NETSCOUT
Guardians of the Connected World | Arbor

Countdown läuft: IoT-Geräte in 5 Minuten gehackt

Nur fünf Minuten haben Anwender vernetzter Geräte Zeit, um die Werkseinstellungen zu verändern. Ansonsten droht eine Übernahme durch Hacker. Das sind Erkenntnisse von ASERT, ein Team aus Sicherheitsspezialisten des Unternehmens NETSCOUT Arbor, ein Anbieter von Business Assurance-, Cybersicherheits- und Business-Intelligence-Lösungen. Das Team hat für diese Erkenntnisse ein globales Netzwerk von Honeypots eingesetzt.

IoT-Geräte, wie beispielsweise vernetzte Kameras, Thermostate und Türöffnungssysteme stehen im Fokus von Cyberkriminellen. Mittels im Internet kursierender Listen von Standardbenutzernamen und Passwörtern sind diese schnell kompromittiert, ohne dass die Nutzer dies mitbekommen. Durch die Übernahme wird es Angreifern möglich, die Geräte in riesigen Botnetzen zu bündeln und ihre Rechenleistung für kriminelle Aktivitäten zu missbrauchen. Ebenso bedenklich sind bereits bekannte, aber nicht geschlossene Sicherheitslücken: Diese lassen sich vom Anwender nicht durch ein bloßes Ändern der Anmeldeinformationen schließen. Cyberkriminelle erhalten über derartige Schwachstellen Zugriff auf private Daten und können Mikrofone und Kameras anzapfen.

- Warum IoT-Geräte gefährlich sind: Immer noch strotzen die meisten Geräte wie Überwachungs- und Sicherheitskameras, Router, Smart-Factory-Devices, Steuerungs-, Türöffnungssysteme, Sensoren und Alarmanlagen nur so vor Sicherheitslücken, Schwachstellen und nicht veränderbaren Default-Einstellung. Erst vor Kurzem konnten Kühlsysteme des taiwanesischen Herstellers Resource Data Management über die voreingestellten Anmeldeinformationen gehackt werden.

- Erpressung leicht gemacht: Einmal gehackt, schließen Cyberkriminelle einzelne IoT-Geräte oft zu größeren und damit mächtigen Botnetzen zusammen. Vor allem Distributed-Denial-of-Service (DDoS) -Angriffe lassen sich über Botnetze schlagkräftig ausführen. Ziel der Angreifer ist es, Internet-Services, IT-Komponenten oder die IT-Infrastruktur eines attackierten Unternehmens zu verlangsamen, gänzlich lahmzulegen oder zu schädigen. So mussten Unternehmen in Deutschland 2017 insgesamt 392 sogenannter DDoS-Angriffe pro Tag oder auch 16 pro Stunde abwehren. Die Motive reichen von Erpressung und Datendiebstahl über Wettbewerbsschädigung bis hin zu staatlicher Einflussnahme.

- 2019 bleiben Mirai-Nachfolger extrem gefährlich: Das Gefahrenpotenzial von Botnetzen ist weiterhin hoch. Laut IHS Markit wird es bis 2030 mehr als 125 Milliarden IoT-Geräte geben. Vor allem Ableger des Mirai-Botnetzes richten Schaden an, denn sie ermöglichen es jeder Person mit minimalen technischen Fähigkeiten, sein eigenes IoT-Botnetz aufzubauen – und mehrere Arten von DDoS-Angriffen sowohl auf Netzwerk- als auch auf der Anwendungsschicht durchzuführen. So kann Unternehmen erheblicher finanzieller Schaden zugefügt werden.

NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) ist auf Business Assurance spezialisiert und unterstützt Unternehmen bei der unterbrechungsfreien Bereitstellung ihrer digitalen Dienste. Der Schwerpunkt der Lösungen liegt auf den Themen Verfügbarkeit, Performance und Sicherheit. Die Kombination aus patentierter intelligenter Datentechnologie und intelligenten Analysefunktionen machte das Unternehmen zum Markt- und Technologieführer. Wir bieten umfassende Transparenz in Echtzeit, detaillierte Einblicke und WLAN-Tools, die Kunden für die Beschleunigung und Sicherung ihrer digitalen Transformation benötigen. Unser Ansatz verändert die Art und Weise, wie Unternehmen und Organisationen Dienste und Anwendungen planen, bereitstellen, integrieren, testen und nutzen. Unsere Monitoringplattform nGenius ermöglicht eine kontextbezogene Echtzeitanalyse der Performance von Diensten, Netzwerken und Anwendungen. Die Sicherheitslösungen von Arbor schützen vor DDoS-Angriffen, die die Verfügbarkeit von Diensten gefährden, sowie vor komplexen Bedrohungen, die in Netzwerke eindringen, um strategische Unternehmensdaten zu entwenden. Weitere Informationen, wie Sie die Leistung von Diensten, Netzwerken und Anwendungen in physischen und virtuellen Rechenzentren bzw. in der Cloud optimieren können und wie die mit Service Intelligence (SI) ausgestatteten Performance- und Sicherheitslösungen von NETSCOUT dazu beitragen, dass Sie gelassen in die Zukunft blicken können, finden Sie auf unserer Website www.netscout.com oder auf Twitter, Facebook oder LinkedIn, wenn Sie @NETSCOUT und @ArborNetworks folgen.

Pressekontakt

Oseon

Carolin Nillert / Yannik Bartling

arbornetworks@oseon.com

+49-69-25 73 80 22 -16/15