ForeScout-Studie untersucht Unternehmen in Europa: 65 Prozent der Organisationen können IoT-Geräte in ihren Netzwerken nicht ausreichend erkennen und verwalten

Klassische Sicherheitslösungen sind nicht in der Lage, die wachsende Vielfalt an Geräten im Internet der Dinge (IoT) richtig abzusichern – daher müssen Unternehmen ihre Strategien für IoT-Sicherheit überdenken

San Jose, Kalif. – 17. Oktober 2016 – ForeScout Technologies, Inc., Pionier für agentenfreie Cyber-Sicherheit, veröffentlicht heute die Ergebnisse seiner neuen Studie „European Perceptions, Preparedness and Strategies for IoT Security". Die Mehrzahl der befragten Teilnehmer sieht durch IoT bessere Chancen für Unternehmen, zeitgleich gestehen aber viele Befragten ein, dass sie nicht genau wissen, wie sie dies Geräte richtig absichern können.

„Der enorme Zuwachs an IoT-Geräten schafft für Unternehmen sowohl Chancen als auch Risiken", erklärt Jan Hof, International Marketing Director, ForeScout Technologies. „Viele Organisationen erkennen im Internet der Dinge eine Möglichkeit zur Optimierung und Vereinfachung von Geschäftsprozessen, doch gehen damit auch Sicherheitsprobleme einher, die gelöst werden müssen – insbesondere dadurch, dass solche Geräte sichtbar und transparent gemacht werden, sobald sie sich mit dem Netzwerk verbinden. Denn was man nicht sieht, kann man auch nicht schützen."

Die Untersuchung wurde von ForeScout in Auftrag gegeben und von dem externen, unabhängigen Marktforschungsinstitut Quocirca durchgeführt. 201 führende IT-Entscheider in Großbritannien und den DACH-Ländern Deutschland, Österreich und Schweiz wurden gebeten, ihre Meinung zu den Sicherheitsmaßnahmen für das Internet der Dinge (IoT) in ihrem Unternehmen abzugeben.

Die wichtigsten Ergebnisse der Studie:

- **Die Angriffsfläche wird immer größer und vielgestaltiger:** Unternehmen von durchschnittlicher Größe gehen davon aus, dass sie im Lauf der nächsten 18 Monate 7.000 IoT-Geräte integrieren müssen. Und selbst kleinere Firmen rechnen mit Zahlen, die in die Hunderte oder Tausende gehen – das sind weit mehr Endpunkte, als im Bereich der herkömmlichen Benutzer-Endgeräte üblicherweise abgesichert werden müssen.
- **Der Gesundheitssektor ist auf das Internet der Dinge zu wenig vorbereitet:** Ein Drittel der Befragten gab an, dass das IoT bereits große Auswirkungen auf ihr Unternehmen hat, und ein weiteres Drittel erwartet, dass dies bald der Fall sein wird. IT und Telekommunikation sind die Sektoren, die für das IoT am besten gerüstet sind. Das Gesundheitswesen, das vom Internet der Dinge erheblich profitieren kann, hinkt vergleichsweise hinterher.
- **Unsicherheit im Hinblick auf die Identifizierung und Überwachung der Geräte:** 65 Prozent der Befragten sind sich nur „ziemlich", „wenig" oder „gar nicht" sicher, dass sie alle IoT-Geräte in ihrem Netzwerk identifizieren und überwachen können. Verstärkt wird diese Unsicherheit durch die Tatsache, dass viele IoT-Geräte Open-Source-Betriebssysteme haben, die von den Geräteherstellern angepasst werden, wodurch zahlreiche Varianten entstehen.

