Internet of Things in Unternehmen: ExtraHop deckt Bedrohungen mit neuen Reveal(x)-Funktionen auf

- Keine Silo-Lösungen für IoT-Geräte mehr nötig: Neue, auffällige und nicht verwaltete Geräte im Netzwerk werden automatisch erkannt, sodass der Überblick über alle aktiven Ressourcen beibehalten wird.
- Angriffe werden dank ML-basierten Verhaltensanalysen, Regeln und benutzerdefinierten Mechanismen umfassend entdeckt.
- Sicherheitsanalysten können dank Auswertung relevanter Kontextinformationen und Beweise Zwischenfälle effektiv und zuverlässig klären.

Seattle/Berlin, 04. März 2020 – ExtraHop, der führende Anbieter für Cloud-native Network Detection und Response, kündigt eine Reihe neuer Funktionen an, die die sichere Einführung und Implementierung von IoT in Unternehmen optimieren sollen. ExtraHop® Reveal(x)™ sorgt für die erweiterte Erkennung, Klassifizierung sowie ein Verhaltensprofiling der IoT-Geräte und schafft Transparenz von der Geräte- bis hin zur Service-Ebene. Damit erweitern sich die Funktionen von Reveal(x) auf die Ebene von Enterprise-IoT-Geräten und ermöglichen eine vollständige Visualisierung, Erkennung und Bekämpfung von Angriffen – ohne dass auf die Implementierung von Insellösungen zurückgegriffen werden muss.

„Reveal(x) ermöglicht es Organisationen, das Risikoniveau eines Gerätes wirklich zu verstehen und bietet einen situativ passenden Umgang damit an. Nicht nur können wir IoT-Geräte entdecken, indem wir ihre Marke und das Modell identifizieren, sondern sie auch automatisch nach Peer-Gruppen segmentieren, um verdächtiges Verhalten und potenzielle Bedrohungen zu erkennen", so Ronnen Brunner, Technology Evangelist EMEA bei ExtraHop.

Das Internet of Things (IoT) vereinfacht betriebliche Abläufe und soll Unternehmenseffizienz und Mitarbeiterproduktivität steigern. Dabei bindet das IoT aber auch Rechenleistung und macht Unternehmen angreifbarer: Oft herrscht wenig Transparenz darüber, welche Geräte sich mit dem Netzwerk verbinden und welche Ressourcen sie dafür blockieren.

„Unsere Forschung weist auf ein beständiges Wachstum der IoT-Nutzung in Unternehmen hin, was – zusammen mit anderen Initiativen – eine größere Angriffsfläche zur Folge hat", so Fernando Montenegro, Principal Analyst Information Security bei 451 Research. „Dies führt zu einer verstärkten Nachfrage von Sicherheitsteams im Unternehmen, nach Transparenz im Netzwerkverkehr, nach Analysen zur Erkennung von Bedrohungen und schließlich nach Abhilfe, wenn Bedarf entsteht."

Mit der neuesten Version bietet ExtraHop® Reveal(x)™ nun die Visualisierung, Erkennung und Nachverfolgung an, die Sicherheits- und IT-Organisationen benötigen, um die expandierende IoT-Entwicklung kontinuierlich zu sichern und zu verwalten:

● Die **kontinuierliche Geräte-Erkennung und -Klassifizierung** entdeckt, identifiziert und stellt eine Übersicht aller IoT-Geräte und -Dienste zusammen, um IT- und Sicherheitsteams vollständige Transparenz zu bieten.

● **Device Behavior Profiling** extrahiert umfangreiche L2-L7-Daten aus dem Netzwerk- und Cloud-Verkehr und ermöglicht so eine tiefere Analyse für alle Geräte auf der Service-Ebene. Werden diese Daten mit Cloud-skalierbarem Maschinellen Lernen von ExtraHop kombiniert und mit anderen Netzwerkereignissen verknüpft, können Bedrohungsmuster schnell und präzise erkannt werden, damit eine sofortige Reaktion erfolgen kann. Unternehmen können damit eine kontinuierliche Überwachung und Erkennung des Verhaltens von IoT-Geräten wie VoIP-Telefonen, Druckern, IP-Kameras, Wearables und Smartboards gewährleisten.

● **Guided Investigation** sammelt automatisch Kontextinformationen, also ähnliche, bereits erkannte Fälle und Details auf Paketebene in einem einzigen Arbeitsablauf, um die Abwehrmaßnahmen zu optimieren und zu beschleunigen, sodass Sicherheitsanalysten die Auswirkungen und den Umfang eines IoT-Ereignisses schnell bestimmen und Einzelheiten auf forensischer Ebene einfacher eingrenzen können.

● **Die IoT-Sicherheitshygiene** hilft Sicherheits- und IT-Betriebsteams, Probleme wie IoT-Geräte und -Dienste mit unverschlüsselter Kommunikation anzugehen. Sollten diese entdeckt werden, kann die Reaktion – wie z.B. die Erstellung eines Tickets oder die Isolierung von Geräten im Netzwerk – mit anderen Systemen automatisiert werden.

Die IoT-Sicherheitsfunktionen für Unternehmen sind jetzt weltweit auf der ExtraHop Reveal(x)-Plattform verfügbar.

Mehr Informationen unter:
www.extrahop.com/solutions/security/iot/ sowie https://www.extrahop.com/demo/

Über ExtraHop

ExtraHop liefert Cloud-native Network Detection und Response (NDR), um das hybride Unternehmen zu sichern. Der innovative Ansatz wendet fortschrittliches Maschinelles Lernen auf den gesamten Cloud- und Netzwerkverkehr an, um vollständige Transparenz, die Erkennung von Bedrohungen in Echtzeit und die intelligente Reaktion darauf zu ermöglichen. Zu den Kunden von ExtraHop gehören weltweit führende Unternehmen wie The Home Depot, Credit Suisse, Liberty Global und Caesars Entertainment, die mit diesem Ansatz Bedrohungen erkennen, die Verfügbarkeit unternehmenskritischer Anwendungen gewährleisten und ihre Investition in die Cloud sichern.

Pressekontakt:
Liubov Levkina

Agentur Frische Fische
Tel.: +49 (0)30 61675559
Mobil.: +49 (0)1739543950