IT-Sicherheit

Risiken im Homeoffice

[14.09.2020] Viele Mitarbeiter wurden in den vergangenen Monaten ins Homeoffice geschickt und von dort an das Behördennetzwerk angeschlossen. Sicherheitsaspekte spielten zunächst keine große Rolle. Das BSI rät nun, verpflichtende Sicherheitsrichtlinien auszugeben.

Die Corona-Krise hat der Arbeitswelt zwangsweise einen Digitalisierungsschub verpasst. Damit Unternehmen und Organisationen weiterhin produktiv und funktionstüchtig bleiben, war es notwendig, die aus Gründen des Infektionsschutzes ins Homeoffice geschickten Mitarbeiter an die institutionellen Netzwerke anzuschließen. Das musste anfangs schnell vonstattengehen, Cyber-Sicherheit spielte zunächst eine untergeordnete Rolle. Wenn man sich vor Augen hält, welche Anstrengungen Firmen, Verwaltungen oder IT-Dienstleister unternehmen, um ein Gütesiegel für IT-Sicherheit – etwa das Grundschutz-Zertifikat des Bundesamts für Sicherheit in der Informationstechnik (BSI) – zu erhalten, darf diese Nachlässigkeit schon erstaunen. Am Arbeitsplatz in der Behörde wird jeder USB-Stick, der in den Rechner gesteckt wird, penibel protokolliert. Im Homeoffice war man jetzt aber über jede halbwegs funktionierende Videokonferenzverbindung heilfroh.

Hinreichende Regelungen

Bereits Ende März gab das BSI erste Hinweise zur IT-Sicherheit an Homeoffice-Arbeitsplätzen und empfahl Institutionen ohne hinreichende Regelungen für die Telearbeit, sich dringend mit IT- und Arbeitsschutz zu befassen. Die Empfehlungen reichen von Regelungen über die Art der Informationen, die außerhalb der Arbeitsstelle bearbeitet werden dürfen (Papier, Daten), sowie die dafür erlaubten Kommunikationsmittel bis hin zu einer verpflichtenden Sicherheitsrichtlinie. Diese sollte auch für die Gefahren sensibilisieren, die mit Telearbeit verbunden sind. Das betrifft sowohl den Zugang zu Daten und Datenträgern, als auch den Umgang mit Informationen beispielsweise bei der Vernichtung von Daten. Außerdem sollte ein Zutritts- und Zugriffsschutz eingerichtet werden, da Homeoffice-Plätze oftmals nicht der Sicherheit in Büroräumen entsprechen. Standardmaßnahmen zum Schutz der IT-Systeme etwa durch Software-Patches und Virenschutz sowie die Verschlüsselung von tragbaren IT-Systemen und Datenträgern und Routinen der Datensicherung verstehen sich offensichtlich auch nicht von selbst.

Updates für Anwendungen

Das Software-Unternehmen Kaspersky, Spezialist für Sicherheitslösungen, hat ebenfalls darauf aufmerksam gemacht, dass Virenschutzprogramme, Updates für Anwendungen und Betriebssysteme, WLAN-Verschlüsselung und die Änderung von Router-Anmeldedaten zu den notwendigen Vorsorgemaßnahmen in puncto IT-Sicherheit im Homeoffice zählen. In öffentlichen Netzwerken, etwa Cafés oder Bibliotheken, sollte man nur via Virtual Private Network (VPN) mit dem Verwaltungsnetzwerk verbunden sein, da öffentliche WLANs meist unverschlüsselt sind.
VPNs sind im kommunalen Raum freilich schon lange Standard bei der Datenkommunikation. Die Kommunen und ihre Dienstleister hatten zu Beginn der Pandemie schnell reagiert und mengenmäßig nachgelegt. So erhöhte die ITK Rheinland die Zahl der regelmäßigen VPN-Nutzer von 400 auf 1.800 und übernahm den Roll-out von 15.000 iPads für Düsseldorfer Schulen. Die KDO realisierte 1.000 zusätzliche Homeoffice-Plätze. Die Stadt Stuttgart baute die VPN-Zugänge auf 5.800 aus und die Zahl der

Telearbeitsplätze von 200 auf 2.000. Und Ende Juni veröffentlichte die Landesregierung Rheinland-Pfalz einen Resilienzbericht, aus dem hervorgeht, dass in dem Bundesland die Zahl der Homeoffice-Plätze im öffentlichen Sektor von 5.000 auf bemerkenswerte 15.000 erhöht wurde. Zudem seien 105 Videokonferenzräume und 83 Audioräume eingerichtet worden.

