EIN WEB-MAGAZIN VON INDUSTR.COM

Sicherer Remote Service

GUT GESCHÜTZT BIS IN DIE TIEFE

TEXT: ULRICH LIESKE, ZEDAS

07.05.2018 | Was sich liest wie aus einem Taktikhandbuch für die Generalstabsakademie ist heute für die digitalisierte Fabrik im Industrie-4.0-Zeitalter ebenso relevant. Eine tiefgehende Abwehr macht die Verteidigung gegen potentielle Angreifer erfolgreicher.

TAGS | REMOTE REMOTE SERVICE DIGITALISIERUNG IT-SICHERHEIT ZEDAS GMBH

Kaum ein Unternehmen verzichtet heute auf den Service für seine produzierenden Anlagen. Stillstand und Ausfall erzeugen rasch horrende Kosten. Hersteller, Lieferanten und Dienstleister bieten deswegen Remote Services an, um schnellen und kostengünstigen Support für ihre Anlagen bereitzustellen. Hat das Unternehmen keine Vorgaben oder eine zentrale Lösung für den Remote Service, entsteht ein Sammelsurium unterschiedlichster Fernzugriffslösungen. Diese wiederum besitzen ganz verschiedene Sicherheitseigenschaften.

Es dauert nicht lange und die Hoheit des Eigners über die Anlagen geht verloren. Niemand weiß mehr sicher, wann, wie und wer von außen auf die Anlagen zugreift. Die zunehmende Vernetzung der Anlagen untereinander öffnet Tür und Tor für den möglichen Querzugriff zwischen den Anlagen und ihren Steuerungen. Sicherheitszonen, die über Firewalls abgeschottet sind, sollen das unterbinden. Sind die Firewall-Regeln immer korrekt und aktuell? Im Zweifelsfall geht jedoch oft Funktion vor Sicherheit.

Nicht wenige Firewalls verbrauchen lediglich Strom, weil ihre Regelwerke deaktiviert wurden. Ist nur mit Firewall und Virtual Private Network (VPN) für externe Servicedienstleister der ruhige Schlaf des Produktionsverantwortlichen einer digitalisierten Fabrik garantiert? Digitalisierung, Vernetzung und der Einsatz verschiedener Systemlieferanten innerhalb der Ausrüstung moderner Produktionsumgebungen stellen den Eigner vor ganz

neue und besondere Herausforderungen.

Wie sich Servicearbeiten Externer regulieren, kontrollieren und nachweisen lassen, sind offene Fragen. Ebenso unbeantwortet ist, wie eine einfache Handhabung komplexer Sicherheitsmaßnahmen möglich wird und wie ein hohes Sicherheitsniveau auch innerhalb des Unternehmens zu gewährleisten ist. Für Unternehmen mit kritischer Infrastruktur, die unter das zukünftige IT-Sicherheitsgesetz fallen, werden sich diese Anforderungen demnächst noch verschärfen.

Nutzen von eigenen Erfahrungen

Es gilt, den Wildwuchs von Lösungen für den Remote Service zu beseitigen und ihn durch eine zentrale und sichere Lösung zu ersetzen, die der eigenen Verantwortung unterliegt. Bewährte Sicherheitskonzepte, ergänzt mit einer einfachen Steuerung und Kontrolle durch Mitarbeiter aus den Produktionsbereichen, sind zwingende Grundlage dafür, die Hoheit über die eigenen Anlagen zu behalten. Aus den eigenen Erfahrungen der Integration von Software-Lösungen entwickelte Zedas eine Remote-Service-Lösung, die erprobte Sicherheitsverfahren mit einer außergewöhnlichen Staffelung in der Tiefe bei einfachster Handhabung kombiniert.

Absicherung der Fernwartungsrechner

SecureFactoryRAS von Zedas gewährleistet den Schutz auf mehreren Ebenen. Es ist eine standardisierte Lösung, die es einem produzierenden Unternehmen einfach und schnell ermöglicht, eine zentrale Lösung out-of-the-box für alle seine externen Service-Dienstleister zu etablieren.

Neben den bekannten und üblichen Maßnahmen zur Absicherung der Netzwerkzugänge (starke Authentifizierung mit PIN und Einmal-Passwort, Network Admission Control) und der Netzwerksicherheit (Zertifikate, Verschlüsselung, Firewall, Sicherheitszonen) erfolgt zusätzlich eine umfassende Absicherung auf den Ebenen der zentral bereitgestellten Fernwartungsrechner, der für den Service verwendeten Softwareanwendungen sowie der betrieblichen Organisation der Zugriffssteuerung und -protokollierung.

Mehr als Netzwerksicherheit

Die für jeden externen Service-Dienstleister in einer dedizierten Sicherheitszone bereitgestellten virtuellen Fernwartungsrechner von SecureFactoryRAS sind im Grundzustand ausgeschaltet. Selbst mit erfolgreichem Netzzugang nach Authentifizierung sind die in den Firewall-Regeln freigeschalteten Zielsysteme nicht erreichbar. Damit lässt sich technisch erzwingen, dass sich externe Dienstleister vor Beginn des Fernzugriffs (telefonisch) anmelden müssen. In einer nutzerfreundlichen App kann zum Beispiel ein Schichtleiter zunächst Informationen zum gewünschten

Fernzugriff erfassen und jeden einzelnen Fernwartungsrechner per Knopfdruck starten und stoppen. Zudem hat er einen permanenten Überblick über alle inaktiven und aktiven Fernwartungsrechner.

Aktuelle Sitzungen auf den Fernwartungsrechnern lassen sich per Mausklick spiegeln (Beobachten-Funktion), so dass ein Vier-Augen-Prinzip beim Fernzugriff möglich ist. Nach dem Start eines Fernwartungsrechners ist dessen Desktop-Oberfläche bis auf einen Beenden-Button leer. Im Zuge der Erfassung des Fernzugriffswunsches wird die Anlage beziehungsweise das Zielsystem abgefragt, worauf der Zugriff erfolgen soll. Der Schichtleiter „pusht“ per Klick die zugehörige Serviceanwendung auf den Desktop des externen Service-Partners.

Eine starke Firewall gegen „Hopping“

Ein weiteres Highlight ist die Absicherung der installierten Serviceanwendungen über eine darunterliegende Anwendungsfirewall. 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 wirkungsvoll verhindert. Ein abgesicherter, bidirektionaler Datenaustausch über SFTP mit den externen Service-Dienstleistern ist in die Lösung integriert. Mittels kontrollierter Synchronisation zwischen Sicherheitszonen ist auch hier kein direkter Durchgriff auf Produktionsanlagen möglich.

Einsatz in der Praxis

Mit dem umfassenden Einsatz von Virtualisierungstechnologien ist die Lösung sehr gut skalierbar. Sie bietet tief gestaffelte Sicherheitsfunktionen auf Hardware-, Netzwerk-, Software- und Organisationsebene. Im praktischen Einsatz heben Produktionsverantwortliche die schnelle Erfassung von Serviceanforderungen und die sehr einfache Handhabung hervor. Digitalisierte Fabriken sind heute real und benötigen eine Zutritts-, Zugangs- und Zugriffskontrolle, die auch die digitalen Tore schützt. Zwischen dem Schlüssel mit einfachem Bart und einem tiefgehenden Schutz bietet der Markt unterschiedliche Lösungen. Für kritische Produktionssysteme und Infrastrukturen eignet sich SecureFactoryRAS von Zedas.