So lassen sich IT- und OT-Systeme in der Fertigung aus der Ferne verwalten

Sichere Zugänge und Kommunikationswege gehört zu den Basisanforderungen an die Fernwartung im OT- und IT-Umfeld. © bigstockphoto.com / leowolfert

Das Bundesamt für Sicherheit in der Informationstechnik macht sich regelmäßig Gedanken um die Sicherheitslage von hiesigen Unternehmen und gibt dazu das IT-Grundschutz-Kompendium heraus. Seit Februar dieses Jahres ist dort der Abschnitt „IND 3.2 – Fernwartung im industriellen Umfeld“ enthalten. Dies alleine zeigt die Bedeutung dieses Themas seitens des BSI.

Status Quo der Fernwartung im industriellen Umfeld

Sieht man sich die aktuelle – immer weiter digitalisierte - Betriebstechniklandschaft (Operational Technology; OT) genauer an, fällt vor allem eins auf: Sie weist eine enorme Heterogenität auf. Das betrifft dezentrale Infrastrukturen genauso wie die vielfältigen Steuersysteme und deren Zugriffsarten. Alleine das erfordert eine recht hohe Zahl unterschiedlicher Fernwartungszugänge. Diese werden wiederum ganz unterschiedlich realisiert, bestehen also aus einer unüberschaubaren Zahl an Hard- und Software-Komponenten.

Diese und weitere Faktoren stellen vor allem verarbeitende Unternehmen vor die Herausforderung, mithilfe der passenden Fernwartungslösung ein Höchstmaß an Sicherheit und Komfortabilität zu schaffen. Das betrifft die OT und die IT gleichermaßen. Hierfür stehen diverse Ansätze und Möglichkeiten zur Verfügung.

Unterschiede und Gemeinsamkeiten bei der IT-/OT-Fernwartung

Vergleicht man aktuelle Fernwartungssysteme, ergeben sich diverse Gemeinsamkeiten, und Unterschiede. So sollten auf jeden Fall sichere Verbindungen genutzt werden. Das betrifft sowohl die infrage kommenden Protokolle wie Simple Network Management Protocol (SNMP) und Intelligent Platform Management Interface (IPMI). Letzteres wird mehr und mehr von Redfish abgelöst, das Web-Techniken wie JSON als Datenformat HTTPS für die Datenübertragung und mehr unterstützt. Zudem gibt es unterschiedliche kryptografischen Verfahren, die u. a. auf dem AES-256-Standard basieren, mit denen Daten und Verbindungswege verschlüsselt werden. Darüber hinaus werden in OT-Infrastrukturen anstatt erprobter Standards wie TCP/IP oder IPsec immer noch proprietäre Protokolle genutzt. Das birgt unter anderem in OT-Netzwerken diverse Gefahren, wie zahlreiche Cyberattacken der Malware-Varianten Ekans, Triton und Industroyer belegen. So brachte beispielsweise Industroyer die Energieversorgung der ukrainischen Hauptstadt Klev 2016 vollständig zum Erliegen.

OT braucht weitere Funktionen

OT-Fernwartung muss zudem noch weitere Funktionen bereitstellen, die bei der reinen IT-Fernwartung keine Rolle spielen, wie beispielsweise den Zugriff auf das ICS (Industrielles Steuerungssystem), um damit ein Anlaufen bzw. ein Stoppen von Anlagen sicherzustellen und so Personen oder Sachschäden zu verhindern. Aber auch die Integrität der anfallenden Daten und das Beschränken der erforderlichen Kommunikationswege sollte das Fernwartungssystem bereitstellen.

Basis-Anforderungen an die Fernwartung

Für ein Mindestmaß an Sicherheit müssen Fernwartungszugänge laut BSI bestimmte Anforderungen erfüllen. Dazu gehört zum Beispiel die Auswahl der infrage kommenden Systeme, die ausschließlich von außen ferngewartet werden dürfen.

