Homeoffice

Leitfaden für Kommunen

[01.03.2021] Phishing, Ransomware und unsichere Passwörter – auch in Zeiten von Homeoffice suchen Cyber-Kriminelle nach Schwachstellen im Netzwerk der Verwaltungen. Wer die Risiken kennt, kann jedoch effektiv gegensteuern.

Die Corona-Pandemie hat neue Organisationsformen in die Verwaltungen gebracht. Das Homeoffice etwa erweist sich als pragmatische und in vielen Fällen effiziente Lösung, um arbeitsfähig zu bleiben, gleichzeitig aber die Mitarbeiter vor einer Ansteckung mit dem Coronavirus zu schützen. Das heimische Büro schützt allerdings nicht vor digitalen Viren und Cyber-Angriffen. Wer die Schwachstellen kennt, kann diese Risiken deutlich minimieren. IT-Dienstleister ekom21 hat einen entsprechenden Sicherheitsleitfaden formuliert.
Eine Schwachstelle sind und bleiben die Passwörter. Unbefugte erlangen über diese Lücke immer wieder Zugriff auf Daten und Systeme. Sicherheit beginnt deshalb bei einem sicheren Passwort. Generell gilt: Je komplexer und länger, desto sicherer. Laut den Verbraucherzentralen sollten Passwörter mindestens zehn Zeichen lang sein, aus Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen. Sie sollten in keinem Wörterbuch zu finden sein und auch nicht mit dem Nutzer in Verbindung stehen. Ähnlich sieht es das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es empfiehlt für manche Anwendungen aber sogar noch längere Passwörter. Einen 45 Zeichen langen Code kann man sich wiederum nicht ohne Weiteres merken. Hier helfen Passwort-Sätze. So könnte beispielsweise der Merksatz für das Passwort „TdCu12adF,kgdP!“ lauten: „Tanzt der Chef um zwölf auf dem Flur, klingelt gleich die Pausenuhr!“.

VPN-Lösung ist Voraussetzung

Häufige Schwachstellen sind zudem die Router im Homeoffice, also die Verbindungsrechner zwischen Telefon- oder Datenleitung und Endgerät. Eine Funkverbindung per WLAN ist praktisch, allerdings gilt auch hier: Ein sicheres Passwort ist unabdingbar. Noch sicherer sind feste Kabelverbindungen (LAN) zwischen Router und Endgerät. Handelsübliche Router erlauben mühelos eine Kabelverbindung. Damit wird auch das Internet-Signal deutlich stabiler, was man bei Videokonferenzen oder VoIP-Anwendungen schätzen wird.
Per Virtual Private Network (VPN) erreichen die Daten aus dem Homeoffice den Arbeitgeber. Dabei wird sichergestellt, dass Daten vor der Übertragung ins Internet in einen verschlüsselten Tunnel gepackt und nur verschlüsselt übermittelt werden. An Anfang und Ende lassen sich die Daten bearbeiten, während der Übertragung im öffentlichen Netz hat hingegen niemand Zugriff darauf. In der Regel stellen die Kommunen geeignete VPN-Lösungen zur Verfügung. Mit videma21 von IT-Dienstleister ekom21 können sie den Mitarbeitern alternativ gleich einen kompletten und gesicherten Remote-Arbeitsplatz anbieten. Fernzugriff ohne VPN erlauben sie in der Regel nicht. Denn wer ohne VPN arbeitet, geht im übertragenen Sinn ohne Badebekleidung schwimmen: Er zeigt schlicht alles.

Im Zweifel: Anruf

Während COVID-19 das gesellschaftliche und wirtschaftliche Leben erheblich einschränkt, kennt Cybercrime keine Krisen. Im Gegenteil, die Zahl der Angriffe steigt – was sicher auch damit zu tun hat, dass die Arbeit im Homeoffice zusätzliche Angriffspunkte bietet. Wer hat nicht in den vergangenen Monaten Werbe-E-Mails für Atemschutzmasken erhalten? Häufig handelt es sich dabei um Phishingmails,

die versuchen, Passwörter, TANs oder sonstige Transaktionsschlüssel zu stehlen. Ebenso schlimm ist das Einschleusen von Schad-Software per E-Mail-Anhang. Ein unbedachter Klick kann zur Folge haben, dass Ransomware die Festplatte verschlüsselt. Der beste Schutz ist Misstrauen. Unbekannte Mitteilungen sollten nicht geöffnet werden. Wer E-Mails von einer fremden Bank erhält, wird gewarnt sein. Aber viele E-Mails kommen mittlerweile in täuschend echtem Layout und in tadelloser Sprache daher. Da Phishingmails also immer schwerer zu erkennen sind, sollte man sich im Zweifel telefonisch beim Absender rückversichern.

