Cybersecurity – von Grund auf sicher

Datenausleitung und Remote Access – Zugriff auf sensible Anlagen organisieren

Damit die Öffnung sensibler Bereiche in der Prozessindustrie nicht zu einem Fiasko wird, muss zusätzlich zum Thema der IT-Sicherheit die OT-Security weit nach oben auf die Tagesordnung gerückt werden. Allerdings reichen altbewährte Schutzmaßnahmen allein nicht mehr aus. Unterstützung zur Sicherung kritischer Anlagen bekommen Anwender von Experten, die modernste Methoden implementieren.

©Eakrin - stock.adobe.com

Industriespionage, Erpressung, Sabotage, die Liste der Sorgen bei Verantwortlichen in der Prozessindustrie ist so lang wie berechtigt. In der Industrie gibt es zuhauf Schadensfälle rund um Cyberkriminalität, nur gelangen sie meist nicht an die große Öffentlichkeit. Wer in Zeiten der Digitalisierung jedoch noch denkt, das Abkapseln der eigenen Anlagen von der Außenwelt sei die einzig richtige Lösung, der irrt. Zu schwergewichtig sind die Argumente, die für immer leistungsstärkere digitale Hilfsmittel sprechen. Und: Zu groß ist der Wettbewerbsdruck. Kaum ein Betrieb wird es sich mittelfristig erlauben können, ohne Prozessdatenanalyse, Betriebsmittelfernwartung und Monitoring des Produktionsprozesses zu produzieren.


© Genua

Beim Remote Access ist die Gefahr für die Integrität und die Verfügbarkeit der Anlagen zunächst einmal sehr groß.

Markus Maier, Genua

Datenausleitung mit der Datendiode sichern

Während vernetzten Maschinen in vielen Szenarien eine rosige, manchmal sogar autonom produzierende Zukunft vorausgesagt wird, gehört der vorausschauenden Instandhaltung bereits die Gegenwart. Das Monitoring ist häufig ein erster Schritt, mit dem Informationstechnologie (IT) und Betriebstechnologie (OT, Operational Technology) zusammenwachsen. Grundlage ist immer, den Zustand eines Assets möglichst gut beurteilen zu können. Dazu müssen entsprechende Daten – am besten lückenlos – an eine übergeordnete Einheit übermittelt werden. In solchen Szenarien besteht kein Schreibzugriff auf die Maschinen und Anlagen, jedoch ist eine mehr oder weniger permanente Datenverbindung vorhanden.

Bei Monitoring oder Predictive Maintenance entsteht zunächst keine große Gefahr für die Integrität und Verfügbarkeit der Anlagen. Voraussetzung ist allerdings, dass es wirklich keine Rückkopplung auf die Maschinen gibt. Dem Namur-Open-Architecture-Ansatz folgend, wird dies durch eine spezielle Hardware sichergestellt – auch als Daten- oder Cyber-Diode bezeichnet. Ein solches NOA Security Gateway garantiert eine absolut zuverlässige Datenverbindung. Es gibt nur einen minimalen Feedback-Kanal für Status-Meldungen.

Die One-Way-Datenübertragung über eine Cyber-Diode kann direkt und gesichert aus verschiedenen Ebenen der Automatisierungspyramide erfolgen, z.B. in die Cloud zur Datenanalyse. Auf diese Weise geschützt, versenden Maschinen, Anlagen und IT-Systeme Daten über öffentliche Netze, ohne dass ihre Integrität gefährdet wird. Auch ein Datentransfer aus der Steuerungsebene in die Prozessleitwarte ist direkt und ohne Rückkoppelung möglich.

