Hackerangriff am Küchentisch

Autor(en): **Staub, Michael**

Objekttyp: **Article**

Zeitschrift: **Wohnen**

Band (Jahr): **96 (2021)**

Heft 4: **Sicherheit**

PDF erstellt am: **05.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-977380

Bild: istockphoto

Der sorglose Umgang mit Daten im Homeoffice birgt Risiken für die IT-Sicherheit.

Baugenossenschaften sollten sensible Daten besonders schützen

Hackerangriff am Küchentisch

Zur «neuen Normalität» gehört auch für viele Baugenossenschaften das Homeoffice. Andere erledigen die Verwaltungsarbeit seit je im Nebenamt von zuhause aus. Doch wenn die Wohnung zum Arbeitsplatz wird, hat dies auch Folgen für die IT-Sicherheit. Drei Fachleute erläutern, worauf besonders zu achten ist.

Von Michael Staub

Noch zu Beginn des letzten Jahres war Homeoffice das Privileg einer Minderheit. Zwei Pandemiewellen später wird es vom Bundesrat wenn immer möglich verlangt. Der Arbeitstag findet in den eigenen vier Wänden statt. Den Arbeitnehmerinnen und Arbeitnehmern bringt das durchaus Vorteile: Das Pendeln zum Arbeitsplatz entfällt, die eigene Zeiteinteilung ist in der Regel flexibler, und nicht selten wird auch der private Alltag entspannter. Als Nachteile werden häufig die fehlenden oder stark eingeschränkten sozialen Kontakte, die verschwimmende Grenze zwischen Arbeits- und Privatleben oder der fehlende persönliche Austausch genannt. Eher selten ist die IT-Sicherheit ein Thema. Doch bereits während der ersten Coronawelle im Frühling 2020 war in Europa ein deutlicher Anstieg von Meldungen zu Cyberangriffen festzustellen. Anscheinend begünstigt das Homeoffice solche Attacken auf die IT-Infrastruktur. Woran liegt dies, und wie können sich Baugenossenschaften dagegen wappnen?

Dezentralisierte Sicherheit

Solange alle Angestellten im Büro arbeiten, ist die IT-Sicherheitslage relativ überschaubar. In der Regel werden identische Computer und

Mobilgeräte mit abgestuften Berechtigungen verwendet. Sicherheitslücken können dank automatischen Updates schnell geschlossen werden, und die Verbindungen zur Aussenwelt können gut abgesichert werden, etwa mit einer Firewall (Blockieren unerwünschter Zugriffe) oder einem Virenscanner (Blockieren von schädlicher Software). Zudem unterliegt der physische Zugang zu den Arbeitsplätzen und zur IT-Infrastruktur einer gewissen Kontrolle. Ganz anders sieht es hingegen aus, wenn das Büro gewissermassen auf ein Dutzend verschiedene Homeoffices dezentralisiert wird. Nun arbeiten alle von ihrem eigenen Netzwerk aus und verwenden private Anschlüsse und Infrastrukturen.

Welche Folgen hat diese Verlagerung ins Private? Hannes Lubich ist emeritierter Professor an der Fachhochschule Nordwestschweiz (FHNW) und Spezialist für IT-Sicherheit. Er fasst die Sicherheitsproblematik in drei Stichworten zusammen: «Ausrüstung, Nutzung und Vertraulichkeit». Erstens werde für die Arbeit zuhause oft die eigene Ausrüstung verwendet, etwa private Laptops, Tablets oder Internetrouter: «Der Arbeitgeber weiss nichts über die Sicherheit und Zuverlässigkeit dieser Geräte. Er darf und kann sie auch nicht überwachen, auf den neusten Stand bringen oder deaktivieren.» Zweitens würden private Netzwerke meistens auch von Drittpersonen genutzt: «Familienmitglieder oder Mitbewohner sind nicht an die Vorschriften und Sorgfaltspflichten des Arbeitgebers gebunden. Man weiss schlicht nicht, wer sich im selben Netzwerk oder auf anderen gemeinsam genutzten Infrastrukturen bewegt.» Drittens sei die Vertraulichkeit beim Arbeiten am Küchentisch oder im Kinderzimmer reduziert: «Heimarbeitsplätze sind oft nicht geeignet, um sensitive Daten zu bearbeiten.»