Analog absichern

Angriffe erfolgen aber nicht nur digital. Das BSI warnt in seinen Handreichungen ebenso vor physischen Risiken und rät zu „Maßnahmen, mit denen sich ein Sicherheitsniveau erreichen lässt, das mit einem Büroraum vergleichbar ist. Verschließen Sie Türen, wenn Sie den Arbeitsplatz verlassen, geben Sie Dritten keine Chancen durch einsehbare oder gar geöffnete Fenster.“ Es mag unwahrscheinlich anmuten, dass jemand durch das Fenster einsteigt und die aktuelle Wasserverordnung stiehlt. Aber kommunale Informationen – der Bebauungsplan, Sitzungsprotokolle, Finanzdaten und dergleichen – sind hochsensibel. Oft genügt schon ein Blick, um wertvolle Kenntnisse zu erlangen. Wer Bahn fährt, hat bestimmt schon ungewollt Umsatzzahlen gesehen, die der Mitreisende gegenüber gerade bearbeitet. Dagegen helfen eine Sichtfolie und die Windows-Taste plus L. Dann ist nämlich der Bildschirm mit Passwort blockiert. Kinder im Homeoffice? Das Sperren des Rechners hilft dann auch gegen Datenverluste. Zu ärgerlich ist es nämlich, wenn Filius oder Filia Spaß am Tippen haben und versehentlich stundenlange Arbeit zerstören.

Datenverlusten vorbeugen

Datensicherung ist ein weiterer wichtiger Aspekt bei der IT-Sicherheit im Homeoffice. Idealerweise arbeitet man live auf den Produktionssystemen der Organisation. Bei videma21 ist das ohnehin der Fall, in anderen Fällen hilft das VPN. Damit sind Datenverluste praktisch ausgeschlossen und nach einem Virenbefall lassen sich die Daten wiederherstellen. Wer auf lokalen Medien speichert, tut sich keinen Gefallen und macht sich unter Umständen sogar strafbar. Das gilt vor allem für beliebte Online-Speicher wie OneDrive, Google Drive oder Dropbox. Die mögen bequem sein, doch hat der Europäische Gerichtshof die als Privacy Shield bekannte Datenschutzregelung mit den USA – wo viele der Service-Anbieter sitzen – für ungültig erklärt. Mit der ebox21 stellt etwa ekom21 einen ebenfalls komfortablen, aber zugleich sicheren Dienst für Datenspeicherung und -austausch bereit.

Sicher kommunizieren

Sichere Kommunikation ist das A und O im Homeoffice. In der Regel bekommen Verwaltungsmitarbeiter und Mandatsträger Hard- und Software gestellt, die eigens für die benötigten Aufgaben ein zertifiziertes Sicherheitsniveau haben. Klar ist die Verlockung groß, mal eben einen alternativen Kommunikationsweg aus der privaten Welt zu nutzen. Chat- und Messenger-Dienste bergen aber deutliche Sicherheitsrisiken. Nutzer sollten sich im Homeoffice deshalb an die bereitgestellte Technik der Organisation halten und nur die zugelassenen Dienste nutzen. Denn dahinter stehen in der Regel ein erfahrener Dienstleister, ein Sicherheitskonzept und Support-Experten. Sicherheitslücken entstehen zudem, wenn Updates nicht eingespielt werden. Ein Support-Team macht das meist automatisch im Hintergrund, sodass sich Experten im Homeoffice auf ihre Dienstgeschäfte konzentrieren können und zu aller Zusatzbelastung nicht auch noch einen Schnellkurs in IT-Administration belegen müssen.

()

Dieser Beitrag ist in der Ausgabe März 2021 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Homeoffice, Datenschutz, videma21