Serie Cyber-Sicherheit

Achtung, Homeoffice!

[16.01.2023] Auch im heimischen Büro lauern Gefahren durch Cyber-Angriffe. Neben den IT-Verantwortlichen ist jeder Einzelne gefordert, für IT-Sicherheit im Homeoffice zu sorgen. Der Beitrag beschreibt Angriffsphänomene und gibt Tipps für das Verhalten im Verdachtsfall.

Homeoffice, Telearbeit, mobiles Arbeiten – nicht erst seit der Corona-Pandemie gibt es für viele Beschäftigte im öffentlichen Dienst die Möglichkeit, von zu Hause aus zu arbeiten. Doch auch im heimischen Büro lauern Gefahren durch Cyber-Angriffe, mit denen sich die Mitarbeiterinnen und Mitarbeiter oft eigenverantwortlich auseinandersetzen müssen. In den meisten Kommunen gibt es zumindest eine IT-Fachkraft oder einen Dienstleister, der sich um die Server- und Netzwerkarchitektur kümmert und diese fachgerecht einrichtet. Im privaten Zuhause ist dies eher selten der Fall. Der IT-Experte hat keinen Einblick in die Einstellungen des heimischen Netzwerks. Hierdurch können Sicherheitslücken entstehen, die Angreifer ausnutzen. Mit dem Abschluss eines Vertrags über einen Internet-Anschluss erhält man den in den Firmenfarben des Internet-Anbieters gehaltenen Router. Sobald man diesen erfolgreich installiert und die Endgeräte im Netzwerk anmeldet, hat man Internet-Zugriff. Die einzelnen Endgeräte senden Anfragen an den Router, dieser leitet die Anfragen an das Internet weiter und schickt die angeforderten Daten an das Endgerät zurück. **Zunächst Überblick verschaffen** Inzwischen tummeln sich im heimischen Netzwerk oft viel mehr Geräte als uns bewusst ist. Drucker, Computer, Handy, Tablet, Fernseher, Heizung, Spielekonsolen, Kühlschränke – fast alle modernen Geräte haben Internet-Zugang und schicken sekündlich Anfragen an den Router oder senden Daten an die Hersteller und deren Partner. Manchmal tun sie das, weil es zur Bereitstellung eines Diensts notwendig ist, oftmals jedoch auch, weil die Hersteller und deren Partner persönliche Kundenprofile erstellen, um gezielter werben zu können. In dieses unübersichtliche und für den IT-Betrieb der Kommune nicht zu kontrollierende, private Netzwerk wird nun ein dienstliches Endgerät eingeführt. Jedes Gerät in diesem Netzwerk ist ein potenzielles Einfallstor für Cyber-Kriminelle. Gelingt dem Angreifer ein Zugriff auf die Spielekonsole oder das Smart-TV, dann hat er einen Brückenkopf, von dem aus er die anderen Geräte angreifen kann. Eine erste Maßnahme zur Abhilfe ist es, sich einen Überblick zu verschaffen, welche Geräte Internet-Zugang haben. Die von den Herstellern vergebenen Passwörter des Routers und aller Geräte mit Internet-Zugang sollten geändert und die Betriebssoftware regelmäßig aktualisiert werden. Wo möglich, sollte über die Einstellungen begrenzt werden, welche Daten an wen gesendet werden. Mehr Sicherheit erreicht man durch die Einrichtung einer Firewall oder die Unterteilung des Netzwerks in Zonen (Netzwerksegmentierung). Viele Privathaushalte haben einen Gastzugang in ihrem WLAN eingerichtet. Die Einrichtung eines Netzwerkzugangs, in dem sich nur dienstliche Geräte anmelden, ist oftmals analog möglich. Der IT-Verantwortliche der Kommune sollte die Dienstgeräte so konfigurieren, dass aus fremden Netzen heraus nur über eine VPN-Verbindung Zugang in das Verwaltungsnetz hergestellt werden kann, im Idealfall beschränkt auf dienstliche Endgeräte. **Keine fremden USB-Sticks verwenden** Beim Virtual Private Network (VPN) handelt es sich um ein privates, in sich geschlossenes Netzwerk, welches ein bestehendes Kommunikationsnetz nutzt und daher nur virtuell besteht. Der sich im privaten Netzwerk befindliche Rechner einer Mitarbeiterin oder eines Mitarbeiters erhält über VPN Zugriff auf das Netzwerk, die Daten und Anwendungen der Dienststelle. Hierdurch hat die Dienststelle Einfluss auf Verschlüsselung und Übertragungsprotokoll und kann so eine abhör- und manipulationssichere Kommunikation gewährleisten. In der Pandemie kam die Umstellung auf Homeoffice für viele Kommunen unglaublich

