Home Office – aber sicher

Von zu Hause aus arbeiten hat mit Vorsichtsmassnahmen rund um Corona neuen Auftrieb erhalten. Aber auch schon vorher (und danach) war das Remote Arbeiten sehr beliebt. Doch auch am heimatlichen Arbeitsplatz gelten klare Vorgaben an den Datenschutz und die Informationssicherheit.

Artikel vonAndreas Wisler, Senior Security Consultant, CISSP, CISA

Auch wenn das Thema eigentlich selbstverständlich ist, haben gemäss einer Umfrage von WatchGuard nur 30% der Unternehmen Regeln im Zusammenhang mit dem Arbeiten von zu Hause, in Co-Working Bereichen oder von unterwegs erstellt und geschult. Dies macht es für beide Seiten unnötig schwer, sich richtig zu verhalten.

In der Regel stellen Unternehmen den Mitarbeitern entweder ein Arbeitsgerät zur Verfügung (z.B. ein Laptop) oder der Mitarbeitende muss sich auf seinem privaten Gerät mit den Servern des Unternehmens verbinden (z.B. via Citrix oder Terminal Server).

Als erstes sollte das Unternehmen klare Regeln aufstellen.
Diese sollten mindestens die folgenden Fragen beantworten: Was darf alles von zu Hause aus gemacht werden? Was ist nicht erwünscht oder gar verboten? Dürfen ausgedruckte Informationen mit nach Hause genommen werden? Dürfen Informationen zu Hause ausgedruckt werden? Wie müssen die Unterlagen aufbewahrt werden? Welche weiteren Pflichten und Aufgaben gilt es zu beachten?

Für ein Unternehmen ist es wichtig, dass die Datenschutzbestimmungen, wie auch die Vorgaben zur Informationssicherheit, zu jeder Zeit eingehalten werden. Es darf nicht sein, dass im Büro strenge Regeln umgesetzt sind, regelmässige Kontrollen durchgeführt werden und zu Hause wird alles über den Haufen geworfen.
Dies kann bei einer Verletzung der Sorgfaltspflicht strafrechtlichen Folgen nach sich ziehen. Gerade die Bestimmungen der DSGVO sind hier unbarmherzig. Daher gilt es klare Vorgaben zu definieren und durchzusetzen.

Klare Regeln geben Sicherheit

Das Gerät darf nicht mit anderen Familienmitgliedern geteilt werden. Unabhängig, ob es dem Mitarbeitenden oder dem Unternehmen gehört. Daten werden in diesem Fall lokal, das heisst auf dem verwendeten Gerät, abgespeichert und plötzlich haben andere Personen im Haushalt auch Zugriff darauf. Auch wenn keine böse Absicht dahintersteckt, aber mal ein spannend klingendes PDF öffnen und einen Blick riskieren, ist schnell passiert.

Je nach Umsetzung hat das Gerät keine Verbindung mit den Serverlaufwerken des Unternehmens. Das bedeutet, dass die erstellten oder veränderten Daten auch nicht automatisch gesichert werden. Die Mitarbeitenden sind also für die regelmässige Sicherung der Daten selber verantwortlich.

Wird dies mit Wechselplatten oder USB-Sticks ausgeführt, müssen diese verschlüsselt sein. So kommen auch bei einem unerwarteten Diebstahl keine Daten in falsche Hände.

Auch Ausdrucke und Papier-Unterlagen gilt es zu schützen. Ausdrucke sind sofort aus dem Drucker zu entfernen. Unterlagen dürfen bei Abwesenheit, auch wenn dies nur kurz ist, nicht offen herumliegen, sondern müssen sicher aufbewahrt werden, idealerweise in einem abschliessbaren Behältnis z.B. Beispiel ein Schrank oder ein Korpus. Familienmitglieder und Fremde dürfen zu keinem Zeitpunkt die Möglichkeit haben, an diese Unterlagen zu gelangen.

Weiter sollte der Datentransfer zwischen dem Unternehmen und dem Mitarbeitenden geklärt sein. Dürfen Daten per E-Mail verschickt werden? Wenn es von Geschäftsadresse zu Geschäftsadresse geschieht, ist dies in der Regel unproblematisch, da das E-Mail nie den E-Mail-Server des Unternehmens verlässt. Auf keinen Fall dürfen solche E-Mails an private Adressen, z.B. zu Google oder anderen Dienstleistern gesendet werden.