OT-Fernwartung muss beispielsweise ein sicheres Anlaufen bzw. ein Stoppen von Anlagen regeln, um Personen oder Sachschäden zu verhindern. © bigstockphoto.com / Freshpixel

© ProSoft GmbH

Autor:
Robert Korherr
Geschäftsführer
ProSoft GmbH
www.prosoft.de

Die Software-basierte Fernwartung kennzeichnet sich durch integrierte Betriebs- und Monitoring-Funktionen aus.
© bigstockphoto.com / ShamimHR

Aber auch ein Minimum an benötigten Zugängen und Kommunikationswegen gehört zu den Basisanforderungen an die Fernwartung im OT- und IT-Umfeld. Ebenfalls sollte eine zuverlässige Verschlüsselung wie AES-256 zum Einsatz kommen.

Empfohlene Anforderungen

Neben diesen Basisanforderungen sollten weitere Standard-Bedingungen erfüllt werden, was die Fernwartung betrifft. Dazu zählt beispielsweise eine Ende-zu-Ende-Verschlüsselung, die auf eine möglichst geringe Zahl an Fernwartungsverbindungen angewandt wird. Aber auch allgemein gültige Richtlinien sollten definiert und beschrieben werden, mit denen sich Rollen, Zuständigkeiten und Verantwortlichkeiten definieren lassen. Hinzu kommt der Einsatz kryptografisch verschlüsselter Protokolle. Für noch mehr Sicherheit empfiehlt sich der Einsatz von sogenannten MFA-Verfahren, die häufig auf dem Einsatz von Hardware-Token basieren. Hierbei sorgt ein USB-Schlüssel beispielsweise für den kennwortlosen Zugriff auf besonders schützenswerte Anwenderkonten. Wichtig ist obendrein ein Notfallplan, der die notwendigen Schritte im Störungsfall beschreibt. Darin wird unter anderem beschrieben, wie auf einen möglichen Malware-Angriff reagiert werden soll. Hierfür werden personelle Zuständigkeiten definiert, die Art und Weise der Systemwiederherstellung, und vieles mehr.

Anforderungen bei erhöhtem Schutzbedarf

Speziell bei Betreibern von kritischen Infrastrukturen (KRITIS) - wie zum Beispiel Wasser- und Stromversorgungsunternehmen - ergibt sich aufgrund ihrer gesellschaftlichen Bedeutung ein erhöhter Schutzbedarf, woraus sich im Bezug auf das erforderliche Fernwartungssystem unter anderem folgende Aspekte ergeben:

- Der Funktionsumfang des OT-Fernwartungssystems sollte an die Administration von IT-Systemen angepasst werden.
- Es sollten möglichst nur solche Fernwartungssysteme eingesetzt werden, mit denen sich IT- und OT-Clients verwalten lassen.
- Redundante Kommunikationsverbindungen sollten für eine möglichst hohe Ausfallsicherheit sorgen.

Zwei Arten der Fernwartung

Bei der Fernwartung von industriellen IT- und OT-Systemen wird in zweierlei Ansätzen unterschieden: Hardware- und Software-basiert. Beide Methoden haben ihre Vor- und Nachteile.

Die Software-basierte Fernwartung kennzeichnet sich vor allem durch den schnellen Einsatz, durch integrierte Betriebs- und Monitoring-Funktionen sowie günstige Lizenzkosten aus. Auf den ersten Blick bieten sich Online-Fernwartungslösungen an, die über eine Internetverbindung zustande kommen. Oftmals mangelhaft geschützte OT-Systeme, die über eine externe Verbindung ferngewartet werden, widersprechen sich. Abgeschlossene OT-Infrastrukturen, sollten auch mit Fernwartungssoftware verwaltet werden, die keine externen Zugänge benötigen um zu funktionieren. Deshalb empfiehlt das Grundschutz-Kompendium diese Art der Fernwartung möglichst selten einzusetzen.

