arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Sicherheit bei Cyberattacken in der Fertigungsindustrie schließt auch die Backups ein

Von Sven Richter, Marketing Manager DACH bei Arcserve

Im aktuellen Ransomware-Report 2024: Fertigung und Produktion stellt der IT-Security-Anbieter Sophos fest, dass mit 65 Prozent mehr als die Hälfte der Fertigungsunternehmen im vergangenen Jahr von Ransomware betroffen waren. Noch schwerwiegender ist, dass die Verschlüsselungsrate mit 74 Prozent den höchsten Stand seit fünf Jahren erreicht hat. Bei dieser Risikolage reicht es nicht aus, einen guten Cyberschutz zu etablieren, sondern auch für die Sicherheit der Backups zu sorgen, die im Ernstfall die letzte Verteidigungslinie darstellen.

Risiko IoT im Fertigungssektor

Die wachsende Präsenz von Internet-of-Things-Geräten (IoT) im gesamten Fertigungssektor hat eine neue Front im Kampf gegen Ransomware eröffnet. Laut Statista gab es im Jahr 2022 weltweit 112 Millionen IoT-Cyberattacken, und mit den Fortschritten in der KI, von der auch die Kriminellen profitieren, wird es in Zukunft zweifellos noch mehr geben. Die zunehmende Abhängigkeit von teils unsicheren IoT-Geräten zur Überwachung und Steuerung industrieller Abläufe, hat die Angriffsflächen für Fertigungsunternehmen drastisch erweitert.

Zu den häufigsten Bedrohungen gehören Angriffe auf IoT-Geräte aufgrund schwacher Standardkennwörter, ungepatchter Firmware-Schwachstellen und ungesicherten Netzwerkverbindungen. Angreifer setzen häufig gängige Malware-Programme wie Mirai oder Bashlite ein. Diese erstellen Botnets und übernehmen die Kontrolle über infizierte Geräte, um bösartige Aktivitäten zu

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

starten. Ransomware ist mutmaßlich die größte Bedrohung, die Produktionsbetriebe zum Stillstand bringen kann, indem sie den Zugriff auf wichtige Daten blockiert. Die Ausfallzeit und die Kosten können verheerend sein. Nur eine schnelle Wiederherstellung der Daten und Systeme aus speziell geschützen Backups kann den wirtschaftlichen Schaden maßgeblich mindern und vor allem die Erpressungsversuche der Cyberkriminellen ins Leere laufen lassen.

IoT-Geräte gegen Cyberattacken verteidigen

Es gibt einige wichtige Maßnahmen zur Cyber- und Datensicherheit, die IT-Experten in der Fertigungsindustrie in Verbindung mit IoT-Geräten ergreifen können. Die sieben wichtigsten Tipps von Arcserve sind:

- **Risikobewertung:** IT-Administratoren sollten eine gründliche Risikobewertung durchführen, um festzustellen, welche Systeme und Daten für ihr Unternehmen entscheidend sind und Ziel von Cyberangriffen sein könnten.
- **Anmeldeinformationen ändern:** Die Standard-Anmeldeinformationen – Benutzernamen und Passwörter – von vernetzten IoT-Komponenten sollten durch starke, eindeutige Passwörter ausgetauscht werden.
- **Firmware aktualisieren:** IT-Administratoren sollten regelmäßig ein Update der Firmware, Anwendungen und Patches auf IoT-Geräte durchführen, sobald diese verfügbar sind. So lassen sich bekannte Schwachstellen beheben.
- **Netzwerksegmentierung:** Um die Ausweitung der Angriffe im Unternehmen einzuschränken empfiehlt es sich, das Firmennetzwerk zu segmentieren. Dabei werden die Anwender, die den Produktionsbetrieb und die unterstützenden IoT-Geräte verwalten von anderen Unternehmensbereichen getrennt.

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Geschütztes Backup und Disaster Recovery: ein Muss in der Fertigung

Unabhängig davon, ob Malware über IoT-Geräte oder durch einen erfolgreichen Phishing-Angriff eindringt, die Sicherung der Daten und die Bereitstellung einer effektiven Notfallwiederherstellungslösung ist unerlässlich. Wirkungsvolle Backup- und Recovery-Lösungen stellen sicher, dass alle Daten und Systeme auf unveränderlichen oder Air-Gap-fähigen Speichern vor Cyberattacken geschützt werden – vor Ort oder in der Cloud. Darüber hinaus können Unternehmen ihre RTOs, RPOs und SLAs mit integrierten Assured Recovery-Tests validieren, so dass sie sich auf die Geschäftskontinuität verlassen können.

Die Cyber-Bedrohungslage ist hoch. Fortschrittliche und umfassende Backup- und Notfallwiederherstellungslösung sind der beste Schutz für die IT-Infrastruktur produzierender Unternehmen. Mit dem Einsatz dieser Lösungen, können sich die Unternehmen darauf verlassen, dass ihre Daten schnell wiederhergestellt werden können und der Betrieb so schadlos wie möglich nach der Cyberattacke wieder aufgenommen werden kann.

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

###

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Über Arcserve

Arcserve ist der Pionier für einheitliche Daten-Resilienz-Lösungen. Seit mehr als 40 Jahren vertrauen fast 150.000 Kunden und über 30.000 Vertriebspartner in 150 Ländern auf Arcserve, um ihre Datenresilienz zu stärken, verlorene Daten wiederherzustellen und die Kontinuität ihres Geschäftsbetriebs zu gewährleisten. Mit einem einheitlichen Ansatz für Datensicherung und -wiederherstellung, erstklassigem technischen Support und dem niedrigen Total Cost of Ownership (TCO) hilft Arcserve Unternehmen, ihre Daten zu verwalten, zu schützen und - was am wichtigsten ist - in jeder Situation wiederherzustellen.
Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter oder LinkedIn.

Unternehmenskontakt
Alex Plotnikov
Arcserve
alex.plotnikov@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 157 524 437 49
Thilo Christ
+49 171 622 06 10
arcserve@tc-communications.de