

VoIP-Sicherheitslücken in Büro-Telefonen? So erhöht man die Sicherheit gegen Spionage oder Hacker-Angriffe

Essenbach – Viele Büro-Telefone weisen schwere Sicherheitsmängel auf, wie Medien in den letzten Tagen berichteten. Diese Meldung betrifft Telefone, die – wie bei fast allen größeren Unternehmen und Organisationen – via Voice-over-IP (VoIP) funktionieren und ins Firmennetzwerk eingebunden sind. Sicherheitsforscher des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) hatten 33 verschiedene Geräte von 25 Herstellern untersucht und dabei insgesamt 40 teils gravierende Schwachstellen und Sicherheitslücken gefunden. Die Verunsicherung bei Telefon-Nutzern ist nun sehr hoch – doch mit wenigen Maßnahmen können Anwender die Sicherheit ihrer Telefonie gegen Spionage, Hacker-Angriffe oder einen Totalausfall deutlich erhöhen, wie Digitalexperten dringend raten.

Die Meldung der vergangenen Tage sorgte für Unruhe in unserer digitalen Welt: Forscher des Fraunhofer SIT fanden gravierende Sicherheitslücken in VoIP-Telefonen und stellten diese Ergebnisse bereits am 10. August 2019 auf der DEF CON in Las Vegas vor, einer der weltweit größten Hackerkonferenzen (<https://www.sit.fraunhofer.de/de/presse/details/news-article/show/verkehr-uebers-telefon/>). In ihrem Vortrag „I'm on your phone, listening – Attacking VoIP Configuration Interfaces“ erläuterten die Wissenschaftler Stephan Huber und Philipp Roskosch, die sich mit zentralen Sicherheitsherausforderungen in Wirtschaft, Verwaltung und Gesellschaft beschäftigen, wie Angreifer so Gespräche abhören, das Telefon außer Betrieb setzen oder sich über Schwachstellen im Gerät Zugriff auf weitere Teile des gesamten Firmennetzwerks verschaffen können. Inzwischen wurden die Hersteller der betroffenen VoIP-Endgeräte informiert und diese Schwachstellen geschlossen.

Darüber hinaus gibt es wichtige Maßnahmen, um die Sicherheit von Telefonen zu erhöhen. Thorsten Skotnica, Channel Manager des Digitalunternehmens TDT, erläutert: „Die Sicherheitsprobleme der vom Fraunhofer untersuchten Endgeräte basieren meist auf älteren Telefonen – mit älteren Firmware-Versionen. Den Kunden ist aus unserer Sicht, wie auch vom Fraunhofer SIT empfohlen, dringend anzuraten, VoIP-Komponenten immer mit der aktuellen Firmware des Herstellers zu betreiben, um potenzielle Angriffsvektoren zu minimieren.“

Eine aufgedeckte Schwachstellenart war so schwerwiegend, dass es den Sicherheitsforschern gelungen war, die komplette administrative Kontrolle über das VoIP-Telefon zu erlangen. Hierüber könnten Angreifer auch andere Geräte manipulieren, die sich im selben Netzwerk befinden, unter anderem weitere VoIP-Telefone, Rechner oder Produktionsmaschinen. Ein weiteres Angriffsszenario war eine Denial-of-Service-Attacke, die die VoIP-Telefone außer Gefecht setzt – und für Kundenhotlines, beispielsweise von Banken oder Versicherungen, geschäftsschädigend sein kann. Um diesen ‚worst case‘ zu verhindern, hat der Digitalexperte Michael Pickhardt (Vorstandsvorsitzender der TDT AG) einen Tipp: „Als BSI zertifiziertes Unternehmen wissen wir, wie wichtig Sicherheit auch und gerade in der Telefonie ist. Mit diesem seit Firmengründung bewährten Grundsatz für unsere Produkte haben wir im August 2019 die TK-Anlage VA1000 auf den Markt gebracht. Bei den jetzt vom Fraunhofer SIT geschilderten Fällen raten wir dazu, zusätzlich zu dem regelmäßigen Update der Firmware ein virtuelles eigenes Netz für die Telefonie anzulegen – und dieses Netz von inhouse bzw. dem Produktionsnetz mittels VLAN abzuschotten.“ Der TDT-Sicherheitsexperte Wolfgang Hofbauer führt aus: „Die Kommunikation eines unsicheren Endgeräts mit anderen Office-VLANs lässt sich durch Routing oder Firewall verhindern. Von Vorteil ist es auch, Netzkomponenten mit integriertem IDS/IPS einzusetzen und auf eventuell angreifbaren Endgeräten einen guten Sicherheitsschutz mit speziellen Sicherheitsmodulen zu verwenden.“ Patrick Kirschenhofer (Leiter Expert Support bei TDT) fasst zusammen: „So können Angriffe nahezu ausgeschlossen werden, die über das Telefon das firmenweite Netz betreffen würden.“

Pressekontakt:

Dr. Sascha Priester
Leiter der Pressestelle / Pressesprecher/ Head of Press
TDT AG
Siemensstraße 18
84051 Essenbach
Tel.: +49 8703 929 102
Mobil: +49 173 6556882
Email: spriester@tdt.de