Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

EMPFEHLUNG: IN DER PRODUKTION

Fernwartung im industriellen Umfeld

Systeme zur Prozesssteuerung, Fertigung und Automatisierung – subsumiert unter dem Begriff Industrial Control Systems (ICS) – sind inzwischen ähnlichen Bedrohungen ausgesetzt wie konventionelle IT-Systeme. Aufgrund von betrieblichen oder wirtschaftlichen Gründen besteht häufig die Anforderung, eine Fernwartung der Systeme über öffentliche Netze vornehmen zu können. Derart angelegte Fernwartungszugänge führen dazu, dass industrielle Anlagen sehr viel stärker exponiert werden und somit zugleich einer gestiegenen Bedrohungslage ausgesetzt sind. Industrielle Fernwartungskomponenten müssen daher heute ein hinreichendes Sicherheitsniveau erfüllen.

Das Spektrum der am Markt verfügbaren Lösungen für Fernwartung im industriellen Umfeld ist sehr groß. Die Angebote reichen von VPN-Lösungen über Cloud-basierte Ansätze bis hin zu Provider-Lösungen im Bereich Machine-to-Machine (M2M). Die Produkteigenschaften einzelner Lösungen unterscheiden sich dabei teilweise signifikant. Die vorliegende Empfehlung gibt einen Überblick über die generischen Anforderungen für industrielle Fernwartung gemäß dem Stand der Technik. Es sei explizit darauf hingewiesen, dass Bestandslösungen auf Basis von analogen oder ISDN-Modems sowie die direkte Internetanbindung von Komponenten wie Speicher-programmierbaren Steuerungen (SPS) nicht dem aktuellen Stand der Technik genügen.

1 Architektur

Die folgenden Anforderungen sollten bereits bei der Planung und Integration einer Fernwartungslösung beachtet werden:

- ✔ Einheitliche Lösung: Besonders in größeren Infrastrukturen sollte möglichst eine einheitliche Lösung zum Einsatz kommen. Dies verringert sowohl die Anzahl der Angriffsvektoren als auch die Komplexität (kein „Wildwuchs“).
- ✔ DMZ: Die Fernwartungskomponente sollte sich möglichst in einer vorgelagerten Zone (DMZ) befinden und nicht direkt im Produktionsnetz lokalisiert sein. Fernwartungszugänge dürfen nicht dazu führen, dass vorhandene umgangen werden. Vielmehr sind Firewalls geeignet, um beispielsweise erlaubte IP-Adressbereiche für eine Fernwartung festzulegen.
- ✔ Granularität der Kommunikationsverbindungen: Der Fernwartungszugriff sollte möglichst nicht pauschal pro (Sub)Netz erfolgen, sondern vielmehr feingranular pro IP und Port geregelt werden können. Dies minimiert die „Reichweite“ von Fernwartungszugängen und beschränkt somit auch die Folgen einer Kompromittierung. Ein möglicher Ansatz ist beispielsweise der Aufbau von 1:1-Verbindungen mittels SSH statt der Kopplung ganzer Netze durch IPsec.

- ✔ Verbindungsaufbau: Der Fernzugriff sollte, sofern möglich, ausschließlich aus dem Unternehmen heraus initiiert werden können. Es sollten keine offenen Ports für einen Verbindungsaufbau von außen vorhanden sein. Alternativ können Fernwartungszugänge temporär aktiviert werden. Dies setzt eine hinreichend sichere Authentisierung und einen aktuellen Patchlevel sowie organisatorische Prozesse zur Gewährleistung der anschließenden Deaktivierung voraus.
- ✔ Dedizierte Systeme: Die zur Fernwartung eingesetzten Komponenten sollten nur diesem Anwendungszweck dienen und nicht mit anderen Funktionalitäten vermischt werden.

2 Sichere Kommunikation

Die Sicherheit der Kommunikation bei einer Fernwartung wird in erster Linie durch etablierte Standardlösungen gewährleistet.

- ✔ Sichere Protokolle: Es werden ausschließlich etablierte Protokolle wie IPsec, SSH oder SSL/TLS in aktuellen Versionen eingesetzt, um einen Tunnel zwischen zwei Endpunkten bzw. Netzen herzustellen. Dabei sind lediglich die aktuellen Versionen der jeweiligen Protokolle zu empfehlen. Weiterführende Informationen hierzu liefert der Mindeststandard TLS 1.2 des BSI[1]. Zudem sollte stets nach aktuellen Meldungen zu Schwachstellen aus diesem Themenbereich Ausschau gehalten werden.
- ✔ Sichere Verfahren: Es werden hinreichend starke kryptographische Verfahren zur Verschlüsselung verwendet, zum Beispiel AES mit mindestens 192 Bit Schlüssellänge[2]. Eine Verwendung der minimal empfohlenen Schlüssellänge, wie z.B. 128 Bit bei AES, ist angesichts der typischerweise langen Lebenszeiten nicht anzuraten. Die Stärke der verwendeten Schlüssel sollten im Rahmen des Sicherheitsmanagements regelmäßig überprüft und ggf. angepasst werden.

