arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Die IoT-Datenherausforderung: Gewährleistung der Sicherheit im Zeitalter der Zettabytes

Von Florian Malecki, Executive Vice President Marketing bei Arcserve

Der Einsatz von IoT-Geräten, sowohl im privaten als auch im industriellen Bereich, hat in den letzten Jahren erheblich zugenommen. Die Folge: Die Datenmenge wächst überproportional. Von vernetzten Autos über Fitness-Tracker bis hin zu intelligenten Häusern und Fabriken – unser Alltag und unsere Arbeitsplätze sind vom Internet der Dinge umgeben. Weltweit sind Milliarden von IoT-Geräten im Einsatz, und sie erzeugen Datenmengen im Zettabyte-Bereich (eine Eins gefolgt von 21 Nullen). Diese Daten haben gleichzeitig auch die Angriffsfläche für Cyberattacken erheblich vergrößert und machen es für Unternehmen schwieriger, sich zu schützen. Das IoT bietet Hackern eine riesige Chance, indem es eine ungeheure Menge an Daten inklusive vieler neuer Hintertüren liefert, die möglicherweise nicht ausreichend gesichert oder noch nicht einmal bekannt sind.

Unternehmen müssen das weltweit rasant wachsende Informationsuniversum schnell in den Griff bekommen, denn die Daten können nicht einfach gelöscht oder archiviert werden. Neben dem sicheren Sammeln und Verwalten werden Daten, inklusive der IoT-Daten, beispielsweise in KI-Algorithmen benötigt, um Geschäftsentscheidungen basierend auf fundierten Informationen treffen zu können.
Und damit endet die Komplexität noch lange nicht. Denn je mehr Daten vorhanden sind, desto wichtiger werden sie. IoT-Geräte steuern heute Unternehmen, kontrollieren Gesundheitssysteme und sind bereits in vielen Haushalten anzutreffen. Folglich kann jeder Funktions- oder Datenverlust

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

erhebliche Auswirkungen auf das Geschäft eines Unternehmens oder sogar auf das Leben von Menschen haben.
Darum ist es besonders wichtig, dass Unternehmen ihre IoT-Daten sichern, um diese im Falle eines Angriffs oder eines Ausfalls so schnell und effizient wie möglich wiederherzustellen. Andernfalls besteht die Gefahr, dass sie ihr Geschäft aufgeben müssen.

Im Folgenden werden drei Aspekte beschrieben, wie Unternehmen ihre IoT-Daten erfolgreich schützen und einen Verlust verhindern können.

1. IoT-Geräte kennen

Das Hauptproblem bei IoT-Geräten liegt darin, dass sie von Natur aus oft nicht sicher sind. Die meisten werden mit Blick auf Benutzerfreundlichkeit, einen niedrigen Preis und gute Konnektivität entwickelt. Ihnen fehlen integrierte Sicherheitsfunktionen und in vielen Fällen auch die Möglichkeit für Updates und Patches. Damit sind diese Geräte ein attraktives Ziel für Hacker.

Der erste Schritt zu mehr Sicherheit besteht darin, die genaue Anzahl der IoT-Geräte im Unternehmensnetzwerk zu bestimmen und ein detailliertes Inventar zu erstellen. Sobald Unternehmen einen Überblick über alle IoT-Endpunkte haben, ist es wichtig, die Sicherheit mit guten Passwörtern zu verbessern, da viele Geräte mit schwachen voreingestellten Standardpasswörtern ausgeliefert werden. Administratoren sollten das vorinstallierte Passwort durch ein komplexeres und sichereres Passwort ersetzen, sobald ein IoT-Gerät mit dem Netzwerk verbunden wird.
Außerdem sollte eine Patch-Verwaltung zum Einsatz kommen. Anders als die meisten IT-Systeme erhalten IoT-Geräte keine regelmäßigen Software-Updates, um Sicherheitslücken zu schließen. Das bedeutet, dass es an den

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Unternehmen liegt, ein geregeltes Patch- und Upgrade-Management sicherzustellen, um Angriffen und Datenverlusten vorzubeugen.

2. Doppeltes Engagement beim Datenschutz

Ein weiteres wichtiges Mittel zur Sicherung von IoT-Daten ist die 3-2-1-1-Datenschutzstrategie. Diese Strategie sieht vor, dass drei Sicherungskopien der Daten auf zwei verschiedenen Medien (z. B. Festplatte und Band) erstellt werden, wobei sich eine dieser Kopien zur gesicherten Wiederherstellung an einem anderen Ort befindet. Das letzte Element in dieser Gleichung ist die unveränderliche Objektspeicherung.

Unveränderliche Objektspeicher sichern IoT-Daten kontinuierlich, indem sie beispielsweise alle 90 Sekunden Snapshots der Daten erstellen. Diese ermöglichen eine zeitgenaue Datenwiederherstellung. Im Falle eines Ausfalls, einer Naturkatastrophe oder eines Ransomware-Angriffs sorgen sie dafür, zu einem aktuellen Dateistatus zurückzukehren. Ein weiterer Vorteil von Snapshots ist, dass sie „immutable" sind, also nicht geändert, überschrieben oder gelöscht werden können. Sie schützen somit die Datenintegrität vor Verlusten durch menschliches Versagen, Hardwareausfälle und vor allem durch Ransomware-Angriffe.

Mit unveränderlichen Snapshots können Unternehmen auch unter Einsatz von potenziell unsicheren IoT-Geräten Ausfallzeiten vermeiden und die reibungslose und unterbrechungsfreie Bereitstellung von Diensten und Abläufen sicherstellen.

3. Den richtigen Partner wählen

Die Möglichkeiten und die Vielfalt an IoT-Geräten verändern sich schnell und jeden Tag kommen viele neue Geräte auf den Markt. Deshalb ist für

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Unternehmen die Wahl der Partner und Technologien entscheidend. Sowohl der Anbieter von IT-Lösungen als auch die präferierten Partner und Managed Service Provider müssen im Bereich der Datenspeicherung und -wiederherstellung sehr erfahren und auch flexibel sein, um mit den schnellen Veränderungen Schritt zu halten und die Daten zu schützen. Dies gilt für jede Unternehmensgröße, da IoT-Systeme riesige Datenmengen produzieren. Die Verwaltung dieser Daten und ihre Wiederherstellung sind von entscheidender Bedeutung, um eine Business Continuity zu gewährleisten.

Als das Internet aufkam, stellten Unternehmen zunächst fest, dass es eine Menge Daten produziert. Dann lernten sie, wie wertvoll diese Daten sind und dass es wichtig ist, diese Daten zu schützen. Das Internet der Dinge folgt einer ähnlichen Entwicklung und Unternehmen beginnen jetzt zu verstehen, wie wichtig es ist, die von den IoT-Geräten im Netzwerk erzeugten Daten zu schützen.

Folgen Sie Arcserve auf LinkedIn oder Twitter und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de
www.tc-communications.de