IoT fordert die Cyber Security heraus

IoT ist omnipräsent und bietet immenses Potenzial – birgt aber auch Risiken. Schwachstellen in Geräten sind allgegenwärtig und die Anzahl der Cyberangriffe steigt kontinuierlich. Trotzdem zählt IoT immer noch zu den meistunterschätzten Bedrohungen. Bewährte Ansätze helfen, Cyber Security zu etablieren und so die Risiken zu minimieren.

Das Potenzial des Internets der Dinge («Internet of Things», IoT) ist immens und hält überall Einzug. So ist es nicht verwunderlich, dass laut Experten in wenigen Jahren acht von zehn Schweizer Unternehmen IoT-Komponenten im Einsatz haben werden. Dadurch steigt aber auch die Gefahr, dass solche Systeme manipuliert werden. Diebstahl, Betrug, Erpressung und Manipulation sind mögliche Folgen.

Smart – aber nicht ohne Risiken

Die Anzahl der Geräte, die mit Unternehmensnetzwerken verbunden sind, wird weiter ansteigen. IoT birgt aber auch ein (oft vernachlässigtes) Risiko: Cyberkriminalität. Obwohl dies keine neue Tatsache ist, fliessen immer noch grundlegende Sicherheitsprinzipien oftmals nicht in IoT-Projekte ein. Das kann erhebliche Schäden verursachen, beispielsweise durch Abfluss von Kunden- und Produktionsdaten oder wenn ein Wartungszugang zur Hintertüre eines Angreifers wird. Cyber Security gehört deshalb von Beginn an oben auf die Agenda – nicht erst, wenn etwas schiefgelaufen ist.

Schlüsselfaktoren bei IoT-Netzwerken

Ein systematischer Sicherheitsansatz ist das A und O erfolgreicher Cyber Security. Dabei müssen sowohl das Risikomanagement, der Schutz der Informationen, die Erkennung und Reaktion auf Sicherheitsvorkommnisse als auch die Wiederherstellung und Optimierung berücksichtigt werden.

Technologisch liegt der Schlüssel zur Sicherheit unter anderem in einer geeigneten Architektur und der entsprechenden Zonierung von IoT-Netzen. Wichtige Aspekte sind dabei die Identität, die Authentisierung und der Schutz der Daten, ebenso wie die optimale Segmentierung im Backend und die Überwachung der dadurch geschaffenen Zonenübergänge. Es gilt, verschiedene Verteidigungslinien aufzubauen und diese mit angemessenen Sicherheitsmassnahmen zu versehen. Best-Practice-Ansätze und bewährte Frameworks, wie beispielsweise die ISO 270xx-Familie oder das NIST Cyber Security Framework, dienen zur Orientierung.

Unternehmen sind gegenüber globalen Risiken im Zusammenhang mit bekannten und neuen «Zero-Day»-Bedrohungen und anderen Schwachstellen exponiert. Diese werden aktiv und systematisch ausgenutzt. Unabhängig ob IoT oder klassische IT-Komponenten, jedes Gerät kann Schwachstellen enthalten und so zum Angriffspunkt werden. Daher sollten Geräte im Design-, Entwicklungs- und Betriebsprozess (DevOps) regelmässig auf Schwachstellen geprüft werden. Wichtig ist dabei natürlich, dass sie Updates unterstützen – was leider sehr oft nicht der Fall ist. Unzureichendes Patch-Management und mangelhafte Prüfung auf Schwachstellen sind nicht nur ein Problem von IoT. So bleiben immer wieder bekannte Schwachstellen ungepatched, obwohl passende Updates verfügbar wären. Cyberkriminellen fällt es dann relativ leicht, das schwächste Glied in der Kette zu finden und auszunutzen. Deshalb darf das regelmässige Update- und Patch-Management nicht vergessen werden – natürlich auch bei IoT-Geräten. Falls sich exponierte Geräte mit bekannten Schwachstellen in der Infrastruktur befinden, die nicht aktualisiert werden können, sollten diese segmentiert und von der Produktionsumgebung abgetrennt werden.

Risiken erkennen, bevor das Licht ausgeht

Da sich die Risikosituation stetig ändert, muss die aktuelle Bedrohungslage immer beobachtet und das Sicherheitsdispositiv entsprechend angepasst werden. Risk Assessments, organisatorische Audits und Penetrationtests sind wichtige Elemente in der Cyber Security. Unternehmen sollten gleichzeitig in der Lage sein, Sicherheitsvorfälle zu erkennen, schnell darauf zu reagieren und die Auswirkungen auf ein Minimum zu reduzieren. Somit gilt: Wer sich mit IoT beschäftigt, muss sich auch intensiv mit Cyber Security auseinandersetzen.

InfoGuard
SWISS CYBER SECURITY

InfoGuard AG
Lindenstrasse 10, CH-6340 Baar
✆ +41 (0)41 749 19 00
info@infoguard.ch, www.infoguard.ch