Arbeiten im Homeoffice – so wird es sicher

Viele Firmen bieten ihren Mitarbeitern an, von Zuhause zu arbeiten, sei es partiell oder sogar dauerhaft, weil Fachkräfte in der globalisierten Welt nun einmal nicht immer vor Ort sind - oder weil, wie im aktuellen Fall, das Corona-Virus besondere Maßnahmen erfordert. Das kann gut gelingen, wenn Unternehmen und Belegschaft ein paar Sicherheitsmaßnahmen beachten. Sophos hat sie zusammengefasst.

Geübte Homeworker kennen sich bereits mit Heimarbeit aus und verfügen über die entsprechenden Zugänge und das Equipment wie Laptop und Smartphone. Aktuell aber gehen viele Unternehmen angesichts des explorativen Ausbruchs von SARS-CoV-2 auf Nummer sicher und bieten ihren Mitarbeitern die Möglichkeit, von Zuhause zu arbeiten.
Aber, damit die physische Sicherheit der Belegschaft nicht zugleich zur Bedrohung für die Cybersicherheit wird, müssen wichtige Maßnahmen beachtet werden.

Vorweg: Bleibt ein Kollege aus Präventionsgründen mit sofortiger Wirkung zuhause, bleibt keine Gelegenheit mehr, sich über den üblichen Weg – eingerichtetes Laptop und Telefon abholen und Vor-Ort-Schulung zum sicheren Teleworker – vorzubereiten. Das wahrscheinlichere Szenario sieht eher so aus: aus der Ferne und von Null an müssen die Geräte für die Verbindung mit dem Unternehmensnetzwerk aufgesetzt werden. Das ist mühsam und fehleranfällig.

Deshalb hier fünf Tipps, wie der Start in die Heimarbeit sicherer und einfacher gelingt:

1. Einfache Startbedingungen schaffen
Es gibt Produkte, die ein SSP, anbieten, ein Self-Service-Portal. Ein Service, mit dem sich der Nutzer aus der Ferne verbinden kann, womöglich sogar mit einem Laptop ab Werk, und das sicher und einfach eingerichtet werden kann, ohne Vorort-Setup durch die betriebliche IT-Abteilung.

Viele SSPs erlauben es den Nutzern, zwischen verschiedenen Zugangslevels zu wählen, so dass sie entweder ein persönliches Gerät (wenn auch mit geringerem Zugang zu wenigeren Unternehmenssystemen als mit einem dezidierten Gerät) oder eines, das ausschließlich der Firmennutzung dient, verwenden können.

Die drei Schlüsselelemente, die man schnell und genau installieren sollte, heißen:
Verschlüsselung – Schutz – und Patching.

- Verschlüsselung bedeutet hier, dass die gesamte Geräteverschlüsselung aktiviert ist. Das schützt bei Diebstahl sämtliche Daten auf dem Gerät.
- Schutz heißt, zunächst einmal auf bewährte Sicherheitssoftware (wie Anti-Virus) zu setzen, Konfigurierung nach Bedarf.
- Patching inkludiert die Einstellung für den User, so viele Sicherheitsupdates wie möglich automatisch zu erhalten.

Notsituation Datendiebstahl: Hier gilt es zu klären, ob ein meldepflichtiger Datendiebstahl vorliegt. Um darzulegen, dass man als Unternehmen alle notwendigen Vorsichtsmaßnahmen erledigt hat, sollte man im Betrieb die Maßnahmen (als Beweis) dokumentieren.

2. Arbeitsfähigkeit ermöglichen
Wenn der Mitarbeiter seine Arbeit nur mit Zugang zu Server XY erledigen kann, dann muss dieser auch im Homeoffice gewährleistet sein. Im Idealfall hat man dieses VOR dem Ernstfall bereits wirksam getestet.

Nicht alle Arbeitsprozesse im Betrieb funktionieren auch im Homeoffice, sei es aus Sicherheitsgründen, juristischen Hürden oder auch einfach Unternehmensregeln. Das sollte klar und rechtzeitig kommuniziert werden, um Frust und fehlende Arbeitsschritte zu vermeiden. Als Mitarbeiter im Homeoffice sollte man sich auf der anderen Seite aber auch darüber im Klaren sein und nicht versuchen, diese Grenzen kreativ zu umgehen.

