Rechner ausschalten!

Ein Beitrag zu mehr Sicherheit bei Fernwartung

Ein ausgeschalteter Rechner gilt als sicher – arbeiten kann man darauf allerdings auch nicht. Das Dilemma zwischen Funktion und Sicherheit beschäftigt jeden, der die IT industrieller Anlagen schützen soll. Alle Rechner mit Kommunikationsverbindung zu einer Produktionsanlage sind ein potentielles Einfalltor und eine Gefahr für die IT-Sicherheit.

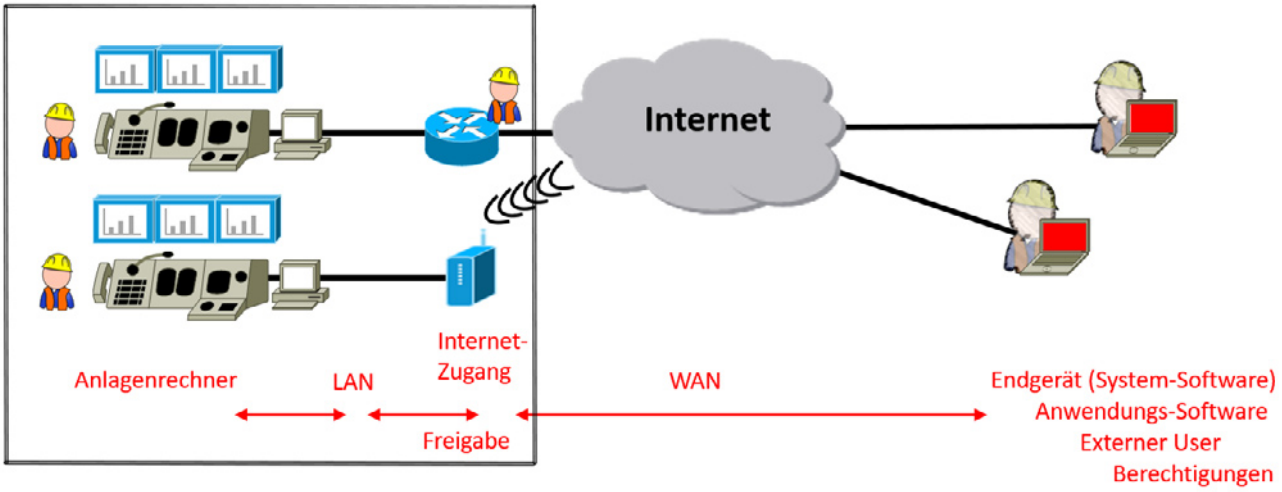

Bild: Zedas GmbH

Schutzbedarf bei Fernwartung

Oft wird suggeriert, dass durch den Einsatz eines VPN-Routers bereits die IT-Sicherheit hergestellt ist. Das greift aber zu kurz. In der Realität wird mittels Fernwartung das Anlagen-Netzwerk, sicher verschlüsselt und über das Internet, mit dem Firmennetzwerk oder den Endgeräten des externen Dienstleisters verbunden. Und Fernwartung umfasst mehr schutzbedürftige Komponenten als nur das verbindende Netzwerk. Dazu gehören:

- Anlagenrechner (Zielsysteme)
- Lokales Netzwerk (LAN)
- Internetzugang (Verbindung von LAN und WAN)
- Weitverkehrsnetzwerk (WAN)
- Endgeräte (Servicerechner) inklusive Systemsoftware
- Anwendungssoftware für Zugriff auf Zielsysteme
- User-Accounts/Authentifizierung/Berechtigungen
- Freigabe und Kontrolle durch Produktionsverantwortliche
- Systemadministration

Mit der IEC62443, dem Security-Kompendium für industrielle Kontrollsysteme des Bundesamtes für Sicherheit in der Informationstechnik (BSI), dem Standard von VGB PowerTech namens VGB-S-175 und dem Whitepaper des BDEW (Bundesverband der Energie- und Wasserwirtschaft) existieren mittlerweile Normen und Referenzarchitekturen, die einen Überblick zum Thema IT-Sicherheit, speziell in Industriebereichen, geben. Das BSI hat die grundlegenden Anforderungen an sichere Fernwartungszugänge im industriellen Umfeld wie folgt zusammengefasst:

- Architektur,
- sichere Kommunikation,
- Authentisierungsmechanismen,
- Organisatorische und
- Kundenspezifische Anforderungen.