Sichere «Tunnel»

Ein bekanntes Mittel gegen einige dieser Risiken sind Virtual Private Networks (VPN). Damit wird der gesamte Datenverkehr gewissermassen durch einen Tunnel direkt ins Firmennetzwerk geleitet. So hat man auch von zuhause den gewohnten Zugriff auf Server, Dateien oder Kontakte. In einigen Branchen sind solche VPN-Verbindungen schon länger Standard. Sie reichten für sich allein jedoch längst nicht aus, wie Hannes Lubich anmerkt. So brauche es etwa eine Mehrfach-Faktor-Autorisierung aller Zugriffe von ausserhalb der Firma (siehe Infobox). Auf allen beteiligten Geräten – Laptops, Smartphones, Tablets, aber auch Internetrouter – müsse die aktuelle Software aufgespielt sein. «Daneben braucht es spezielle Schutzsoftware für die Geräte, etwa eine Firewall oder ein Anti-Schadsoftware-Programm», erläutert Lubich. Nicht zuletzt müsse man auch dafür sorgen, dass sämtliche Zugriffe aus dem Homeoffice gut überwacht und fälschungssicher protokolliert würden.

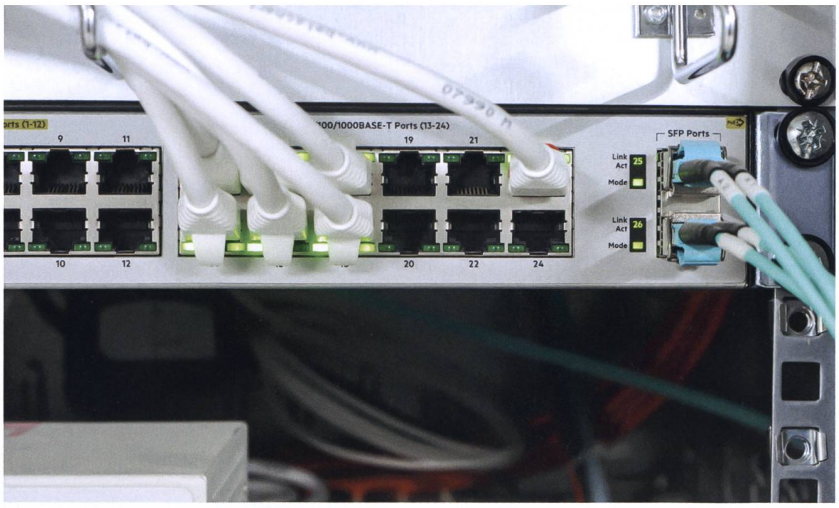

Bild: Michael Staub

Private Netzwerke können vom Arbeitgeber nicht überwacht werden.

Doch wie gut sind die Firmen für das sichere Arbeiten im Homeoffice gerüstet? «Während des Lockdowns im letzten Frühling waren viele Unternehmen mit der Situation überfordert. Derzeit haben wir den Eindruck, dass sich die Situation etwas entspannt hat», sagt Max Klaus, stellvertretender Leiter Operative Cybersicherheit (OCS) beim Nationalen Zentrum für Cybersicherheit (NCSC) (siehe auch «Nachgefragt»). Die benötigten Lösungen, etwa für VPN oder Videokonferenzen, sowie mobile Geräte seien vielerorts beschafft worden und stünden nun im Einsatz. «Wichtig ist der sogenannte Grundschutz, und zwar im normalen Büro ebenso wie im Homeoffice», sagt Klaus. Dieser umfasst den Einsatz von Virenscannern und Firewalls sowie die regelmässige Datensicherung und das möglichst rasche Aktualisieren aller Systeme und Geräte mit Software-Updates.

Mehr Faktoren für mehr Sicherheit

Benutzername und Passwort schienen lange Zeit eine ausreichende IT-Sicherheit zu gewährleisten. Doch beide Elemente können erraten beziehungsweise mit automatisiertem Ausprobieren («brute force») geknackt werden. Deshalb setzt sich immer mehr die sogenannte Zwei-Faktor-Authentifizierung durch. Sie arbeitet mit zwei der folgenden Faktoren:

- Wissen (zum Beispiel ein Passwort oder eine PIN)
- Besitz (ein physisches Objekt wie ein Smartphone oder ein elektronischer Schlüssel)
- Biometrie (eine persönliche Eigenschaft wie Fingerabdruck oder Handvenenmuster)
- Ort (ein bestimmter geografischer Ort – zum Beispiel der Hauptsitz der Firma)

Ein einfaches Beispiel für die Zwei-Faktor-Authentifizierung ist der Bargeldbezug am Bancomaten: Hier werden eine EC-Karte (Besitz) und Wissen (PIN-Code) benötigt. Auch bei der Verwendung von VPN-Anwendungen ist meistens ein Passwort und ein weiterer Gegenstand für die Identifizierung (sogenannter Token) notwendig.

