Im Homeoffice

Massive Schwachpunkte in der Homeoffice-Absicherung auf – Smarte Haushaltsgeräte sind trojanische Pferde für Hacker

Millionen Arbeitsplätze wurden im Zuge der Corona-Pandemie in die heimischen vier Wände verlagert. Während vor der Krise nur knapp vier Prozent von zuhause arbeiteten, ist mittlerweile ein Viertel der Beschäftigten in Deutschland im Home Office. Ein Großteil der Haushalte nutzt dabei smarte Devices mit Anbindung an das heimische Netzwerk – Router, smarte Staubsauger, Mediensysteme, Lichtsteuerungen oder smarte Schließanlagen. Neun von zehn dieser Geräte weisen allerdings eklatante Sicherheitslücken in der Firmware auf, ergaben Untersuchungen des IoT-Security-Spezialisten IoT Inspector.

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

FragAttacks - Neue WLAN-Schwachstellen

Nachezu alle WLAN-Geräte betroffen

CSW-Nr. 2021-216748-1032, Version 1.0, 11.05.2021

IT-Bedrohungslage*: 3 / Orange

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten

BSI warnt vor Schwachstellen in WLAN-Routern

Sicherheitsmaßnahmen oder Richtlinien für solche Einfallstore gibt es kaum in den Unternehmen, ein Bewusstsein für das Risiko ist nicht vorhanden – 71 Prozent der Unternehmensvertreter sind sicher, dass traditionelle Sicherheitsmechanismen nicht mehr ausreichend sind, um Risiken durch IoT Devices ebenfalls abzudecken. Ebenfalls 71 Prozent sind der Meinung, dass die Maßnahmen zur Absicherung von IoT Devices nicht ausreichend sind. Sieben Prozent geben sogar die Schulnote „mangelhaft", nur 12 Prozent der Befragten halten die Maßnahmen für ausreichend.

Die jüngsten Warnungen des Bundesamts für Sicherheit in der Informationstechnik vom 12. Mai unterstreichen diese Einschätzungen. Das BSI veröffentlicht eine ausdrückliche Warnung der Stufe 3 – „die IT-Bedro-

hungslage ist geschäftskritisch“. KLICKEN Sie einfach auf das Bild und die BSI-Warnung öffnet sich als PDF Die Schwachstelle für sogenannte „FragAttacks“ betrifft WLAN-Router fast aller Hersteller.

Home Office als Schlüssel zum Firmennetzwerk

Für die Studie „(I)IoT Sicherheitsreport 2021“ wurden 260 Unternehmen aus der IT-Branche befragt – 57 Prozent sehen in diesen Devices ein Risiko für Hacker-Attacken auf Unternehmensnetzwerke. „Diese smarten Haushalts- und Heimgeräte sind ein trojanisches Pferd, mit dem Hacker relativ leicht Zugang zu einem WLAN-Netzwerk im Haushalt bekommen. Darüber lassen sich eingebundene Computer attackieren, und letztlich auch Firmennetzwerke, auf die beispielsweise per VPN zugegriffen wird“, erklärt Rainer M. Richter, Geschäftsführer von IoT Inspector.

57 Prozent der Befragten halten zwar eine VPN-Verbindung für sicher, jedoch hält keiner der 260 befragten UnternehmensvertreterInnen diese Form der Verschlüsselung für „sehr sicher“. 30 Prozent hingegen klassifizieren die Verschlüsselung als „weniger sicher“ oder sogar „unsicher“. „Der Zugriff auf das lokale Heimnetzwerk und die Infektion eines Rechners darin sind der Schlüssel zum Firmennetzwerk. Ist das passiert, schützt beim gewöhnlichen Unternehmens-Setup selten noch etwas vor Attacken mit Ransomware oder anderer Schadsoftware“, analysiert Rainer M. Richter. Mit der IoT Inspector Plattform ermöglicht sein Unternehmen die einmalige oder laufende Überprüfung der Firmware solcher IoT Geräte auf Sicherheitslücken und mögliche Einfallstore für Cyber-Kriminelle. Die Lücken reichen dabei vom problemlos im Klartext lesbaren WLAN-Schlüssel bis zum versteckten Administratoren-Zugang in der Firmware, mit dem Hacker in wenigen Minuten beginnen können, ihr Unwesen zu treiben.

Über IoT Inspector

Die Technologie von IoT Inspector ermöglicht mit wenigen Mausklicks eine automatisierte Firmware-Prüfung von IoT-Devices auf kritische Sicherheitslücken. Der integrierte Compliance Checker deckt gleichzeitig Verletzungen internationaler Compliance-Vorgaben auf. Schwachstellen für Angriffe von außen und Sicherheitsrisiken werden in kürzester Zeit identifiziert und können gezielt behoben werden. Die einfach per Web-Interface zu bedienende Lösung deckt für Hersteller und Inverkehrbringer von IoT-Technologie unbekannte Sicherheitsrisiken auf. Dies gilt insbesondere für Produkte, die von einem OEM-Partner gefertigt werden. Auch Infrastrukturanbieter, Beratungsunternehmen, Wissenschaftler und Systemhäuser profitieren von dem Angebot und können Ihren Kunden wertvollen Mehrwert bieten.

Julia Alunovic