5 Empfehlungen für Mitarbeiter im Homeoffice

Wir sind uns bewusst, dass Homeoffice für einige von Ihnen vielleicht neu ist und Sie sich in der Zeit, in der Sie sich an diese neue Umgebung gewöhnen müssen, auch etwas überfordert fühlen können. Eines unserer Ziele ist es, Ihnen zu helfen, so sicher wie möglich von zu Hause aus zu arbeiten.

Die nachfolgenden fünf Empfehlungen sorgen für Sicherheit. Und das Beste daran ist, dass sie nicht nur Ihre Arbeit sicherer machen. Diese Massnahmen schützen auch Sie und Ihre Familie, weil sie Ihr ganzes Zuhause vor Cyberangriffen bewahren.

1. Sie selbst

Das Wichtigste gleich zu Beginn: Die Technologie alleine kann Sie nicht umfassend schützen – Sie selbst sind die beste Verteidigung. Kriminelle haben gelernt, dass sie ihr Ziel am besten erreichen, indem sie nicht Ihren Computer oder Ihre sonstigen Geräte, sondern Sie persönlich ins Visier nehmen. Wenn sie es auf Ihr Passwort oder Ihre geschäftlichen Daten abgesehen haben oder Ihren Computer kontrollieren wollen, dann versuchen diese Täter, Sie auszutricksen: Sie sollen dazu gebracht werden, ihnen Zugang zu geben. Oft wird dazu ein Gefühl der Dringlichkeit erzeugt. Beispielsweise erhalten Sie einen Anruf von jemandem, der sich als Microsoft-Support-Mitarbeiter ausgibt und behauptet, Ihr Computer sei infiziert. Oder Sie erhalten eine E-Mail mit dem Hinweis, dass ein Paket nicht geliefert werden konnte. Auf diese Weise sollen Sie dazu verleitet werden, auf einen manipulierten Link zu klicken.

Zu den häufigsten Anzeichen eines sogenannten Social-Engineering (https://www.ebas.ch/social-engineering/) -Angriffs zählen:

- Es wird ein grosses Gefühl der Dringlichkeit erzeugt, oft durch Angstmacherei oder Einschüchterung oder indem eine Krise oder ein wichtiger Termin vorgeschoben wird.
- Es wird Druck ausgeübt, die Sicherheitsrichtlinien oder -verfahren zu umgehen, oder eine Nachricht ist einfach zu gut, um wahr zu sein. (Nein, Sie haben in keiner Lotterie gewonnen!)
- Eine Nachricht von einem Freund oder einer Arbeitskollegin, bei der Unterschrift, Tonfall oder die Formulierung nicht nach ihnen klingen.

Letztlich sind Sie selbst die beste Verteidigung gegen solche Angriffe!

Weitere Informationen (https://www.ebas.ch/5-aufpassen-und-wachsam-sein/)

2. Heimnetzwerk

Fast jedes Heimnetzwerk beruht auf einem drahtlosen Netzwerk (oft als WiFi oder WLAN bezeichnet). Es ermöglicht es Ihren Geräten, sich mit dem Internet zu verbinden. Die meisten drahtlosen Heimnetzwerke werden von Ihrem Router oder einem separaten Wireless Access Point (WAP) kontrolliert. Beide funktionieren gleich: Sie senden ein Funksignal aus, mit dem sich die Geräte verbinden. Die Sicherung Ihres WLANs ist somit der Schlüssel zur Sicherung Ihres Zuhauses.

Wir empfehlen Ihnen dazu die folgenden Massnahmen:

- Ändern Sie das Standardpasswort für den Administrator: Über das Administrator-Konto können Sie die Einstellungen für Ihr WLAN konfigurieren. Für einen Angreifer ist es nicht schwierig, das Standardpasswort des Herstellers herauszufinden.
- Geben Sie nur Personen Zugang zu Ihrem WLAN, denen Sie vertrauen: Wählen Sie eine strenge Anmeldesicherheit, damit sich nur Personen, denen Sie vertrauen, in Ihr WLAN einloggen können. Ein gesichertes WLAN verlangt ein Passwort, um sich damit zu verbinden. Sobald die Verbindung aufgebaut ist, werden die Aktivitäten verschlüsselt.
- Wählen Sie starke Passwörter: Das Passwort für die Verbindung zu Ihrem WLAN muss stark sein und sich vom Administrator-Passwort unterscheiden. Denken Sie daran: Sie müssen das Passwort für jedes Gerät nur einmal eingeben, weil die Geräte es dann speichern und sich daran erinnern.

Sie sind nicht sicher, wie das geht?
Fragen Sie Ihren Internet Service Provider, schauen Sie auf seiner Webseite nach, studieren Sie die Anleitung, die mit Ihrem Router geliefert wurde, oder gehen Sie auf die Webseite des Anbieters.