Erhöhte Achtsamkeit

Neben harten technischen Faktoren spielen auch softe Maßnahmen und Verhaltensregeln bei der IT-Sicherheit eine Rolle. So empfiehlt Kaspersky, die Sperrfunktion am Rechner zu nutzen, wann immer man sich vom Gerät entfernt. Zudem sei eine erhöhte Achtsamkeit für die Gefahren von Cyber-Kriminalität etwa durch E-Mail-Phishing angeraten. Für den E-Mail-Verkehr und Austausch von Dokumenten sollten allein die Firmenressourcen genutzt werden und keine Privatgeräte. Um Dokumente elektronisch zu verschicken, müssen diese in digitaler Form vorliegen, etwa als E-Akte. Das ist in vielen Kommunen noch nicht der Fall, sodass auch hier – schwer überprüfbare – Zugriffsregelungen auf die Papierakten im privaten Homeoffice notwendig werden. Dass in der jetzigen Situation keine ergonomische Maßstäbe an Telearbeitsplätze angelegt werden, wie sie sonst in der Verwaltung üblich sind, ist allerdings verständlich.

Rechtsgrundlage entzogen

Die Sicherheitsvorkehrungen mögen noch so umsichtig sein, und nützen doch wenig, wenn der Datenschutz nicht stimmt. Der Europäische Gerichtshof (EuGH) hat im Juli das Privacy-Shield-Abkommen zwischen der EU und den USA für ungültig erklärt und somit dem transatlantischen Datenverkehr die Rechtsgrundlage entzogen. Man geht davon aus, dass personenbezogene Daten in den USA nicht sicher vor dem Zugriff von Geheimdiensten sind. Unlängst hatte die Berliner Datenschutzbeauftragte Maja Smoltczyk eine Kurzprüfung von Videokonferenzsystemen veranlasst und war zu dem Ergebnis gekommen, dass eine rechtskonforme Nutzung der Dienste nicht möglich sei. Nach der EU-Datenschutz-Grundverordnung (DSGVO) müssen Anbieter vollständig weisungsgebunden arbeiten und dürfen personenbezogene Daten nicht zu eigenen Zwecken oder Zwecken Dritter weiterverarbeiten. Tatsächlich fließen aber vielfach zumindest Angaben zur Teilnehmerzahl, Länge der Videokonferenz, IP-Adresse und dem Standort der Teilnehmer an die Anbieter, die größtenteils in den USA sitzen.

Ungewollter Datenfluss

Das Problem gilt allerdings für Arbeitsplätze im Unternehmen wie im Homeoffice gleichermaßen. Einige Anbieter ermöglichen den Kauf von Software on premise, die dann auf den eigenen Servern läuft statt in der Cloud. Damit kann ein ungewollter Datenfluss weitgehend unterbunden werden, doch längst sind nicht alle Sicherheitsrisiken aus der Welt geschafft, die das Homeoffice bereithält. Beim Videokonferenz-Anbieter Zoom war es eine Zeit lang möglich, sich in fremde Konferenzen zu schalten, bis schließlich ein Passwortschutz eingerichtet wurde. Auch Anbieter wie Cisco Webex, Microsoft Teams oder Google Hangouts fallen in puncto Ende-zu-Ende-Datenverschlüsselung durch, die bei Video-Gruppenchats tatsächlich eine technische Herausforderung ist. Kollaborationstools wie Slack oder Trello haben sich ebenfalls als problematisch erwiesen, da sie sensible Daten in temporäre Dateien schreiben und dadurch ein Sicherheitsrisiko darstellen. Trello überträgt zudem Metadaten an mehrere Tracking-Dienste inklusive Gerätemodell, Betriebssystem, Netzbetreiber und Werbe-ID.
Zur Wahrheit gehört aber auch, dass die Angebote sehr komfortabel und schnelle Alternativen mit höherem Sicherheitsniveau nicht in Sicht sind. Insofern kann die Devise nur „mehr ist weniger“ lauten: Je umsichtiger und bewusster mit potenziellen Gefahren umgegangen wird, desto geringer ist das potenzielle Risiko. Die Berliner Datenschützerin Smoltzyk gab beispielsweise zu bedenken, dass Telefon- gegenüber

Videokonferenzen deutlich datenschutzkonformer seien.

()

Zu den Tipps des Bundesamts für Sicherheit in der Informationstechnik für sicheres mobiles Arbeiten

Dieser Beitrag ist in der Ausgabe September 2020 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder abonnieren.

Stichwörter: IT-Sicherheit, BSI, Homeoffice