plötzlich. Für die Beschäftigten standen oft nicht ausreichend dienstliche Endgeräte zur Verfügung, sodass notgedrungen auch private Endgeräte zum Einsatz kamen. Im Normalbetrieb sollte dies vermieden werden. Sobald mobiles Arbeiten zum Normalfall wird, sollten dienstliche Endgeräte zur Verfügung stehen, deren Verwaltung durch die IT-Verantwortlichen der Kommune erfolgt. Wenn eine Nutzung privater Endgeräte nicht vermieden werden kann, müssen feste Regelungen getroffen werden, beispielsweise darüber, wie schnell Software Updates zu installieren sind oder ob der Arbeitgeber im Notfall das gesamte Endgerät inklusive aller privaten Daten remote löschen darf. Der dienstliche und private Gebrauch sollten soweit wie möglich getrennt werden. Für Datenübertragungen zwischen privaten und dienstlichen Geräten bedarf es gesonderter Regelungen, zum Beispiel einer datenschutzrechtlich geprüften Filesharing-Lösung in der Cloud, der Nutzung von VPN-Verbindungen oder der ausschließlichen Verwendung bereitgestellter USB-Sticks. Diese sollten, nachdem sie an einen externen Rechner angeschlossen waren, auf Schad-Software geprüft werden, bevor sie an einen Dienstrechner angeschlossen werden. Fremde, gefundene oder geschenkte Sticks sollten niemals verwendet werden. Cyber-Kriminelle nutzen sie gerne zum Einschleusen von Schad-Software. Das Abfotografieren von Unterlagen mit dem (Privat)-Handy, um diese von zu Hause aus weiter zu verarbeiten, sollte ebenfalls untersagt und der Umgang mit Papierakten im Homeoffice klar geregelt werden. **Angriffsfläche Homeoffice** Die Distanz und Isolation, die durch das mobile Arbeiten entstehen können, werden von Cyber-Kriminellen bewusst ausgenutzt. Es gibt einige Angriffsphänomene, welche besonders bei der Arbeit von zu Hause zur Herausforderung werden können. CEO Fraud ist eine Art von Phishing. Dabei bringen Cyber-Kriminelle zunächst in Erfahrung, wie das Unternehmen strukturiert ist. Hierzu nutzen sie unter anderem Internet-Seiten, Pressemitteilungen, Medienberichte und öffentlich einsehbare Organigramme. Mit diesen Informationen können sie sich zum Beispiel als Bürgermeister ausgeben. Per E-Mail mit gefälschtem Absender schreiben sie Beschäftigte an und geben ihnen die Anweisung, hohe Geldbeträge zu überweisen oder wichtige Unterlagen zu schicken. Abhilfe schaffen gut geschultes Personal, welches das Phänomen CEO Fraud erkennt, sowie feste Kommunikationswege und Abläufe, die auch von Vorgesetzten konsequent eingehalten werden. Eine Überweisung oder der Versand von wichtigen Daten auf Zuruf sollte so ungewöhnlich sein, dass eine solche Aufforderung sofort misstrauisch macht. Diese verbindlichen Verhaltensregeln und direkten Kommunikationswege, auf denen man sich schnell, etwa durch einen Anruf, rückversichern kann, können Kommunen vor finanziellen Schäden in Millionenhöhe bewahren. Bei einem Man-in-the-Middle(MITM)-Angriff schaltet sich der Angreifer unbemerkt in die Mitte einer Kommunikation. Er empfängt die Nachrichten des Senders und leitet diese weiter, ohne dass Sender und Empfänger sich dessen bewusst sind. Cyber-Kriminelle können so Kommunikation mitlesen und sich unbemerkt in diese einschalten. Phishing- und CEO-Fraud-E-Mails können ganze Verläufe enthalten und dem Empfänger wie eine reale Antwort auf eine von ihm gesendete Nachricht erscheinen. Besonders anfällig für MITM-Angriffe sind öffentlich zugängliche WLAN-Hotspots. Cyber-Kriminelle können sich jedoch auch Kontrolle über den Router eines privaten Netzwerks verschaffen oder einen eigenen WLAN-Hotspot mit einem offiziell anmutenden Namen einrichten und so die Kommunikation über sich umleiten. Man-in-the-Middle-Angriffe lassen sich durch eine Verschlüsselung der über das Netzwerk verschickten Datenpakete verhindern. **Grundregeln bei Verdachtsfällen** Es gibt einige Maßnahmen, die Dienststelle und Mitarbeitende treffen können, um das mobile Arbeiten sicherer zu gestalten. Doch was, wenn es trotzdem zu einem IT-Sicherheitsvorfall kommt? Es ist eine dringende Führungsaufgabe, gemeinsam mit den IT-Experten Verhaltensregeln bei IT-Sicherheitsvorfällen festzulegen und den Beschäftigten zu kommunizieren. Hessen3C empfiehlt bei Verdachtsfällen oder Sicherheitsproblemen einige Grundregeln. Erstens: den Rechner vom Netzwerk trennen, indem das LAN-Kabel entfernt und die Verbindung über WLAN und mobile Daten manuell unterbrochen wird. Hierdurch wird eine Ausbreitung der Schad-Software eingedämmt. Zweitens: den Rechner nicht herunterfahren, da sonst wichtige Daten für die forensische

Analyse verloren gehen können. Die Ergebnisse der forensischen Analyse erlauben eine Bewertung des Schadens und gegebenenfalls eine Strafverfolgung. Drittens: eine vorab benannte Ansprechperson für IT-Sicherheitsvorfälle informieren. Die Kontaktdaten müssen den Mitarbeiterinnen und Mitarbeitern zu Hause auch ohne Zugang zu Internet und Intranet vorliegen. Diese Stelle entscheidet über weitere Schritte. In Hessen können sich Kommunen zudem an die rund um die Uhr besetzte Hotline des Hessen3C wenden.

()

Weitere Teile der Serie Cyber-Sicherheit
Das Hessen CyberCompetenceCenter (Hessen3C)

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, Hessen CyberCompetenceCenter, Hessen CyberCompetenceCenter (Hessen3C) Serie Cyber-Sicherheit