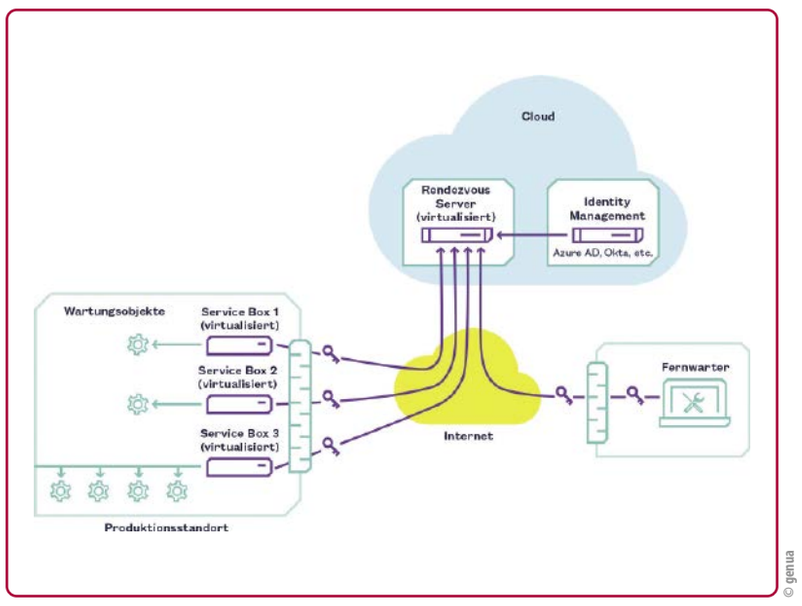
In der jüngsten Version unterstützt die Cyber-Diode auch die native OPC-UA-Verschlüsselung und Authentifizierung. Es kann zudem sichergestellt werden, dass lediglich eine Teilmenge der OPC-UA-Nodes ausgelesen wird. Zum Hintergrund: Steuerungen senden in der Regel eine große Anzahl an Daten auf unterschiedlichen Knoten, von denen die Zielsysteme meist aber nur einen kleinen Ausschnitt benötigen. Der Vorteil liegt in einem optimierten Datendurchsatz sowie geringeren Lizenzkosten für den Endanwender.

Aktiven Zugriff via Remote Access ermöglichen

Im wesentlichen Unterschied zur reinen Datenausleitung muss beim Remote Access mehr Aufwand betrieben werden, um Anlagen vor fremdem Zugriff zu sichern. Doch es lohnt sich: Manches Problem lässt sich bereits durch einen einfachen Mausklick aus der Ferne lösen. Eine Kalibrierung ist schnell angestoßen oder eine Firmware per Mausklick aktualisiert.

Es gilt also abzusichern, dass jemand aktiv und schreibend auf das System zugreift. Dabei hilft es, dass eine Person nur zeitlich begrenzt Zugriff auf eine bestimmte Anwendung erhalten muss. Wichtig ist, dass wir BSI-konform indirekten Zugriff auf ein Zielsystem durch ein sog. Application Level Gateway ermöglichen.

Der VDMA-Arbeitskreis „Sichere Fernwartung“ hat verschiedene Fernwartungsarchitekturen mit Vor- und Nachteilen beschrieben. Viele dieser Varianten unterliegen hohen Risiken, da sie VPN-basiert eine direkte Netzkopplung zwischen Fernwarter und Zielsystemnetzwerk herstellen.



© genua

Architektur einer sicheren Fernwartung. Ein Rendezvous-Server, auf dem sich Fernwarter und Betreiber „treffen“, kann On-Premise oder in der Cloud betrieben werden. Die finale Freigabe auf das zu wartende Zielsystem erfolgt immer Seitens des Betreibers von einem VPN Client aus. Durch Mikrosegmentierung eines Wartungsprojekts vom restlichen Netz kann die Sicherheit weiter erhöht werden.

Stand der Technik ist daher eine rendezvousbasierte Architektur. Hier steht bspw. ein VPN-Rendezvous-Server in einer speziellen Netzwerkzone. Auf einen solchen Server kann von außen nur verschlüsselt zugegriffen werden. Die Freigabe auf das zu wartende Zielsystem erfolgt seitens des Betreibers intern von einem VPN Client aus – bei Genua die Servicebox. Diese verbindet sich ebenso mit dem Rendezvous-Server, auf dem sich interne und externe Partner „treffen“.

Der Rendezvous-Server steuert die Fernwartung, indem er die Identität des Zugreifenden überprüft und die Anfrage durch den Empfänger bestätigen lässt. Im klassischen Fall muss also immer ein Operator innerhalb der Firma zu einem vereinbarten virtuellen Treffpunkt kommen und den Fernwarter in Empfang nehmen. Allein diese Vorgehensweise ergibt eine wesentlich höhere Sicherheit, da es bei abgebauter Verbindung keine Möglichkeit gibt, durch die Firewall von außen in die Industrial Zone durchzukommen.