Integrieren müssen Betreiber

Der Abgleich der aufgeführten Normen und Standards mit den Angeboten des Marktes führt zur Erkenntnis, dass etablierte und praxiserprobte Standardprodukte verfügbar sind, die technische IT-Sicherheit mittels ‘defense in depth’ realisierbar machen. Dazu gehören Firewall-Systeme, VPN-Lösungen, starke Authentifizierung, Network Access Control, Virenschutz, Backup & Recovery, Intrusion Detection und Prevention, Fernsteuer-Software, bis hin zur Anomalie-Erkennung. Diese einzelnen Bausteine werden von verschiedenen Anbietern miteinander kombiniert und auch als dedizierte Fernwartungslösungen angeboten. In vielen Fällen ist Fernwartung auf diesem Niveau fester Lieferbestandteil einer Anlage. Damit laufen auf dem Boden der Anlagenbetreiber eine Vielfalt unterschiedlicher IT-Security-Lösungen. Zumal der Bedarf

Auszug aus IT&Production, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 12/2019.

nach Fernwartung rasant steigt. Die Integration der Fernwartung in ein übergreifendes IT-Sicherheitskonzept für Produktionsanlagen bleibt indessen dem Betreiber vorbehalten.

Lücken im Schutzwall

In Bezug auf IT-Sicherheit fokussieren Fernwartungslösungen meist auf den Schutz des Anlagen-Netzwerkes und des Netzwerkzuganges. Firewall-Regelwerke bis auf Protokollebene, Verschlüsselung des Datenverkehrs und starke Authentifizierung sind charakteristisch. Die Endgeräte und die verwendete Software der externen Dienstleister bleiben jedoch außerhalb der Kontrolle des Eigners der Produktionsanlagen. Ein weiteres Manko zahlreicher Fernwartungslösungen ist die verwendete Fachsprache innerhalb der Lösungen, die sich oft nur an IT-Spezialisten richtet. Diese Abteilung soll aber in der Regel nicht die Prozesssicherheit verantworten. Des Weiteren fehlen oft integrierte Organisationslösungen, die ein zentrales und dezentrales Beobachten, Koordinieren und Kontrollieren von Fernwartungsarbeiten durch Mitarbeiter der Produktion gewähren.

Angriffspunkt Endpoint

In den BSI-Veröffentlichungen zur Cyber-Sicherheit gehören im Jahr 2019 zu den zehn häufigsten Bedrohungen und Gegenmaßnahmen von Industrial-Control-Systemen:

- das Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware,
- Infektionen mit Schadsoftware über Internet und Intranet,
- die Kompromittierung von Extranet und Cloudkomponenten und
- der Einbruch über Wartungszugänge.

In allen vier Punkten nutzen Angreifer ihre externe Hard- und Software, um über unzureichend gesicherte Netzwerkzugänge, interne Systeme und Software Schaden zu stiften. Das Prinzip 'Minimal need to know' gilt als wesentlicher Baustein einer Problemlösung. Demnach stehen einer Person nur die Informationen zur Verfügung, die unmittelbar ene konkreten Aufgabe erforderlich sind. Organisationsmängel, Social Engineering, menschliche Schwächen und unklare Definition der Aufgaben führen leicht zur Kompromittierung dieses Wissens. Deswegen ergänzt das Prinzip 'Minimal to have' den IT-Schutz. Einer Person stehen dabei nur die Ressourcen und Systeme zur Verfügung, die unmittelbar für die Erfüllung einer konkreten Aufgabe notwendig sind. Eine Vielzahl von technischen Maßnahmen, wie verschlüsselte Übertragung von Daten per VPN, Firewall-Regelwerke, Zugriffsberechtigungen, Network Access Control, Härtung der Zielsysteme dienen der Umsetzung des Prinzips. Die Ausnutzung von Software-Schwachstellen, Denial of Service – Angriffe, Pishing, Brute Force Attacken und vor allem die unsichere Konfiguration von Systemen bieten jedoch auch hier zahlreiche Angriffsvektoren.

(Fast) alles verboten

'Security by Default' fasst die beiden Minimal-Prinzipien dahingehend zusammen, dass per Default alles verboten ist, was nicht explizit erlaubt wurde. Konsequenterweise heißt das, dass zum Zeitpunkt der Erfüllung einer konkreten Aufgabe ausschließlich die dafür notwendigen Hardware-, Software- und Netzwerk-Ressourcen einem berechtigten Anwender zur Verfügung stehen dürfen. Rechner und Software bei Externen, die z.B. per Fernwartung auf eine Anlage zugreifen, sind vom Anlageneigner allerdings kaum zu kontrollieren. Die Installation von Endpoint-Security-Software auf fremden Rechnern wird fast nie erlaubt. Die digitale Hoheit des Anlagen-Eigners endet zumeist vor den Fernwartungsrechnern seiner externen Dienstleister.

