Pressemeldung von SentinelOne vom 12.08.2020

SentinelOne identifiziert IoT-Schwachstellen, die eine ferngesteuerte Übernahme und das Eindringen in das Netzwerk ermöglichen

Barak Sternberg stellte die Forschungsergebnisse auf der DefCon vor, nachdem er mit dem Smart Device Provider HDL Automation an Schwachstellen-Patches gearbeitet hat

München – 12. August 2020 – SentinelOne <https://www.sentinelone.com>, das Unternehmen mit der führenden autonomen Cybersicherheitsplattform, gibt heute bekannt, dass Barak Sternberg, Sicherheitsforscher von SentinelLabs, vier einzigartige Schwachstellen in intelligenten Geräten von HDL Automation identifiziert hat. Die Schwachstellen setzten Tausende von HDL-Geräten der Fernsteuerung durch Angreifer aus, was zum Eindringen in das Netzwerk, zur geheimen Ausschleusung von Informationen und sogar zu Ransomware-Angriffen führen kann. SentinelOne hat HDL auf die Probleme aufmerksam gemacht, und die Schwachstellen wurden gepatcht. Die Ergebnisse wurden auf der DefCon <https://www.defcon.org/> am 8. August präsentiert.

IoT-Geräte sind Zuhause und am Arbeitsplatz allgegenwärtig und verbinden Licht, Klimaanlagen und sogar Wärmesensoren mit Heim- oder Firmennetzwerken. Diese Geräte sind auch potenzielle Sicherheitsschwachstellen, auf die Angreifer abzielen, um interne Netzwerkkonfigurationen auszunutzen, bestimmte Steuereinheiten zu manipulieren und Software- oder Hardwareschäden zu verursachen. Da Unternehmen immer mehr Geräte mit ihren Netzwerken verbinden, sind Schwachstellen wie die in der SentinelLabs-Forschung beschriebenen bedenklich, da jede Verbindung zum Unternehmensnetzwerk eine potenzielle Schwachstelle darstellt.

„Das IoT kann eine erhebliche Bedrohung für die Unternehmenssicherheit darstellen. Alles, was man an sein Netzwerk anschließt, ist ein potenzielles Einfallstor und IoT-Geräte enthalten oft unerwünschte Hintertüren, die vom Hersteller erstellt wurden. Viele Organisationen entwerfen smarte Thermostate oder Kühlschränke nicht unter dem Gesichtspunkt der Sicherheit. Doch selbst solche banalen Geräte können für Angreifer zugänglich sein, weshalb es entscheidend ist, genau zu verstehen, wie viele Geräte man an sein Netzwerk angeschlossen hat, und jeden Endpunkt abzusichern“, erklärt Sternberg.

SentinelLabs hat zwei Schwachstellen entdeckt, die eine Account-Übernahme ermöglichten: einen Fehler in der Funktion „Passwort vergessen?“ und eine Übernahme des Debug-E-Mail-Kontos. Außerdem wurden zwei weitere Schwachstellen in Bezug auf Endpunkt-APIs identifiziert. Aufgrund dieser Schwachstellen waren die SentinelLabs-Forscher in der Lage, Remote-Server zu kompromittieren, die als Proxys für die Konfiguration von smarten Geräten verwendet wurden, und arbeiteten mit HDL Automation an Patch-Lösungen. Durch die Schwachstelle wären potenzielle Angreifer in der Lage gewesen, physischen Schaden anzurichten, indem sie beispielsweise die Temperatur in einem Serverraum erhöhen, Sicherheitskameras deaktivieren oder Sensoren zur Erkennung von Leckagen oder Spannungsstößen ausschalten. Die vier neu entdeckten IoT-Schwachstellen verdeutlichen die Empfindlichkeit und die Kosten von IoT-Cyberangriffen, die sich auf unsere digitale Lebensweise auswirken.

Um mehr darüber zu erfahren, wie SentinelOne Geräte absichert und Unternehmensnetzwerke vor IoT-Gefahren schützt, besuchen Sie www.sentinelone.com.

Die SentinelOne Singularity-Plattform verfügt über umfassende IoT-Fähigkeiten durch SentinelOne Ranger, der jedes angeschlossene Gerät im Netzwerk identifiziert und verhindert, dass es ausgenutzt wird.

Über SentinelOne
SentinelOne bietet autonomen Endpunktschutz durch einen einzigen Agenten, der Angriffe über alle wichtigen Vektoren hinweg erfolgreich verhindert, erkennt und darauf reagiert. Die Singularity-Plattform wurde für eine extrem einfache Bedienung entwickelt und spart Kunden Zeit, indem sie KI zur automatischen Beseitigung von Bedrohungen in Echtzeit sowohl für standortbasierte als auch für Cloud-Umgebungen einsetzt. Sie ist die einzige Lösung, die direkt vom Endpunkt aus, eine vollständige Transparenz über Netzwerke hinweg bietet. Wenn Sie mehr erfahren möchten, besuchen Sie www.sentinelone.com/de oder folgen Sie uns bei @SentinelOneDE, auf LinkedIn oder Facebook.

Kontakt
Kafka Kommunikation GmbH & Co.
Dr. Bastian Hallbauer-Beutler
Lukas Reck
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de