Use Case Logistik

TREND MICRO™ | Global Leader in Cybersecurity

Mehr Effizienz ohne Sicherheitsverlust

IoT-Cloud-Konvergenz

INTEROPERABILITÄT IN DER IOT-CLOUD

Der Nutzen des Industrial Internet of Things (IIoT) entfaltet sich längst nicht nur auf die Fabrikhalle. Auch in der Logistik ermöglicht es immer häufiger automatisierte Lösungen. Es identifiziert Beförderungsgut von Anfang bis Ende des Prozesses, steuert und kontrolliert die Lieferkette, überwacht Kühlketten etc.

Doch je umfangreicher die Implementierungen werden, desto deutlicher zeigt sich: Ohne Interoperabilität sowie Anbindung an externe Verarbeitungs- und Speicherkapazität lassen sich derart komplexe Aufgaben nicht mehr erledigen. Dazu bedarf es einer „IoT-Cloud". Sie hilft den Administratoren, aus der Ferne Daten zu sammeln, Remote-Wartung zu betreiben und das System zu konfigurieren, ohne es physisch anzufassen. In der Wolke stehen Speicherplatz und Verarbeitungsfunktionen nahezu unbegrenzt zur Verfügung.

Bis zu einem gewissen Grad steigert die Cloud auch das Sicherheits-Level, indem sie beispielsweise die Größe der Angriffsfläche auf wenige Interfaces begrenzt. Gleichzeitig ist aber auch das Gegenteil der Fall: Durch das Zusammenspiel von IoT und Cloud treten die Sicherheitsprobleme nur noch deutlicher zu Tage. Was aber ist die Alternative? Gefragt ist vor allem ein ausgeklügeltes Sicherheitssystem.

WAS KANN PASSIEREN?

Zwischen der unternehmenskritischen Infrastruktur und der Cloud gibt es meist nur wenige und relativ enge Ein- beziehungsweise Ausgangstore. Und die, so sollte man meinen, lassen sich gut durch eine Firewall schützen. Wirklich? Der vermeintliche Vorteil kann sich leicht ins Gegenteil verkehren, falls es den Angreifern gelingt, genau hier einen „Tunnel" zu graben, denn in diesem Fall liegt das ganze System offen vor ihnen.

Sind Kommunikation und Datenfluss zwischen Edge und Cloud nicht sorgfältig – durch strikte Authentifizierung und Verschlüsselung – geschützt, werden Zugriffskontrolle und Datenintegrität wertlos. Das ist besonders gefährlich, wenn IoT-Geräte und Sensoren personenbezogene Daten oder andere sensible Informationen sammeln, die auf diese Weise in die Public Cloud geraten können. Die Frage, wo die Daten gespeichert werden, ist entscheidend. Klären Sie diesen Punkt mit Ihrem Cloud Provider, bevor Sie den Vertrag unterschreiben! Sonst riskieren Sie Schadensersatzforderungen und Imageverlust.

WIE LÄSST SICH GEGENSTEUERN?

Voraussetzung für die Sicherheit der IoT-Cloud ist, dass beide Teile des Systems, Internet of Things sowie Cloud, sauber implementiert und konfiguriert sind. Dazu gehören physisch abgesicherte Devices und eindeutig segmentierte Netze. Voreingestellte Passwörter sind sofort zu individualisieren und regelmäßig zu ändern. Selbstverständlich dürfen die Passwörter nirgendwo in Textform gespeichert sein. Und die Gültigkeit der Zugriffstokens auf die Cloud sollte zeitlich begrenzt sein. Alle Komponenten – vom Betriebssystem, über Libraries und Frameworks bis zu den Anwendungen – müssen regelmäßig aktualisiert und gepatcht werden. Ist dann noch die Cloud sicher konfiguriert, so ist das weit mehr als nur die halbe Miete.

ACHT REGELN FÜR DEN EINSATZ VON IOT-APPS

- Laden Sie die Apps ausschließlich von legitimen Plattformen.
- Beschränken Sie die Zugriffe, und prüfen Sie die Berechtigungen regelmäßig.
- Seien Sie kritisch hinsichtlich der eingesetzten Devices, denn nicht alle Anbieter haben denselben Sicherheitsstandard.
- Lassen Sie kein Update von Anwendungen und Geräten aus.
- Erstellen Sie einen Verbindungsplan aller Devices im Netz und beobachten Sie den Netz-Traffic.
- Sichern Sie die Kommunikationsprotokolle und -kanäle durch Kryptographie.
- Sorgen Sie für den regelmäßigen Austausch der Credentials.
- Etablieren Sie eine Multi-Faktor-Authentifikation (MFA). wSo ziehen Sie eine weitere Sicherheitsdecke ein.

WAS IOT-CLOUD-KONVERGENZ SICHERER MACHT

Erlauben Sie keine halben Sachen: Es nutzt wenig, wenn bestimmte Teile des Ökosystems super sicher sind, andere aber vernachlässigt werden. Wer Schwachstellen sucht, wird sie genau dort finden. Sicher kann nur ein System sein, das Sie überall gleichermaßen unter Kontrolle haben – angefangen von der Cloud bis zu den Endpunkten am Edge:

- Je früher im Prozess Sie den Datenfluss zwischen der Edge und der Cloud absichern, desto größer ist die Wahrscheinlichkeit, dass Sie Anomalien entdecken, bevor diese das System infizieren. Implementieren Sie Monitoring- und Filter-Software also möglichst nah an der Datenquelle.
- Cloud-basierte Lösungen haben hierbei Vorteile, allen voran die größere Verarbeitungskapazität.
- Empfehlenswert ist eine „Fog-Computing"-Infrastruktur, in der Daten, Verarbeitung, Speicherung und Anwendungen dezentral, sprich: irgendwo zwischen der Edge und der Cloud, angesiedelt sind.
- Der verwendete Code und die genutzten Anwendungen sollten regelmäßig überprüft werden; als Best Practice gelten statische und dynamische Applikationsanalysen.
- Hinsichtlich der Zugriffskontrolle empfiehlt sich das „Prinzip des geringstmöglichen Privilegs" (Principle of Least Privilege): Niemand sollte mehr Rechte bekommen, als sie oder er für die jeweilige Aufgabe benötigt.

DER PARTNER AN IHRER SEITE

Mit Cloud Security Lösungen von Trend Micro erhalten Sie Best of Breed-Lösungen vereint aus einer Hand von einem Marktführer. Trend Micro hat laut IDC mit 29,5 Prozent den mit Abstand größten Marktanteil im Bereich Hybrid Cloud Workload Security und wurde im Forrester Wave™: Cloud Workload Security als Leader genannt.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss."

Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.