3 Authentisierungsmechanismen

Nur unter Einhaltung der folgenden Anforderungen an eine Authentisierung der Nutzer kann für eine Fernwartungslösung ein hinreichendes Sicherheitsniveau geschaffen werden.

- ✔ Granularität der Accounts: Es sollte nur ein Benutzer pro Account vorgesehen werden. Gruppenaccounts sind unbedingt zu vermeiden.
- ✔ Starke Authentisierungsmechanismen: Das beste Sicherheitsniveau bieten Zwei-Faktor-Verfahren, bei denen nicht nur Wissen (z.B. ein Passwort), sondern auch Besitz (z.B. X.509-Zertifikat) nachgewiesen werden muss. Besonders hoch ist das Sicherheitsniveau bei Hardware-basierten Lösungen wie Generatoren für Einmalpasswörter (One-Time Passwords), Smart Cards oder USB-Token, bei denen ein Kopieren der Hardwarekomponente ausgeschlossen ist. Die Verwendung solcher Mechanismen ist einer einfachen Authentisierung mittels Passwort in jedem Fall vorzuziehen.
- ✔ Passwortsicherheit: Bei der Verwendung von Passwort-basierter Authentisierung ist eine Password-Policy erforderlich, welche ein Mindestniveau der Passwortqualität sicherstellt. Eine solche Policy muss durch die jeweilige Lösung zur Fernwartung umsetzbar sein (z.B. Verwendung von Sonderzeichen, Passwortlänge, etc.). Eine Fernwartungslösung sollte eine Password-Policy möglichst auch technisch forcieren können. Es sei explizit darauf hingewiesen, dass die Verwendung von alleinig Passwort-basierten Authentisierungsverfahren nicht mehr als einen Basisschutz bieten kann. In jedem Fall sind die zugehörigen organisatorischen Prozesse umzusetzen (siehe unten).
- ✔ Angriffserkennung: Wünschenswert wären Mechanismen zur Detektion von Angriffen auf Passwort-basierte Authentisierungsverfahren (z.B. Brute Force oder Dictionary Angriffe). Notwendig sind Vorkehrungen gegen das wiederholte Durchprobieren (Online Brute-Force), etwa durch Aktivierung einer temporären Sperre nach einer definierten Anzahl von Fehlversuchen. Anders als in der konventionellen IT sind mit Blick auf die besonderen Anforderungen hinsichtlich Verfügbarkeit und Safety solche Sperren aber beispielsweise erst nach 20 statt bereits nach drei Fehlversuchen vorzunehmen.

1 Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls in der Bundesverwaltung, https://www.bsi.bund.de/dok/6623850

2 BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

4 Organisatorische Anforderungen

Ein sicherer Fernzugriff kann niemals allein durch technische Maßnahmen gewährleistet werden. Daher sind die folgenden Anforderungen für die Integrations- und Betriebsphase unverzichtbar.