Kostenlose Verschlüsselung

Die pEp Foundation ist eine Stiftung, die sich für sichere Kommunikation via E-Mail einsetzt. Im Zug der Coronapandemie bietet sie KMU ihre E-Mail-Apps für iOS und Android kostenlos an. Es handelt sich um sogenannte Open-Source-Software. Das heisst, jede und jeder kann den Quellcode einsehen.
www.pep.foundation

Nachgefragt bei Max Klaus vom Nationalen Zentrum für Cybersicherheit (NCSC)

Besonders kritische Systeme schützen

Seit Beginn der Coronapandemie im letzten Frühling häufen sich Meldungen über Cyberangriffe. Wie beurteilen Sie die Lage?
Wir konnten einen deutlichen Anstieg an Meldungen feststellen. Die Zahl der tatsächlichen Cyberangriffe stieg jedoch nur leicht. Wir führen die gestiegene Zahl von Meldungen auf die höhere Sensibilität von Unternehmen und Privatpersonen zurück.

Inwiefern nutzen Cyberkriminelle die Pandemie für ihre Zwecke?
Wir haben einen deutlichen Anstieg von Cyberangriffen festgestellt, der sich auf die Pandemie bezieht. So gibt es beispielsweise Websites, die Dokumente mit angeblichen Coronafallzahlen zum Download anbieten. Ein Download führt dann mit einer Schadsoftware zu einer Infektion des Geräts. Zu erwähnen ist, dass dieser Bezug auf aktuelle Ereignisse eine beliebte Strategie von Cyberkriminellen ist. Sie versprechen sich davon eine höhere Glaubwürdigkeit für ihren Angriffsversuch und eine höhere Zahl potenzieller Opfer.

Für viele Firmen und Organisationen ist die IT-Sicherheit ein abstraktes Thema. Wie viel Schutz ist denn überhaupt nötig?
Oft herrscht die Meinung vor, man müsse das ganze Unternehmen wie Fort Knox schützen. Dies ist selten notwendig. Es lohnt sich, eine Risikoanalyse für die einzelnen IT-Systeme zu erstellen. Besonders kritische Systeme müssen entsprechend geschützt werden. Bei einer Baugenossenschaft könnte dies zum Beispiel die Immobilien- und Mieterinnenverwaltung sein. Weniger wichtige Systeme können mit einem entsprechend tieferen Schutz auskommen.

Auch ohne Cyberangriffe kann es im Homeoffice Probleme mit der Vertraulichkeit geben, etwa wenn geschäftliche Dokumente auf dem privaten Laptop bearbeitet werden. Welche Vorkehrungen empfehlen Sie dafür?
Private Geräte sollten dieselben Mindestanforderungen erfüllen wie Unternehmensgeräte – dazu gehört auch eine entsprechende Schutzsoftware. Zudem sollte ein Unternehmen definieren, welche Dokumente unter welchen Voraussetzungen auf privaten Geräten gelesen oder bearbeitet werden dürfen. Deshalb empfehlen wir, unbedingt eine Klassifikation von Dokumenten vorzunehmen. In der Bundesverwaltung sind dies zum Beispiel die Stufen «intern», «vertraulich» und «geheim». Je nach Klassifikation eines Dokumentes darf dieses dann zum Beispiel über E-Mail versendet werden oder eben nicht.

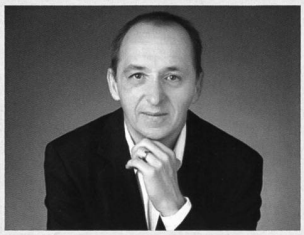

Bild: zVg.

Max Klaus ist stellvertretender Leiter Operative Cybersicherheit (OCS) beim Nationalen Zentrum für Cybersicherheit (NCSC). Das NCSC ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, die Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS).

Alle sind Ziel

Baugenossenschaften, die sich bisher eher zögerlich mit der IT-Sicherheit auseinandergesetzt haben, mögen den zusätzlichen Aufwand scheuen. Doch die Beschäftigung mit dem Thema sei dringend nötig, sagt Volker Birk, Pressesprecher beim Chaos Computer Club Schweiz (CCC Schweiz): «Es gibt zwar gezielte Attacken auf hochwertige Ziele, doch die meisten Angriffe laufen heute vollautomatisiert ab. Von diesen unspezifischen, aber sehr häufigen Angriffen sind Wohnbaugenossenschaften genauso betroffen wie jedes andere Unternehmen.» Zu den bekannten Gefahren gehören etwa das Bombardieren von Webservern mit Anfragen, bis diese zusammenbrechen («Distributed Denial of Service», DDoS) oder das Verschlüsseln beziehungsweise Verfälschen sämtlicher Daten auf den Firmensystemen durch einen Trojaner (Ransomware) inklusive hoher Lösegeldforderungen.

