erlauben ihren Mitarbeitern teilweise die Nutzung eigener Geräte zu Heimarbeit oder die Nutzung des Firmenrechners im privaten Umfeld. Auf erstere Maßnahme, auch "Bring-your-own-device" (BYOD) genannt, wird insbesondere bei kleinen Firmen, mit unzureichender Hardware zurückgegriffen. Jedoch sorgen private Geräte, wenn sie nicht professionell gesichert werden, schnell für Sicherheitslücken - für die das Unternehmen haftet. Der Arbeitgeber kann nicht überprüfen ob Daten ausreichend geschützt sind. Ebenso nutzen Arbeitnehmer zunehmend mobile Apps, die oft auf privaten Smartphones installiert werden, insbesondere wenn kein Betriebstelefon für die Heimarbeit zur Verfügung gestellt wird. In Hinblick auf das Stichwort "mobiles Arbeiten" sollte gerade bei der Nutzung von Apps eine ausreichende Sicherung bestehen. In Zusammenhang mit der Schulung der Mitarbeiter, sind Nutzervereinbarungen zu empfehlen, die festlegen, welche Daten wo gespeichert und verarbeitet werden dürfen. Auf Nummer sicher gehen Unternehmen allerdings mit firmeneigenen Geräten - die eindeutig vor der Nutzung privater Geräte bevorzugt werden sollten - auch im Sinne einer Haftbarkeit des Unternehmens.

3. VPN's nutzen und den Fernzugriff überwachen

Eine Verbindung zu sensiblen Unternehmensnetzwerken von zu Hause über einen sicheren VPN-Zugang abzuwickeln, ist in vielen

Unternehmen bereits Standard. Bei der Einrichtung sollte sich allerdings nur auf Fachpersonal verlassen werden. Läuft der komplette Datenverkehr über das Firmennetzwerk, welches meist Anwendungen wie Microsoft Office oder zusätzlich SaaS-Lösungen beinhaltet, kommt es ansonsten schnell zu einer Überlastung, wenn sich eine große Anzahl an Mitarbeitern im Home Office befinden. Die bloße Einrichtung eines VPNs reicht allerdings nicht aus. Gab es einen Angriff, kann nur durch den VPN nicht erkannt werden, ob sensible Daten heruntergeladen wurden oder nicht. Das Netzwerk sollte deshalb umfassend überwacht und die Aktivitäten und der Fernzugriff ständig überprüft werden. Im Falle eines Angriffes ist es wichtig, dass das IT-Team umgehend handlungsfähig ist - denn bei einem Hacker-Angriff zählt jede Minute, wenn Schäden vermieden werden sollen.

4. Cloud-Software mit Bedacht auswählen

Neben der Sicherung des eigenen Netzwerkes ist vor allem die Wahl sicherer Software-Lösungen wichtig - gerade im Cloud-Bereich. Cloud-Lösungen und Collaboration-Tools sind für die Arbeit im Home Office beinahe unerlässlich geworden und erleben dadurch gerade einen großen Aufschwung. Die vorgegebenen Security-Möglichkeiten und Einstellungen variieren allerdings je nach Anbieter - und nicht alle werden den hohen Sicherheitsanforderungen der Unternehmen gerecht. Besonders in Branchen, in denen mit sensiblen personenbezogenen Daten umgegangen wird, ist eine sichere Software von zentraler Bedeutung. Die Konformität mit den EU-DSGVO Datenschutzrichtlinien sollte jederzeit gewährleistet sein, insbesondere seit der Aufhebung des EU-Privacy Shields und bei Datenaustausch mit dem Ausland. Bei der Auswahl sollten Unternehmen demnach nur Anbieter in Betracht ziehen, die eine Sicherung gemäß DSGVO und zertifizierte Rechenzentren vorweisen können.

5. Verschlüsselte Lösungen einsetzen

Ein zentraler Aspekt für eine sichere digitale Zusammenarbeit während des mobilen Arbeitens ist die Verschlüsselung des Datenaustauschs. Gerade beim Versand von Dateien, auf dem Weg zwischen dem Absender und dem Empfänger, sind unverschlüsselte Daten ein leichtes Angriffsziel für Hacker. Eine konsequente Ende-zu-Ende-Verschlüsselung, bei der die Daten nicht von Dritten eingesehen werden können, schützt davor zuverlässig, sowohl unternehmensintern als auch zwischen Kunden und weiteren Parteien. Eine solche, hochsichere Lösung wird beispielsweise angeboten von Tresorit. So kann - auch mit minimalem IT-Know-how - die Basis für eine sichere Speicherung und Verarbeitung unternehmenseigener Daten gelegt werden.

Fazit: Der plötzliche Umzug ins Home Office war für Unternehmen und ihre Mitarbeiter gleichsam eine Herausforderung - und eine beachtliche Leistung aller Beteiligten. Bei der schnellen Implementierung neuer, digitaler Lösungen stand jedoch die Funktionalität oftmals vor der Sicherheit im Vordergrund. Das wiederum nutzten Cyber-Kriminelle umgehend aus. Hier ist es nun wichtig, nachzubessern und Sicherheitslücken zu schließen - damit auch beim mobilen Arbeiten höchste Sicherheitslevel garantiert sind.

Autor: István Lám, CEO und Co-Founder von Tresorit

Pressekontakt:

PIABO PR GmbH
Julia Loeser
E-Mail: tresorit@piabo.net
Phone: +49 30 2576 205 - 19
Markgrafenstraße 36
10117 Berlin | Germany

Medieninhalte

Zurück im Home Office: 5 Tipps für Unternehmen zur Vermeidung von Sicherheitslücken beim mobilen Arbeiten, Bildquelle: Tresorit / Weiterer Text über ots und www.presseportal.de/nr/148823 / Die Verwendung dieses Bildes ist für redaktionelle Zwecke honorarfrei. Veröffentlichung bitte unter Quellenangabe: "obs/Tresorit AG"