Sicher im Homeoffice. – Geht das? Wie?

Corona hat geschafft, wofür sich viele Arbeitnehmer*innen lange vergeblich einsetzten: Flexibles Arbeiten im Homeoffice. Doch die Verlagerung der Mitarbeitenden lief vielerorts alles andere als blitzschnell und reibungslos. Und sie verstärkt ein Problem, mit dem Unternehmen ohnehin schon lange kämpfen: IT- und Informationssicherheit.

"Working from home" braucht mehr als mobile Arbeitsgeräte: Neben einem perfektem Toolset und technischen Sicherheitsvorkehrungen spielen Mitarbeiter*innen eine noch zentrale Bedeutung in der Cyberabwehr. Nur die Kombination aus technischen und menschlichen Faktoren bringt echten Schutz.

Was sind die Herausforderungen im Home-Office?
Geräte im Home-Office sind bei Weitem nicht so gut geschützt wie im Unternehmen selbst. Netzwerke mit Firewallschutz, Zutrittskontrollen und Kontrolle durch Datenschutzbeauftragte gibt es zuhause nicht. Verteilte Systeme und teilweise unerfahrene Mitarbeiter*innen erschweren die Entdeckung von Sicherheitsverletzungen.

Wir beobachten auch, dass Unternehmen strikte, langjährig bewährte Zugriffsregeln aufweichen, da die Kolleg*innen sich im Homeoffice ohne persönlichen Kontakt vertreten müssen. Nicht selten müssen Mitarbeiter*innen aus Mangel an Firmenlaptops auf Privatrechner ausweichen, um überhaupt arbeiten zu können. Von einem sicheren Arbeitsumfeld kann da keine Rede sein. Und während IT-Admins kaum hinterherkommen, alle nötigen Maßnahmen zu treffen, reicht dem Angreifer eine einzige Sicherheitslücke, um erfolgreich zu sein. Irgendwie unfair, oder?

Und noch dazu kommt, dass Mitarbeiter*innen, die es nicht gewohnt sind, im Homeoffice zu arbeiten, ein echtes Sicherheitsrisiko darstellen können: Denn sie ...:

- agieren unvorsichtiger: So vernachlässigen sie zum Beispiel gerne das Sperren des Laptops in Pausen. Sie notieren Passworte auf Klebezetteln. Sie speichern Dateien lokal ab.
- sind schneller abgelenkt und handeln dadurch möglicherweise unbedacht.
- sind überfordert, wenn etwas Ungewöhnliches passiert und wissen nicht, wen sie bei Fragen oder Problemen ansprechen können. Denn der IT-Admin ist nicht mal eben greifbar oder schnell gefragt.

Folglich steigt das Risiko, Opfer eines Cyber-Angriffs zu werden. Das geht größeren Unternehmen kaum anders als kleineren. Als Lichtblick für Kleinunternehmen, die in der Regel nicht ganz so viel Spielraum für IT-Sicherheit haben: Auch die großen sind manchmal benachteiligt: So kann Social Engineering in Unternehmen, in denen nicht jeder jeden kennt, sogar leichter erfolgreich sein.

Eins ist klar: Die Taktfrequenz von Angriffen steigt. Und Cyberkriminelle sind geschickt und erstaunlich schnell darin, aktuelle Entwicklungen für ihre Zwecke zu benutzen. IT-Sicherheitskonzepte und -maßnahmen sind also ein Muss für Unternehmen jeder Größe. Das fordert die IT-Abteilungen auch so schon. Nun kommt für sicheres, verteiltes Arbeiten weiterer Mehraufwand und Zeitdruck hinzu. Doch es geht nicht anders. Grundlegendste Sicherheits- und Compliance-Vorgaben dürfen nicht vernachlässigt werden, auch wenn es eilt!

Also: Was tun?

- Beginnen wir beim Patchmanagement. Dafür muss es zum einen einen Prozess geben und zum anderen eine passende Software vorhanden sein. Außerdem muss bekannt sein, welche Geräte und Software überhaupt vorhanden sind, damit diese gepatcht oder upgedatet werden können. Und hier ist Sorgfalt gefragt! Fahrlässigkeit oder ein einziges fehlkonfiguriertes Gerät kann für Cyberkriminelle ausreichen, um in ein System und daraufhin in große Teile der Unternehmensinfrastruktur einzudringen. Der Zugriff auf Geräte im Homeoffice muss für die IT jederzeit möglich sein. Nicht nur, um im Notfall helfen zu können, auch für eventuell notwendig werdende, verschärfte Sicherheitseinstellungen bei neuen Angriffsmethoden.
- Für Unternehmenszugriffe "von außen" müssen noch strengere Zugriffsrechte implementiert werden und bestenfalls jeder Zugriff verfolgt werden können.
- Mitarbeiter*innen im Homeoffice dürfen nur durch eine verschlüsselte Verbindung (VPN) und zusätzlich durch eine Firewall ins Unternehmensnetzwerk gelangen.
- Jeder/s PC, Laptop, Tablet, Smartphone, das dienstlich genutzt wird, sollte mindestens einen aktuellen und vom Administrator „überwachten“

Antivirenschutz besitzen.
- Festplatten auf Homeoffice- oder mobilen Geräten sowie USB-Sticks sollten unbedingt verschlüsselt sein, damit im Fall eines Geräteverlustes nicht auf die gespeicherten Daten zugegriffen werden kann.
- Wenn Daten lokal statt auf dem zentralen Firmenserver abgelegt werden, sollten Mitarbeiter regelmäßig Backups anlegen und diese nicht auf dem gleichen Gerät sichern.
- Falls sprachgesteuerte Assistenten wie Siri oder Alexa in Arbeitsnähe stehen, sollten diese bei vertraulichen Telefonaten oder Videokonferenzen abgeschaltet werden.
- In Security Awareness Trainings sollten Mitarbeiter*innen für Cyberbedrohungen sensibilisiert werden, um Cyber-Attacken erfolgreich abzuwehren.

Beenden wir die Liste an dieser Stelle. Sofern Sie die Herausforderungen für sicheres Homeoffice bisher unterschätzt haben, hat der Artikel hoffentlich für ein Stück Aufklärung gesorgt. Und vielleicht schätzen Sie die Kolleg*innen aus der IT-Abteilung künftig (noch) mehr und schenken Ihnen ab und zu ein dankendes Lächeln. Denn sie ermöglichen Ihnen die Freiheit, dort zu arbeiten, wo Sie möchten und das im besten Fall genauso sicher wie im Unternehmensbüro.

Ansprechpartner

Veit Starke
bitbone AG
Prymstr. 3
97070 Würzburg
0931 25099312
starke@bitbone.de
www.bitbone.de

TIPP:

Gerade für kleine und mittelständische Unternehmen ist IT-Security eine besondere Herausforderung, wenn Personal und Mittel für vollumfänglichen Schutz fehlen. Wir empfehlen zur Auswahl und Priorisierung der Unternehmensdaten, die unbedingt schützenswert sind und nachfolgend zum Implementieren der Maßnahmen mit dem besten Kosten-Nutzen-Verhältnis. Wer es bequemer haben möchte, sucht sich einen Managed Security Service Provider seines Vertrauens.

Foto: Veit Starke, bitbone Cybersecurity Expert