Nutzen Sie während Ihrer Arbeit eine VPN-Verbindung
Mit einer VPN-Verbindung können Sie Ihr Gerät zu Hause auf sichere Art und Weise an das Firmennetzwerk anbinden. Dabei werden die Inhalte auf dem Transportweg mittels Verschlüsselung geschützt (Ende-zu-Ende-Verschlüsselung).

3. Passwörter

Wenn Sie auf einer Webseite aufgefordert werden, ein Passwort zu kreieren, dann wählen Sie ein starkes: Je mehr Zeichen es umfasst, desto stärker ist es. Nutzen Sie eine Passphrase: Das ist eine der einfachsten Methoden, um sicherzustellen, dass Ihr Passwort stark ist. Eine Passphrase ist nichts anderes als ein Passwort, das aus mehreren Wörtern besteht, beispielsweise «Biene Honig Bourbon». Ein einmaliges Passwort bedeutet, dass Sie für jedes Gerät und jedes Online-Konto ein anderes Passwort wählen. Wenn dann ein Passwort oder eine Passphrase gehackt wird, sind all Ihre anderen Konten und Geräte weiterhin sicher.

Sie können sich all diese Passphrasen und Passwörter nicht merken?
Nutzen Sie einen Passwort-Manager: Das ist ein spezielles Programm, das all Ihre Passwörter in einem verschlüsselten Format speichert (und auch sonst noch viele tolle Features hat!). Aktivieren Sie zudem wann immer möglich die Zwei-Faktor-Authentifizierung (auch Multi-Faktor-Authentifizierung genannt). Dieses System überprüft neben Ihrem Passwort noch einen zweiten Faktor. Beispielsweise wird nach einem Code gefragt, der an Ihr Smartphone gesendet oder über eine Authentifizierungs-App generiert wird. Die Zwei-Faktor-Authentifizierung ist wahrscheinlich das Wichtigste, was Sie tun können, um Ihre Online-Konten zu sichern. Und das ist viel einfacher, als Sie vielleicht denken.

Weitere Informationen (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/)

4. Updates

Cyberkriminelle suchen ständig nach neuen Schwachstellen in der Software Ihrer Geräte. Wenn sie solche Fehler entdecken, dann nutzen sie sie mit speziellen Programmen aus und hacken Ihre Geräte. Gleichzeitig sind die Unternehmen, welche die Software für diese Geräte entwickelt haben, ständig daran, die Schwachstellen durch Up-

dates zu beheben. Indem Sie sicherstellen, dass Updates rasch auf Ihrem Computer und Ihren mobilen Geräten installiert werden, machen Sie den Hackern das Leben schwer. Damit Sie immer auf dem neusten Stand bleiben, können Sie auch einfach das automatische Update aktivieren, wann immer diese Option angeboten wird. Diese Regel gilt für fast jede Technologie, die mit einem Netzwerk verbunden ist. Dazu zählen nicht nur Ihre Arbeitsgeräte, sondern auch mit dem Internet verbundene Fernseher, Babyphones, Sicherheitskameras, Router, Spielkonsolen oder sogar Ihr Auto.

Stellen Sie sicher, dass auf all Ihren Computern, mobilen Geräten, Programmen und Apps immer die neuste Software-Version installiert ist.

Weitere Informationen (https://www.ebas.ch/3-vorbeugen-mit-software-updates/)

5. Kinder & Gäste

Etwas, worum Sie sich im Büro kaum je sorgen müssen, sind Kinder, Gäste oder andere Familienmitglieder, die Ihren Geschäfts-Laptop oder andere Arbeitsgeräte benutzen. Diese Personen können versehentlich Informationen löschen oder ändern oder – was noch schlimmer ist – das Gerät unabsichtlich infizieren.

Machen Sie Ihrer Familie und Ihren Freunden unmissverständlich klar, dass sie Ihre Arbeitsgeräte nicht benutzen dürfen.

Wird dasselbe Gerät von mehreren Personen genutzt?
Richten Sie für ein Gerät, welches von verschiedenen Personen genutzt wird, pro Person ein separates Benutzerkonto ein. Damit erreichen Sie zumindest eine logische Trennung, und jeder Benutzer kann nur auf die Daten in seinem Bereich zugreifen.

Quelle: SANS Institut (https://security-awareness.sans.org/sites/default/files/2020-03/03-SSA-WorkingFromHome-FactSheet.pdf)

Diese Empfehlungen basieren auf dem Merkblatt des SANS Instituts (https://security-awareness.sans.org/sites/default/files/2020-03/03-SSA-WorkingFromHome-FactSheet.pdf) (englisch).