Sicherer Service im Maschinenpark

Zentrale Lösung für die Fernwartung

Über Fernwartungszugänge vermeiden Hersteller von Maschinen und Anlagen so manchen Stillstand beim Produzenten vor Ort oder verkürzen ihn zumindest deutlich. Für die Betreiber ist das natürlich günstig. Weniger günstig ist es für sie, wenn bei heterogenen Maschinenparks immer mehr verschiedene Fernwartungszugänge verwaltet und abgesichert werden müssen. Die IT-Securitylösung Secure Factory RAS von Zedas hilft dabei.

Bild: ©Kobes/Fotolia.com

Kaum ein Unternehmen verzichtet heute auf den Service für seine produzierenden Anlagen. Stillstand und Ausfall erzeugen rasch hohe Kosten. Hersteller, Lieferanten und Dienstleister bieten deswegen Remote Services an, um schnellen und kostengünstigen Support für ihre Anlagen bereitzustellen. Wenn ein Unternehmen viele verschiedene Maschinen und Anlagen betreibt, die jeweils eigene Dienste für den Fernzugriff mitbringen, können klare Vorgaben oder eine zentrale Lösung dabei helfen, den Überblick über die Anlage zu behalten. Denn die zunehmende Vernetzung der Anlagen untereinander öffnet Tür und Tor für den möglichen Querzugriff zwischen den Anlagen und ihren Steuerungen. Über Firewalls abgeschottete Sicherheitszonen sollen das unterbinden. Hier ist die Herausforderung, alle Firewall-Regeln korrekt und aktuell zu halten. In der Praxis geht Funktion oft vor Sicherheit. Nicht wenige Firewalls verbrauchen lediglich Strom, weil ihre Regelwerke deaktiviert wurden. Selbst wenn sie funktionieren: Ist mit Firewall und Virtual Private Network für externe Servicedienstleister schon das gewünschte Maß an IT-Sicherheit erreicht?

Externe Kräfte im Blick behalten

Digitalisierung, Vernetzung und der Einsatz verschiedener Systemlieferanten innerhalb der Ausrüstung von Produktionsumgebungen stellen Betreiber zudem vor die Herausforderung, die Servicearbeiten von externen Kräften zu regulieren, zu kontrollieren und nachzuweisen. Um Unternehmen dabei zu helfen, die Verwaltung von Fernzugriffen und externen Servicekräften zu lenken, hat die Zedas GmbH eine Remote Service-Lösung entwickelt. Secure Factory RAS soll Schutz auf mehreren Ebenen bieten. Neben den üblichen Maßnahmen zur Absicherung von Netzwerkzugängen mittels Authentifizierung mit PIN und Einmal-Passwort und für die Netzwerksicherheit (Zertifikate, Verschlüsselung, Firewall, Sicherheitszonen) werden auch die Fernwartungsinstrumente abgesichert. Das betrifft neben den Fernwartungsrechnern auch die verwendeten Softwareanwendungen. Zudem lässt sich die Organisation der Zugriffssteuerung und -protokollierung schützen.

Telefonische Anmeldung erforderlich

Die Lösung stellt für jeden externen Service-Dienstleister in einer dedizierten Sicherheitszone einen virtuellen Fernwartungsrechner bereit. Dieser ist im Grundzustand ausgeschaltet. Selbst mit erfolgreichem Netzzugang nach Authentifizierung sind die in den Firewall-Regeln freigeschalteten Zielsysteme nicht erreichbar. Damit kann technisch erzwungen werden, dass sich externe Dienstleister vor Beginn des Fernzugriffs (telefonisch) anmelden müssen. In einer App kann etwa ein Schichtleiter zunächst Informationen zum gewünschten Fernzugriff erfassen und jeden einzelnen Fernwartungsrechner per Knopfdruck starten und stoppen. Zudem hat er einen Überblick über alle inaktiven und aktiven Fernwartungsrechner. Aktuelle Sessions auf den Fernwartungsrechnern lassen sich per Mausklick spiegeln, sodass ein Vier-Augen-Prinzip beim Fernzugriff möglich ist. Nach dem Start eines Fernwartungsrechners ist dessen Desktop-Oberfläche bis auf einen Beenden-Button leer. Bei der Erfassung des Fernzugriffswunsches wird die Anlage beziehungsweise das Zielsystem abgefragt, worauf der Zugriff erfolgen soll. Der Schichtleiter aktiviert per Klick die zugehörige Serviceanwendung auf dem Desktop des externen Service-Partners.

Serviceanwendungen ohne Hopping

Auch die installierten Serviceanwendungen werden mit der Lösung über eine darunterliegende Anwendungsfirewall geschützt. Im Detail ist für jede installierte Serviceanwendung hinterlegt, welche Programme und Plug-Ins gestartet werden dürfen, welche Zielsysteme auf welchen Ports angesprochen werden können und welche Parameter der Anwendung erlaubt sind. Damit wird das 'Hopping' zu Systemen außerhalb der eigenen Sicherheitszone verhindert. Ein abgesicherter, bidirektionaler Datenaustausch über SFTP mit den externen Service-Dienstleistern ist im System integriert. Mittels kontrollierter Synchronisation zwischen den Sicherheitszonen ist auch hier kein direkter Durchgriff auf Produktionsanlagen möglich.

Skalierbar durch Visualisierungstechnik

Mit dem weitreichenden Einsatz von Virtualisierungstechnologien ist die Lösung sehr gut skalierbar. Sie bietet tiefgestaffelte Sicherheitsfunktionen auf Hardware-, Netzwerk-, Software- und Organisationsebene. Gerade für kritische Produktionssysteme und Infrastrukturen kann es sich lohnen, einen Blick auf die IT-Securitylösung und die Sicherheitsfunktionen-Checkliste auf der Zedas-Webseite zu werfen. ■

Autor: ***Ulrich Lieske,***
Leiter BU Systemintegration,
Zedas GmbH
www.zedas.com