- ✔ Risikoanalyse: Es erfolgt eine formale Risikoanalyse der konzipierten Lösung.
- ✔ Minimalitätsprinzip: Es sind nur die unbedingt erforderlichen Fernzugriffsmöglichkeiten zu implementieren. Die Notwendigkeit eines Fernzugriffs ist durch den jeweiligen Verantwortlichen zu dokumentieren („business justification“).
- ✔ Prozesse: Beim Betreiber der Anlage werden Prozesse etabliert, welche beispielsweise die Freigabe von Verbindungen, Sperrungen (z.B. beim Ausscheiden von Mitarbeitern), Notfallprozeduren und den regelmäßigen Wechsel von Authentisierungsdaten regeln.
- ✔ Inventarisierung: Sämtliche Fernzugriffsmöglichkeiten werden im Rahmen eines Sicherheitsmanagements erfasst. Dies beinhaltet die Art des Zugangs, die betroffenen Systeme, die berechtigten Personen sowie die zugehörigen Vorgaben und Prozesse.
- ✔ Zeitfenster: Remote-Zugänge werden nur bei Bedarf oder in einem definierten Wartungsfenster freigegeben (z.B. Schlüsselschalter). Die Aktivierung bzw. Deaktivierung ist zu protokollieren.
- ✔ Funktionsprüfung: Es erfolgt eine regelmäßige Prüfung der Funktionsfähigkeit der Fernwartung.
- ✔ Vorgaben für Fernwartende: Insbesondere im Falle der Fernwartung durch Dritte (Hersteller, Integrator, etc.) werden Vorgaben für die verwendete IT (z.B. keine Smartphones) und Schutzmechanismen der Remote-Clients (z.B. aktueller Virenschutz, Firewall, Systemhärtung, aktueller Patchstand, etc.) getroffen. Diese Vorgaben werden vertraglich vereinbart.
- ✔ Patchprozess: Für funktionale Industriekomponenten (z.B. SPS) ist es häufig nicht möglich, Aktualisierungen und Patches einzuspielen. Da besonders Fernwartungskomponenten sehr exponiert sind, ist das zeitnahe Beheben bekannter Schwachstellen dort von zentraler Bedeutung für Sicherheitsaspekte. Da eine Fernwartungskomponente in der Regel keinen unmittelbaren zeitlichen Einfluss auf Aspekte wie Echtzeitfähigkeit oder Anlagenverfügbarkeit hat, sind solche Aktualisierungen im Rahmen eines definierten Patchprozesses auch meist möglich.
- ✔ Logging & Alerting: Es sind vorhandene Protokollierungsfunktionen zu nutzen, um beispielsweise Verbindungsdaten und auch fehlgeschlagene Anmeldeversuche nach zu halten. Es ist sicherzustellen, dass die Logdaten automatisiert ausgewertet werden und ggf. eine Alarmierung erfolgt. Darüber hinaus sollte periodisch eine manuelle Sichtung erfolgen. Zur Gewährleistung der Revisionssicherheit sollten die Logdaten unbedingt beim Betreiber gesammelt werden statt beim Fernwartenden.

5 Sonstiges

Abhängig vom konkreten Anwendungsfall können weitere Anforderungen sinnvoll sein. Da hierzu allgemeine Aussagen kaum möglich sind, sind hier einige Beispiele aufgeführt:

- ✔ Skalierbarkeit: Vorrangig in größeren Infrastrukturen können die Kosten für Betrieb, Wartung und Pflege durch ein zentrales Management, Bulk-Rollout, Bulk-Configuration oder Bulk-Actions, wie dem Ausführen von Skripten, stark gesenkt werden.
- ✔ Investitionsschutz: Durch Berücksichtigung von möglichen zukünftigen Anforderungen wie beispielsweise der Unterstützung von IPv6 ist eine Auswahl von Produkten mit Blick auf Investitionsschutz und Nachhaltigkeit sinnvoll.
- ✔ Hochverfügbarkeit: Sofern entsprechende Anforderungen bestehen, sind Funktionen zur Umsetzung von HV-Konzepten wie zum Beispiel der redundanten Verwendung mehrerer Mobilfunknetze für die Kommunikation mittels Dual SIM sinnvoll.

Je nach Anforderungen sowie der zu bewertenden Fernwartungslösung sind in einer individuellen Betrachtung weitere Kriterien zu prüfen. Beispielsweise sollten bei Cloud-basierten Pro-

dukten die entsprechenden Empfehlungen des BSI[3] beachtet werden. Insbesondere Public-Cloud-basierte Lösungen implizieren ein erhöhtes Sicherheitsrisiko, weshalb unter Sicherheitsaspekten eher eine Private-Cloud oder ein hinreichend vertrauenswürdiger Anbieter gewählt werden sollte.

Die zuvor beschriebenen Empfehlungen gelten für den verbreiteten Fall einer Fernwartung im Sinne eines Wartungsfalls, bei dem Veränderungen am System vorgenommen werden oder zumindest eine Interaktion erforderlich ist. Für einen rein passiven Fernzugriff – beispielsweise lediglich das Ablesen von Statusinformationen, Messwerten oder Systemzuständen. – bieten sich andere Lösungen an. So kann zum Beispiel das Entkoppeln der Informationen über einen Web- oder FTP-Server erfolgen, an den die Daten aus dem ICS-Netz heraus per Push-Verfahren geliefert werden und der selbst keine Verbindung dorthin aufbauen kann.

Einen vertiefenden Einblick zur Sicherheit von Fernwartung in der IT liefern die Grundregeln zur Absicherung von Fernwartungszugängen[4]. Weiterführende Informationen, insbesondere zu organisatorischen Regelungen, liefert der IT-Grundschutz[5] – insbesondere mit dem Baustein NET.3.3[6]. Zudem liefert die BSI-Veröffentlichung ISi-Fern ergänzende Informationen zu technischen und architekturbezogenen Fragen.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

3 Cloud Computing, BSI, https://www.bsi.bund.de/dok/6622408
4 Grundregeln zur Absicherung von Fernwartungszugängen, BSI / Allianz für Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de/dok/6649756
5 IT-Grundschutz, BSI, https://www.bsi.bund.de/grundschutz
6 https://www.bsi.bund.de/dok/10095792