Darüber hinaus definieren die Anzahl und Verteilung der Service-Boxen, die vor den Wartungszielen platziert werden, den Grad der Sicherheit. Eine einzelne Service-Box sichert ein Werk, eine Produktionslinie oder einzelne Maschinen ab. Sie segmentiert also das Zielsystem vom restlichen Netz und routet die jeweils erlaubte Verbindung an ihr Ziel. Damit solche Zugriffsszenarien auch in komplexen Anlagen mit unterschiedlichen Sicherheitsanforderungen funktionieren, können die Netzwerke beliebig stark segmentiert und Nutzern sehr kleinteilig nur die Berechtigungen für einzelne Netzsegmente erteilt werden, bis hin zu einer Servicebox vor jedem Zielsystem.

Höhere Sicherheit durch Zero Trust und Defense-in-Depth

Die starke Beschränkung von Zugriffsrechten entspricht dem zeitgemäßen Zero-Trust-Paradigma. In der Zero-Trust-Denkweise muss ein Nutzer nachweisen, genau auf diese eine Maschine bzw. für diesen einen Anlagenkomplex zugriffsberechtigt zu sein. Damit der Schutz wirkt, müssen Rechte dementsprechend restriktiv vergeben werden. Bei der auch Least Privilege genannten Vorgehensweise werden nur die absolut notwendigen Zugriffsmöglichkeiten erteilt. So wird bspw. der Zugriff auf möglichst nur ein Protokoll des Zielsystems erlaubt. Auch weitere einschränkende Maßnahmen sind möglich, wie z.B. der Zugriff auf bestimmte Standorte oder Anwendungen oder zu bestimmten Zeiträumen.

Solch ein restriktiver Zugang auf Systeme beschränkt zudem den Schaden, falls sich eine Person unbefugt Zugriff beschafft hat. Je stärker und sinnvoller die Bereiche segmentiert sind, umso geringer fällt ein potenzieller Schaden aus.

Identity-Management in der Cloud

Als weiterer Sicherheitsbestandteil sind starke Identitäten notwendig. Einfache Passwörter sind nicht mehr zielführend. Mehrfaktor-Authentifizierung, kryptografisches Material zur Authentifizierung, Public-Private-Verschlüsselung oder gesonderte Zertifikate sollten Standard sein.

Damit die Identitäten ihrerseits geschützt sind, empfiehlt sich die Nutzung spezieller Services, die dabei helfen, Accounts und Berechtigungen zu managen. Mithilfe von Cloud Identity Providern wird der Zugang grundsätzlich gesteuert. Gerade die Nutzer- und Rollenverteilungen sind bei Cloud-Lösungen einfach zu pflegen und sehr hoch skalierbar. Welches System genutzt wird, bleibt dem Anwender überlassen. Die Genua Fernwartungslösung kann flexibel an unterschiedliche Open-Source- oder Closed-Source-Authentifizierungssoftware wie Active Directory, Azure Active Directory, Keycloak, Radius-Derivate oder Okta angedockt werden.

Mit dem Schlimmsten rechnen

Beim Konzept „Assume Breach“ versucht eine Kombination aus Software und menschlichen Überprüfungen herauszufinden, wann das Risiko einer Lücke auftritt. Im Fall der Fernwartung unterstützen wir diesen Ansatz, indem alle Vorgänge als Logmeldungen im Common-Event-Format an ein zentrales SIEM-System (Security Information and Event Management) des Kunden weitergegeben werden. Mitarbeiter überprüfen entsprechende Vorfälle und leiten ggf. weitere Aktionen ein.

Mit allen Maßnahmen gemeinsam sind die Anlagen zuverlässig vor unbefugtem Zugriff abgesichert. Doch es geht nicht ohne den Willen der Verantwortlichen, Veränderungsprozesse anzunehmen und positiv zu gestalten. Es ist essenziell, dass sich die unterschiedlichen Akteure im Unternehmen von vornherein an einen Tisch setzen, an einem Strang ziehen und die Probleme und Bedürfnisse der jeweils anderen Seite sehr ernst nehmen. Nur so finden wir gemeinsam Lösungen, mit der alle gut arbeiten können und die sinnvolle Maßnahmen wie Remote Access oder Maschinenvernetzung für den Betrieb sicher erschließen.

Markus Maier, Product Owner Industrieprodukte, Genua GmbH, Kirchheim bei München

■ www.genua.de