3. Sicherheitsüberblick über Heimgeräte bewahren
Der Heimschaffende sollte nicht mit der Funktionalität seiner Geräte allein gelassen werden. Verfügt der Nutzer wie empfohlen über ein automatisches Update, muss es Funktionen für das Unternehmen geben, die automatische Umsetzung auch zu überprüfen. IT-Mitarbeiter im Betrieb sollten bei akut auftretenden Problemen remote zur Seite stehen, um die Arbeitsprozesse nicht langwierig zu verzögern. Auch diese Zeit sollte der Betrieb in den Abteilungen einkalkulieren.

4. Ein Briefkasten für Sicherheitsprobleme
Hilfreich ist das Aufsetzen einer betrieblichen E-Mail-Adresse, an die die Mitarbeiter Sicherheitsprobleme schnell und unbürokratisch schicken können.

Vor dem Hintergrund, dass viele Cyberattacken erfolgreich sind, weil die Betrüger es immer wieder und genau so lange versuchen, bis es zu einem gedankenlosen Klick kommt, dient ein Sicherheits-E-Mail-Briefkasten auch der Prävention: Auffälligkeiten lassen sich schnell registrieren und Warnungen können folgen. Alle Hinweise der Nutzer, selbst überflüssige, sollten unbedingt gewürdigt werden. Die Infos zum Security-Service wiederum landen am besten nicht im E-Mail-Account als Link, sondern, um es Betrügern auch in diesem Bereich schwer zu machen, offline via Brief, Infokarte oder Ähnlichem Zuhause.

5. Shadow-IT-Lösungen im Auge behalten
Shadow-IT heißt, dass Nicht-IT-Mitarbeiter mit ihren eigenen Möglichkeiten technische Probleme lösen, sei es aus Bequemlich- oder zeitlicher Dringlichkeit. Dieser Entwicklung muss nicht zwangsläufig Einhalt geboten werden, wie das folgende Beispiel deutlich macht. Allerdings sollte klar sein, dass „Shadow IT“ nicht nur für Probleme sorgen kann, wenn sie schief geht, sondern auch im Erfolgsfall – so z.B. bei Haftungsfragen.

<u>Fallbeispiel</u>
Arbeitet ein Kreis von Kollegen im Büro eng zusammen, ist jetzt aber durch das Homeoffice räumlich getrennt, werden sie vielleicht eine eigene Idee liefern, wie sie sich zukünftig austauschen wollen, auch mit Tools, die sie vorher nie verwendet haben. Diese Dynamik aus den Teams sollten Firmen nicht gleich ausbremsen, sondern unterstützen, sofern sie mit den Betriebssicherheitsregeln konform gehen. Eine temporäre Lösung kann auch neue und erfolgreiche Optionen für ein Unternehmen liefern. Als Organisation sollte man die Sicherheitsvorgaben klargemacht und Zugangsdaten zu den Teamlösungen haben, falls Passworte vergessen werden.

Fazit: Wo es im Realen jetzt Abstand halten heißt, gilt es virtuell zusammenzurücken
Wenn Unternehmen und Mitarbeiter also plötzlich in die Telearbeit einsteigen müssen, sollten sie eng und vertrauensvoll zusammenarbeiten. Wenn beispielsweise das IT-Team plötzlich darauf besteht, dass ein Kennwortmanager und 2 Faktor-Authentifizierung (2FA) verwendet wird, dann sollten Mitarbeiter der Aufforderung uneingeschränkt Folge leisten. Auf der anderen Seite gilt es für die Systemadministratoren im Unternehmen, die heimarbeitenden Mitarbeiter und deren Fragen unbedingt ernst zu nehmen – egal wie oft sie sie stellen. Denn es kann sein, dass sie es beim ersten Mal nicht klar verstanden haben oder die Funktion, die sie

benötigen, wirklich wichtig ist, um ihre Arbeit richtig zu machen. Wir leben in schwierigen Zeiten. Für alle bedeutet dies, nicht zuzulassen, dass Angelegenheiten der öffentlichen Gesundheit die Art von Reibung verursachen, die der ordnungsgemäßen Durchführung der Cybersicherheit im Wege steht!

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de