- **Agentenfrei ist der einzige Weg:** Die Fähigkeit, IoT-Geräte ohne Einsatz von Agenten zu erkennen und zu klassifizieren (die meist nur gängige Betriebssysteme wie Windows, Android, iOS und OS X unterstützen), wurde von 64 Prozent der Befragten als „außerordentlich wichtig“ oder „ziemlich wichtig“ eingeschätzt. Im Gesundheitssektor – wo sehr viele ungewöhnliche Geräte existieren, wie etwa CT-Scanner, Insulinpumpen und Pulsmessgeräte – waren sogar 73 Prozent dieser Ansicht.
- **Das größte Sicherheitsproblem im Zusammenhang mit dem IoT? Die Kooperation der einzelnen IT-Bereiche:** 83 Prozent der Befragten waren der Meinung, dass die größte Sicherheitsherausforderung im Zusammenhang mit dem IoT darin bestünde, eine Zusammenarbeit der verschiedenen IT-Bereiche im Unternehmen zu erreichen (Netzwerk, Sicherheit, DevOps etc.). Eine Minderheit der Umfrageteilnehmer sieht den Mangel an Personal als Problem, und mehr als die Hälfte machen sich Sorgen um die Budgets und die Verfügbarkeit geeigneter Produkte.

Dazu Bob Tarzey, Analyst und Direktor des Marktforschungsinstituts Quocirca, das die Umfrage durchführte: „Die IoT-Implementierungen in europäischen Unternehmen umfassen bereits Millionen von Geräten. Viele davon haben nur eine begrenzte Rechenleistung und dürfen nur wenig Strom verbrauchen. Andere haben ungewöhnliche Betriebssysteme, und in bestimmten Fällen werden die betreffenden ‚Dinge’ dem IT-Sicherheitsteam nicht bekannt sein, wenn sie sich erstmals mit dem Netzwerk zu verbinden versuchen. All dies erfordert Lösungen, die den Sicherheitsstatus aller mit dem Netzwerk verbundenen Geräte erkennen, ohne dass Agenten installiert werden müssen.“

Untersuchungsmethodik
ForeScout beauftragte Quocirca, im Zeitraum von August bis September 2016 die Studie „European Perceptions, Preparedness and Strategies for IoT Security“ durchzuführen. Dazu wurden 201 führende IT-Entscheider in Großbritannien und den DACH-Ländern Deutschland, Österreich und Schweiz befragt. Die Studie analysierte und bewertete die Ansichten der Teilnehmer zu den IoT-Geräten und den zugehörigen Sicherheitsrichtlinien, -maßnahmen und -werkzeugen in ihren Unternehmen. Dabei wurden verschiedene Sektoren sowie Unternehmen jeder Größe einbezogen – von Firmen mit nur 10 Mitarbeitern bis hin zu Großunternehmen mit mehr als 10.000 Beschäftigten. Die Untersuchung schloss sich an eine Umfrage an, die Webtorials zwischen März und April 2016 in den USA durchgeführt hatte.

Über ForeScout Technologies, Inc.
ForeScout Technologies, Inc. verändert Sicherheit durch Sichtbarkeit. ForeScout bietet Global 2000 Unternehmen und Regierungsorganisationen eine einzigartige Möglichkeit in Geräte Einblick zu erhalten, darunter nicht traditionelle Geräte, bei der Verbindungsaufnahme mit dem Netzwerk. Genauso wichtig ist, dass ForeScout Sie diese Geräte verwalten lässt und das Teilen und Organisieren von Informationen über verschiedenste Sicherheitslösungen hinweg orchestriert, um das Incident Response Management zu beschleunigen. Entgegen traditionellen Sicherheitsalternativen erreicht ForeScout dies, ohne den Einsatz von Software Agenten oder aber vorherige Kenntnisse über das Gerät. Die Lösung des Unternehmens integriert sich mit marktführenden Netzwerk-, Sicherheits-, Mobilitäts- und IT-Management-Produkten, um Sicherheits-Silos zu umgehen, Workflows zu automatisieren und signifikante Kosteneinsparungen zu ermöglichen. Bis

Januar 2016 haben mehr als 2.000 Kunden in mehr als 60 Ländern ihre Netzwerksicherheit und Compliance mit ForeScout Lösungen verbessert. Lernen Sie mehr auf www.forescout.de

Pressekontakt:
Ferdinand Kunz
Kafka Kommunikation
089 74 74 70 580
fkunz@kafka-kommunikation.de