Cybersicherheit in der digitalen Fabrik: der optimale Weg zur intelligenten Fertigung

Fernwartung ist ein Resultat der zunehmenden Digitalisierung der Industrie und bietet erhebliche Kosten- und Wettbewerbsvorteile. Lösungen mit optimaler Cybersicherheit schöpfen das volle Potential der Fernwartung und werden nicht zum großen Risiko für die gesamte Produktion.

Die Öffnung von Fernwartungssystemen für Dritte erfordert Cybersicherheitslösungen, die sowohl die Anforderungen der Betriebstechnik (OT; Operational Technology) als auch der IT erfüllen. Ungeplante Ausfallzeiten, verbunden mit wirtschaftlichen Einbußen und daraus resultierende Imageschäden, sollen dadurch vermieden werden.

Kosten senken und Effizienz steigern

Im Bereich industrieller Automatisierung haben sich Fernwartungslösungen in den letzten zehn Jahren durch Einsparungen bei den Reisekosten und einen schnelleren, optimierten Support durch Servicetechniker der Maschinenbauer bewährt. Die Nutzung dieser Fernwartungs-/ Remote-Dienste erhöht die Produktivität sowie Wettbewerbsfähigkeit deutlich und ist zu einem Haupttreiber für Industrie 4.0-Initiativen vieler Unternehmen geworden.

Datensicherheit

Fernwartung setzt Internetnutzung voraus, und der Begriff Internet der Dinge (IoT) ist entscheidend für die Planung und Umsetzung von Strategien für industrielle Steuerungssysteme geworden (ICS; Industrial Control Systems). Heute ist dies nicht nur auf OT-Abteilungen beschränkt, sondern betrifft aufgrund der Auswirkungen auf die Cybersicherheit auch IT-Abteilungen. Die OT-Abteilung hat heute eine viel umfassendere Verantwortung für die Datensicherheit (Security), wobei in der Vergangenheit das dominierende Thema die Betriebssicherheit (Safety) war. Im Bereich der Datensicherheit hat sich der Schwerpunkt von der primären Authentifizierung auf die Bereitstellung robuster Systeme für das Berechtigungsmanagement verlagert.

Um die Vorteile des industriellen IoT (IIoT) umfassend zu nutzen, kommt es auf die Zusammenarbeit zwischen Experten in jedem Bereich an. Führende Anbieter arbeiten eng mit Partnern zusammen, die über fundierte Kenntnisse auf dem jeweiligen Gebiet verfügen, um gemeinsam optimierte Lösungen zu entwickeln, die den sich ständig ändernden Kundenanforderungen gerecht werden.

Zuverlässigkeit

Wenn es um den sicheren Fernzugriff geht, erwarten Kunden den Einsatz modernster Technik und hohe Zuverlässigkeit – nicht nur aus Hardware-Sicht, sondern auch bei der Transformation hin zur digitalen Fabrik. Die Fernwartung ist einer von vielen Bereichen, in denen die Zusammenarbeit mit innovativen Partnern einen erheblichen Mehrwert für die Kunden darstellt.

Benutzerfreundlichkeit

Ein Beispiel ist Secomea. Das IIoT-Unternehmen hat in den letzten zehn Jahren eine Reihe von Fernwartungslösungen und Zugriffsverwaltungssystemen für Dritte entwickelt und verfeinert, die Datensicherheit und Benutzerfreundlichkeit optimal miteinander verbinden. Secomeas langjährige Erfahrung zeigt, dass benutzerfreundliche Lösungen deutlich weniger anfällig für menschliche Fehler sind und folglich ein höheres Sicherheitslevel ermöglichen.

Authentifizierung

Worauf sollte ein Unternehmen, das eine Fernverwaltung oder ein Zugriffsmanagementsystem für Dritte in Betracht zieht also achten, um das erforderliche Maß an Cybersicherheit zu gewährleisten?

Erstens sollten die Remote-Verbindungen von Clients und IoT-Geräten auf einem soliden, sicheren Authentifizierungsdesign basieren, das in der Lage sein muss, Man-in-the-Middle-Angriffe zu verhindern. Zweitens sollte jede in Betracht gezogene Lösung hinsichtlich der Datensicherheit als auch für Industrie 4.0 zertifiziert sein und regelmäßig von externen Sicherheitsexperten überprüft werden.

Die Lösung sollte außerdem über eine Zwei-Faktor-Authentifizierung und über ein Verwaltungssystem für den Benutzerzugriff verfügen, mit dem der Eigentümer zentral steuern und autorisieren kann, wer wann und wie lange Zugriff auf welche Geräte/ Systeme hat, während alle Aktivitäten für die Zugriffsüberwachung gleichzeitig protokolliert werden.

Industrie gerechtes VPN

Bei herkömmlichen VPN-Tunnellösungen, die auf OpenVPN oder IPSec basieren, ist Vorsicht geboten. Diese VPN-Techniken bieten einen vollständigen Netzwerkzugriff zwischen zwei Remote-Netzwerken. Dies entspricht jedoch nicht den IT-Sicherheitsanforderungen moderner Fabriken. Heute sind Lösungen wie das Secomea Relay VPN verfügbar, die den Anforderungen an die Sicherheit und Benutzerfreundlichkeit bei der Anbindung von Servicetechnikern an Industrieanlagen gerecht werden. Diese Art von Lösung bietet auch die Möglichkeit, nur auf bestimmte IP-Adressen und Dienste zuzugreifen, ohne dass Firewall-Regeln konfiguriert werden müssen, und kann entweder mit einem Cloud-basierten oder einem privaten M2M-Server verwendet werden.

Fazit

Cybersicherheit ist ein entscheidender Faktor in der digitalen Fabrik, und jeder Beteiligte muss sich dessen bewusst sein und sicherstellen, dass sie ordnungsgemäß umgesetzt wird. Jede Nachlässigkeit in diesem Bereich kann zu einem Fehlerpunkt in der gesamten Struktur führen – etwas, das sich keine Fabrik leisten kann. Die Implementierung einer benutzerfreundlichen Lösung minimiert die menschlicher Fehler, besonders von Nicht-IT-Spezialisten, und senkt die Cybersicherheitsrisiken, um eine reibungslose Fertigung zu ermöglichen. ◄

Autoren:
Emilie Lerche Fenger, Secomea und Marco Zampolli

Advantech
www.advantech.com