Ob die Daten zusätzlich verschlüsselt werden müssen, gilt es in einer Risiko-Analyse abzuwägen. Gerade wenn kein eigener Mailserver vorhanden ist und nur noch Cloud-Dienste genutzt werden, macht diese Überlegung sicherlich grossen Sinn. Da dies nicht trivial ist, müssen die Mitarbeitenden im Umgang mit der Verschlüsselung geschult sein.

Wird das private Gerät für die Tätigkeiten genutzt, kann es sein, dass wahlweise eine VPN-Verbindung, das bedeutet eine verschlüsselte Verbindung zwischen Gerät und Unternehmen, zur eingesetzt wird. Dies mag zwar für die Wartung von Servern und anderen Systemen durchaus Sinn machen, aus Sicht der Sicherheit ist dies aber keine gute Lösung, ist doch das Gerät dann direkt mit dem Firmennetzwerk verbunden.

Da die Aktualität des privaten Gerätes sowie die Schutzmöglichkeiten (Firewall, Antivirenprogramm, etc.) nicht bekannt sind, geht das Unternehmen ein sehr grosses Risiko ein. Ist ein Schädling auf diesem Gerät aktiv, kann es sein, dass dieser via VPN den Weg ins Unternehmen findet und auch dort Schaden anrichten kann. Daher sollte VPN wirklich nur im äussersten Notfall eine Option sein.

Besser ist es, via ein Remote-Programm zu arbeiten. Viele kennen sicherlich TeamViewer, mit welchem der Bildschirm des entfernten Computers angezeigt wird und auf diesem gearbeitet werden kann. Genau gleich verhält es sich mit Citrix oder Terminal-Server.

Dort sehe ich den Bildschirm des Firmenservers, habe somit meine gewohnte Oberfläche, die üblichen Programme und auch die bekannte Ordnerstruktur zur Verfügung.

Es verhält sich für den Mitarbeitenden, wie wenn er oder sie im Büro sitzen würde. Der grosse Vorteil ist hier natürlich, dass nur Bildinformationen übertragen werden.

Dies schont auch die Internet-Bandbreite. Auch wenn nur eine langsame Verbindung zur Verfügung steht, klappt dies ohne grosse Verzögerungen. Alle Daten bleiben immer im Unternehmen und verlassen dieses nie. Somit ist auch die Frage nach einem aktuell gepatchten System irrelevant.

Wichtig an dieser Stelle ist aber zu erwähnen, dass lokale Laufwerke nicht eingebunden werden. Ansonsten wird die Trennung zwischen den Geräten wieder aufgehoben.

Wie im Büro gilt auch hier: wenn ich den Arbeitsplatz verlasse, muss ich ihn sperren. Die so genannte Clear Screen Regel definiert, dass die Sperre so eingerichtet sein sollte, dass nur mit der Eingabe des Passwortes wieder weiter gearbeitet werden kann. An das private Gerät gelten demnach die gleichen Anforderungen an Passwörtern, wie in der Firma: mindestens 10 Zeichen zusammengesetzt aus Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Zudem sollten die Passwörter keinen persönlichen Bezug haben. Idealerweise kommt auch hier ein Merksatz zum Einsatz. «Ich sperre meinen Arbeitsplatzrechner immer, wenn ich ihn verlasse». ergibt Is1Ai,wiiv. (Bitte nicht diesen verwenden). Dieser Satz ist leicht zu merken und schützt die Daten.

Zu beachten ist, es gelten auch Schutzregeln bei Telefongesprächen. Wenn sich andere Personen in der Nähe befinden, dürfen keine vertraulichen Informationen über diesen Weg ausgetauscht werden.

Vielleicht haben Sie es auch schon mal bei einer Zugsfahrt erlebt, welche spannende Dinge da erzählt werden. Sei es geschäftliche Belange, ja teilweise sogar sehr intime Dinge wie Krankheiten oder Affären. Achten Sie daher darauf, was Sie mündlich weitergeben.

Kleine Dinge helfen, die Informationssicherheit zu gewährleisten

Mit wenigen Verhaltensweisen können Sie auch von zu Hause aus sicher arbeiten. Achten Sie darauf, dass niemand Fremdes an Informationen kommt.

Dies gilt auch für Familienangehörige. Versorgen Sie alle Unterlagen sicher, wenn diese nicht benötigt werden, idealerweise eingeschlossen.

Sperren Sie Ihr Gerät, auch wenn Sie nur kurz weg sind. Und passen Sie auf, welche Informationen Sie per E-Mail oder mündlich weitergeben. Damit können Sie den Datenschutz und die Informationssicherheit jederzeit gewährleisten.

weitere Infos: www.goSecurity.ch