Endpoint Security integriert

Aus den jahrelangen Erfahrungen der Integration eigener Software-Lösungen in Industrieumgebungen entstand bei der Zedas GmbH eine Lösung für Anlagen, die erprobte Sicherheitsverfahren mit gestaffelter Tiefe kombiniert. Die Standardlösung ermöglicht es , den Zugriff aller externen Service-Dienstleister zu verwalten. Die Anwendung namens ZedasSecure kann das Prinzip 'Security by Default' durchgängig sicherstellen, auch auf den

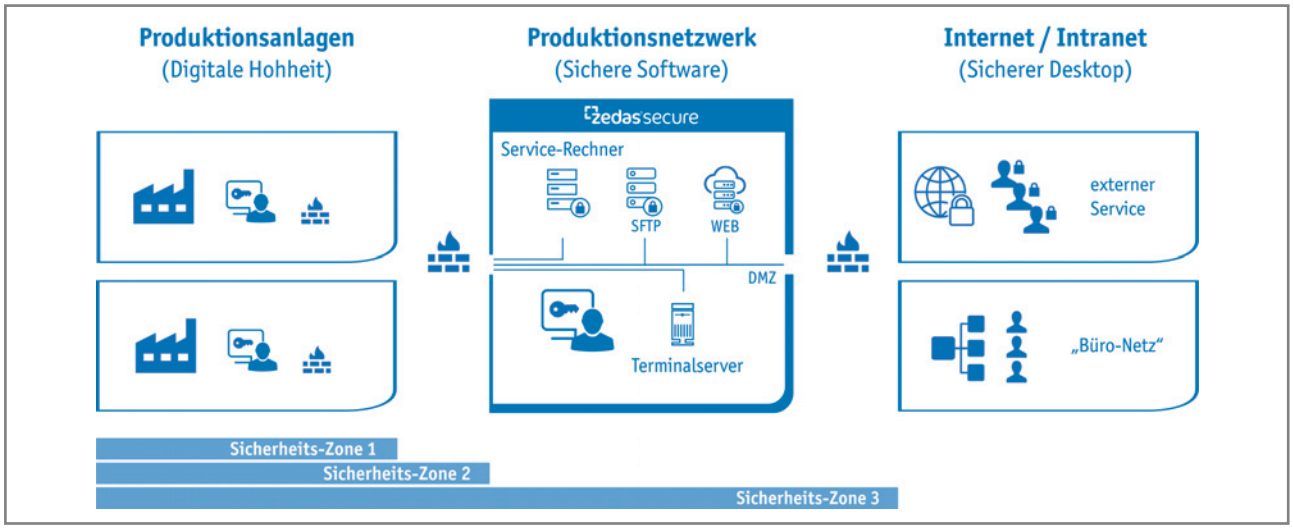

Bild: Zedas GmbH

ZedasSecure – herstellerübergreifendes Sicherheitskonzept im Überblick

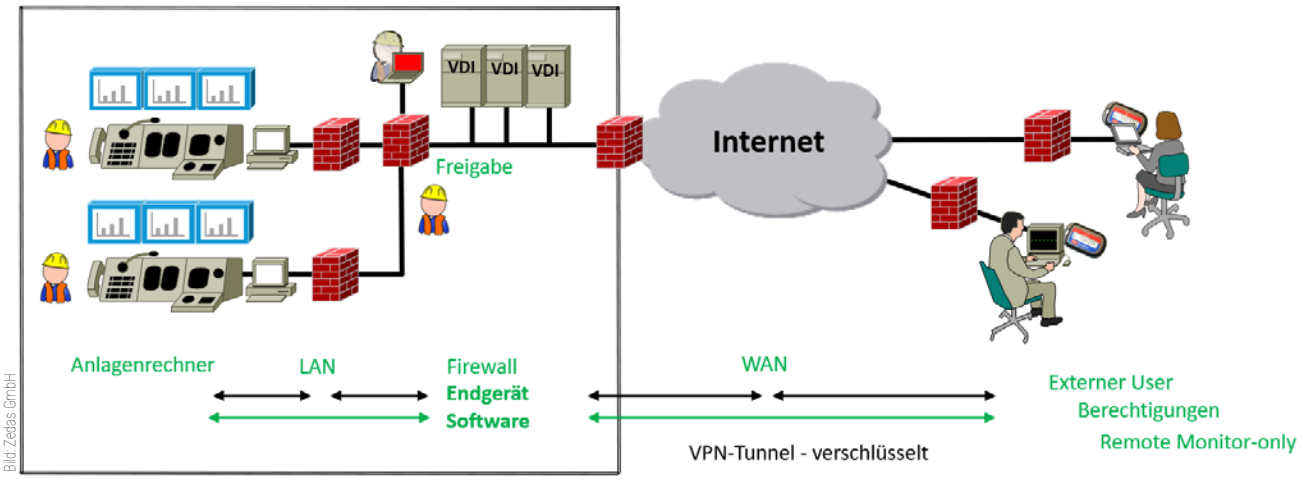

Bild: Zedas GmbH

Umfassender Schutz der Produktionsanlagen bei Fernwartung

Endpoints, die von Externen für den Zugriff auf Produktionsanlagen benutzt werden. Endgeräte, denen Zugriff auf Produktionsanlagen gewährt wird, sind im System als virtuelle Fernwartungsrechner geführt, die vom Anlagenbetreiber kontolliert werden. Für jeden Dienstleister werden sie in dessen zugeordneter Demilitarisierter Zone (DMZ) aufgesetzt. Ihre Desktop-Oberfläche wird ausschließlich über Remote Desktop Protokoll und verschlüsseltes HTML5-VPN bereitgestellt. Dafür benötigt der Dienstleister einen HTML5-fähigen Browser. Die Installation eines VPN-Clients ist nicht erforderlich.

