Medienmitteilung Stuttgart 16.03.2020

Arbeiten im Homeoffice – Heimische Router gefährden IT-Sicherheit von Unternehmen

Durch den Ausbruch von COVID-19 arbeiten momentan immer mehr Arbeitnehmende aus dem Homeoffice. Der Workflow lässt sich meistens gut bewältigen. Aber durch die Verbindung eines externen Rechners mit dem Unternehmensnetzwerk entstehen Risiken für die Informationssicherheit. Einer der größten Schwachpunkte ist der Router im Homeoffice. IoT- Sicherheitsexperte Mirko Ross gibt Tipps, worauf Unternehmen und Mitarbeitende jetzt unbedingt achten sollten.

Immer mehr Unternehmen lassen ihre Mitarbeiterinnen und Mitarbeiter im Homeoffice arbeiten. So will man vermeiden, dass sich das Coronavirus am Arbeitsplatz ausbreitet und viele Menschen infiziert. Allerdings ergeben sich dadurch aber erhebliche Sicherheitsrisiken für die IT des Unternehmens: Denn durch Schwachstellen im Heimnetzwerk der Mitarbeitenden können Angreifer Zugriff auf vertrauliche Informationen erlangen.

Die Gefahr: Heimische Router ohne aktuelles Update

Der Goldstandard für die Verbindung zwischen Unternehmen und dem Laptop im Homeoffice ist der sichere Zugang über ein VPN. Aber: „Die VPN-Infrastruktur vieler Unternehmen ist nicht auf die Masse der plötzlich benötigen Homeoffice-Kapazitäten ausgelegt“, erklärt Mirko Ross, bekannter IoT- & Cybersecurity-Experte. „Viele Unternehmen raten daher ihren Mitarbeitenden im Moment, nur ‚kritische‘, also besonders sensible Arbeiten, über VPN zu erledigen und bei allen anderen Arbeiten auf ein VPN zu verzichten.“

In der Praxis müssen die Mitarbeitenden also vermehrt über den privaten heimischen Internetzugang arbeiten. Dabei ist vielen nicht bewusst, welche Sicherheitsrisiken mit dem heimischen Netzwerk verbunden sind. Der Internet-Router wird dabei leicht zum unsichersten Punkt im Homeoffice. Eine von Avast 2018 veröffentlichte Studie fand beispielsweise heraus, dass 60% der WLAN-Router problemlos angegriffen werden können.
Das verwundert nicht, denn jeder sechste Deutsche ist mit der Einrichtung seines WLAN-Routers überfordert, wie eine Umfrage der Sicherheitsfirma Kapersky 2019 ergab.

Aber selbst beim Arbeiten mit VPN kann der heimische Router eine Eintrittskarte für Angreifer in Unternehmen darstellen. Beispielsweise wenn Zugangsdaten zur Einrichtung des VPN ungesichert per E-Mail versendet werden und Angreifer diese als Man-in-The-Middle am schlecht gesicherten heimischen Router abgreifen können.

Einfache Hygienemaßnahmen schließen Sicherheitslücken

Mirko Ross rät Firmen deshalb, die Mitarbeitenden zu verpflichten, sich zuerst um die Sicherheit ihres Routers zu kümmern, bevor sie sich ins Unternehmenssystem einloggen: „Dabei geht es, ähnlich wie im Kampf gegen das Coronavirus, um Maßnahmen der Grundhygiene: Analog zum Händewaschen und Niesen in die Armbeuge muss man, um Angriffe von Hackern abzuwehren, den Router mit einem sicheren Passwort versehen und die Routerfirmware updaten.“

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Konkret ist dazu zunächst zu klären, ob der Router mit einer automatischen Firmware-Update-Funktion ausgestattet ist. Andernfalls muss man das Update selbst downloaden – und sich auch in Zukunft regelmäßig darum kümmern. Die zweite Schwachstelle – unsichere, zu kurze oder werksseitig eingestellte Passwörter – ist schnell zu schließen: Ein sicheres Passwort sollte aus einer zufälligen Kombination von Buchstaben, Ziffern und Sonderzeichen erstellt werden und mindestens 16 Zeichen lang sein.

Damit das klappt, empfiehlt Mirko Ross Sicherheitsverantwortlichen, die Mitarbeitenden durch Guide- lines und, wenn nötig, durch aktive Hilfestellung bei der Sicherung ihres Routers zu unterstützen. „Wer- den diese Regeln befolgt, kann man ohne großen Aufwand ein Haupteinfallstor schließen, das ansonsten für Angreifer weit offen steht. Diese kleine Investition zahlt sich also unbedingt aus!“

Abdruck honorarfrei, Beleg (Print, Scan) oder Link erbeten.

Mirko Ross ist ein international anerkannter Aktivist, Experte, Redner, Publizist und Forscher im Bereich Cybersicherheit und Internet der Dinge. Für die Sicherheit im IoT engagiert er sich als Mitglied der Experten-gruppe für Sicherheit im Internet der Dinge der Europäischen Cybersicherheitsbehörde ENISA.
Darüber hinaus ist Mirko Ross aktiv in internationalen Forschungsprojekten im Bereich Cybersicherheit und Blockchain-Technologien und Gründer sowie CEO des Cybersicherheits-Start-ups asvin.

Bild:


Portrait Mirko Ross, CEO asvin GmbH

Kontakt:

seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (bei Stuttgart)
T: +40 (0)7181 / 26 29 376
E: medien@seidel-kommunikation.de