Hardware-basierte Lösungen

Auf der anderen Seite stehen dedizierte, hardware-basierte Fernwartungslösungen zur Auswahl. Die Vor- und Nachteile liegen hierbei auf der Hand. Zum einen arbeiten diese Lösungen sehr zuverlässig und weisen einen hohen Sicherheitsgrad auf. Zum anderen sind die Anschaffungskosten recht hoch, außerdem erfordert das Einrichten geschultes Personal.

Organisatorische Überlegungen bei der Fernwartung

Der sichere Fernzugriff auf IT- und OT-Systeme ist nicht nur mit technischen, sondern auch mit organisatorischen Anforderungen eng verknüpft. Dazu gehört neben der bereits erwähnten Risikoanalyse ein minimales Implementieren von Fernzugriffsmöglichkeiten, exakt definierte Prozesse und Abläufe, klar geregelte Zeitfenster von Remote-Zugängen sowie das regelmäßige Verwalten und Auswerten von Protokolldaten.

Die Umsetzung

So funktioniert die Fernwartung von IT- und OT-Systemen gleichermaßen: Wie praktisch wäre es, wenn sich IT- und OT-Systeme mit ein und demselben Tool wie beispielsweise dem NetSupport Manager (siehe Kasten) aus der Ferne verwalten ließen, und das mit den vom BSI geforderten Sicherheitsstandards. Damit könnte man sowohl IT-Endgeräte als auch Maschinen und Steuerungseinheiten im Fertigungsumfeld mit nur einer einzigen, zentralen Software fernwarten.

Das funktioniert im günstigsten Fall über sämtliche Transportmedien hinweg (also via LAN, WLAN und das Internet), und zwar auf Basis bekannter Protokolle wie TCP/IP und HTTPS. Darüber hinaus lassen sich mit solch einem Werkzeug alle verfügbaren Endgeräte gleichermaßen und gleichzeitig verwalten, die sich damit obendrein inventarisieren lassen. So besteht zudem jederzeit ein Überblick über alle vorhandenen Gerätschaften.

Fazit

IT- und OT-Infrastrukturen können aus der Ferne gewartet und verwaltet werden - mit nur einem Tool. Das Bundesamt der Sicherheit in der Informationstechnik legt hohe Standards an, was die Sicherheitsanforderungen an die notwendigen Fernwartungslösungen im IT- und OT-Umfeld betreffen. Das schließt die zum Einsatz kommenden Hardware- und Software-Komponenten genauso ein wie die Verschlüsselungsmechanismen, die die Verbindungswege und die Daten schützen sollen. Darüber hinaus sollte penibel genau auf die Basis- und Standardanforderungen sowie auf die Bedingungen bei einem erhöhten Schutzbedarf geachtet werden. Und dies alles im Verbund mit der passenden Hardware- oder Software-Lösung, mit der sich idealerweise IT- und OT-Systeme aus der Ferne verwalten und überwachen lassen. ◄

NetSupport Manager

Mit dem NetSupport Manager lassen sich über mehrere Standorte verteilte Netzwerke genauso fernwarten wie heterogene Systemumgebungen. Dies geschieht ganz bequem mithilfe mobiler Endgeräte wie Smartphone oder Tablet. Betriebssystemseitig beherrscht das Tool die ganze Bandbreite an aktuellen Plattformen, also Windows, macOS, Linux, iOS, Android und Google Chrome.

Das Besondere an NetSupport Manager ist dessen ausschließliche Installation im eigenen Rechenzentrum, sodass die Kontrolle vollständig beim Unternehmen bleibt. Hinzu kommt eine verschlüsselte Datenübertragung, für ein Höchstmaß an Sicherheit. Dafür sorgt auch der Kennwortschutz sowie die mögliche Integration, NT-Security und Active Directory. Obendrein unterstützt NetSupport Manager Smartcards zur sicheren Authentifizierung.

Praktischerweise ist zu Trainingszwecken die Online-Schulungs- und Präsentationskomponente NetSupport School integriert. Das erleichtert den Einstieg in die Fernwartungssoftware deutlich.