Freigabe nach Telefonanruf

Der Netzwerkzugriff externer Dienstleister setzt eine Authentifizierung des Servicemitarbeiters mittels Token-Einmalpasswort voraus. Ein direkter Zugriff von Endgeräten der Dienstleiter auf Anlagen ist danach trotzdem nicht erlaubt. Das zweistufige Firewall-System gewährt Externen ausschließlich den Zugriff auf jeweils ihre virtuellen Fernwartungsrechner. Diese sind per Default ausgeschalten. Technisch erzwungen, muss sich somit der externe Dienstleister telefonisch beim Anlagenbetreiber melden, um den Start seines Fernwartungsrechners anzufordern. Mittels Software-App erfassen Schichtleiter die Fernwartungsanforderungen externer Dienstleister. Dazu gehören Namen der Firma und des Mitarbeiters, dessen Rückrufnummer, die Auftragsnummer, die Anlage mit Beschreibung der Servicetätigkeit, die Softwareanwendung sowie die voraussichtliche Dauer des Serviceeinsatzes. Dafür werden kaum mehr als 90 Sekunden benötigt. Alle einmal erfassten Eingaben werden wiederkehrend zur Auswahl angeboten. Zudem bietet die App einen permanenten Überblick über alle inaktiven und aktiven Fernwartungsrechner.

Dokumentierte Arbeiten

Die genannten Informationen werden zusammen mit Start- und Abschaltzeit des virtuellen Fernwartungsrechners elektronisch dokumentiert. Ihre Erfassung ist Voraussetzung dafür, dass der zugeordnete Fernwartungsrechner aus der App heraus gestartet werden kann. Nach dem Start eines Fernwartungsrechners befindet sich auf dessen stets leerer Desktop-Oberfläche lediglich ein Herunterfahren-Button. Der Rechtsklick ist deaktiviert. Es können keine Sondertasten, wie Windows-, Alt-, Steuerung- und F-Tasten, verwendet werden. Über den Start-Button sind keine weiteren Anwendungen sicht- oder startbar. Im Zuge der Erfassung des Fernzugriffswunsches wird die Anlage bzw. das Zielsystem abgefragt, worauf der Zugriff erfolgen soll. Der Schichtleiter schiebt per Maus ausschließlich die zugehörige Anwendungsverknüpfung auf den Desktop des externen Service-Partners.

Kontrolle Ende-zu-Ende

Aktuelle Sessions auf den Fernwartungsrechnern lassen sich auf administrativen Systemen spiegeln (Beobachten-Funktion), sodass ein Vier-Augen-Prinzip beim Fernzugriff möglich ist. Die zugewiesene Software wird grundsätzlich durch eine zusätzliche Applikationsfirewall abgesichert. Für jede installierte Serviceanwendung ist hinterlegt, welche Programme und Plug-Ins gestartet werden dürfen, welche Zielsysteme auf welchen Ports angesprochen werden dürfen und welche Parameter der Anwendung erlaubt sind. Nach Abschluss des Fernzugriffs sind die Fernwartungsrechner heruntergefahren und ausgeschaltet. Die zugewiesenen Anwendungsberechtigungen werden automatisiert wieder zurückgenommen. Unabhängig davon hat der Schichtleiter in seiner App zu jeder Zeit die Option zur Zwangstrennung eines Fernwartungsrechners.

Digitale Hoheit

Mit dem Fernwartungssystem steht Anwendern eine nützlich Komponente eines weit gefassten IT-Schutzkonzeptes für industrielle Anlagen zur Verfügung. Es schützt auf Netzwerkebene, auf Endgeräte- und Softwareebene sowie einer durch Produktionsmitarbeiter handhabbaren Organisationsebene. Das Prinzip 'Minimal need to have' wird konsequent auf die virtuellen Fernwartungsrechner und die darauf zu verwendende Software ausgeweitet. Der Anlagenbesitzer ist so in der Lage, seine digitale Hoheit auch über die Endgeräte des Anlagenzugriffs auszuüben. ■

Der Autor Ulrich Lieske ist Leiter Systemintegration bei der Zedas GmbH.

www.zedas.com

IT&Production

Auszug aus IT&Production, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 12/2019.