Selten seien solche Versuche nicht, wie Volker Birk berichtet. Sogar «normale» Webserver würden im Zwei- bis Dreiminutentakt angegriffen. Schwachstellen können sich fatal auswirken. Ein Grund dafür seien überholte Paradigmen für die IT-Sicherheit, sagt Birk. Denn seit rund 30 Jahren gelte die Doktrin der «perimeter-based security»: «Man versucht, das Firmennetz gegen aussen zu verteidigen, betrachtet die Computer innerhalb des Netzes aber als sicher. Diese Denke ist überholt. Heute muss man Computer auch innerhalb des Netzwerkes gegeneinander absichern.»

Umdenken nötig

Diese neue Sicherheitsarchitektur, die sogenannte Zero Trust Architecture, wird unter anderem vom National Institute of Standards and Technology (NIST) propagiert. Dieses US-amerikanische Institut findet zwar viel Gehör, doch die Umstellung aller Netzwerke und angeschlossener Systeme wird nach Schätzung von Volker Birk «die nächsten zehn Jahre benötigen». Der IT-Experte empfiehlt deshalb, wenigstens die E-Mail-Kommunikation angemessen zu verschlüsseln, etwa mit der kostenlosen Software der PEP-Stiftung, deren Präsident er ist (siehe Infobox). Die IT-Sicherheit auf die leichte Schulter zu nehmen, sei keine Option: «Wer glaubt, er müsse seine Computer nicht schützen, macht einen Denkfehler und wird diesen bitter bereuen.» ■

Bitte beachten Sie auch den Beitrag zu allen rechtlichen Fragen rund um Homeoffice auf Seite 36-37.

Publireportage

Mit vernetztem Licht Energie einsparen

Verschiedene Bauprojekte in der Stadt Zürich zeigen eindrücklich, wie dies in der Praxis aussehen kann. Ein Projektleiter einer grossen Immobilienverwaltung in der Stadt Zürich sagt dazu: «Wir sind sehr interessiert an Lösungen, welche nachweislich wirtschaftlich sind und sich in der Praxis bewähren.»

So wird beispielsweise in einer grösseren Einstellhalle im Zürcher Seefeld – wie Messungen gezeigt haben – nach der Sanierung der Beleuchtung 65 % weniger Energie verbraucht als vorher. Dabei wurde nicht etwa eine ineffiziente Beleuchtung saniert, sondern effiziente Leuchtstoffröhren mit Bewegungsmeldern, wie dies bis vor 10 Jahren dem neusten Stand der Technik entsprach. Die hier mittels intelligenten TRIVALITE Leuchten von Swisslux realisierte Energieeinsparung, kommt zum einen durch die höhere Effizienz der LED-Leuchten und zum anderen durch deren Vernetzung untereinander und das Schwarmverhalten der Leuchten zustande: Das Licht brennt stets nur dort wo Personen anwesend sind zu 100 %. Die direkt angrenzenden Bereiche werden nur so stark wie nötig erhellt, um die Raumorientierung und das Sicherheitsgefühl zu gewährleisten. Wo früher die Fläche der Einstellhalle für über 100 Fahrzeuge beim Betreten komplett erhellt wurde, wird jetzt im Schnitt nur noch rund ein Drittel der Energie benötigt und gleichzeitig eine deutlich bessere Ausleuchtung und Raumorientierung erzielt. «Seit wir auf intelligente Leuchten setzen, sparen wir sehr viel Energie ein und gleichzeitig ist die Zufriedenheit der Mieter viel grösser als vorher.», sagt der Leiter des technischen Dienstes des zuständigen Unternehmens.

Um die Ziele der Energiestrategie 2050 mit ihren Sanierungsprojekten zu unterstützen, setzen verantwortungsbewusste Bauherrschaften auf intelligente Leuchten, wie beispielsweise hier in einer Tiefgarage im Zentrum der Stadt Zürich, und sparen ab dem ersten Tag rund 65 % der Energie ein.

www.trivalite.ch

Swisslux AG
8618 Oetwil am See
www.swisslux.ch

TRIVALITE
SWISSLUX