Infrastruktur sicher schützen, aber wie?

Ende-zu-Ende-Verschlüsselung als optimale Lösung

Der Schutz der öffentlichen Infrastruktur gegen Cyber-Angriffe hat oberste Priorität und gehört zum Pflichtprogramm der Betreiber. Allerdings stellen sich hinsichtlich der Schutzmechanismen Viele die Frage, was verschlüsselt werden soll und was nicht. Dazu gibt es unterschiedliche Ansichten, die die Experten von Bachmann und Omicron anhand von Fallbeispielen erörtern.

Grundsätzlich gilt die Ende-zu-Ende-Verschlüsselung als optimale Lösung für alle Anwendungsfälle im Internet. Auf Steuerungssysteme übertragen bedeutet das, dass ausschließlich die unmittelbaren Kommunikationspartner, zum Beispiel ein intelligentes Gerät und das SCADA-System, gemeinsam einen Schlüssel „aushandeln". Somit bleibt auf der gesamten Übertragungsstrecke der Dateninhalt geheim; selbst beim direkten Zugriff auf Netzwerkkomponenten oder dem Mithören von (Mobil-)Funkübertragungen können Angreifer keine Informationen abgreifen.

Im OT-Bereich, also dort, wo IT-Mittel zu Produktionszwecken eingesetzt werden, ist der Einsatz von Verschlüsselungen differenzierter zu betrachten. Hier wird zwischen den Begriffen Authentication und Encryption unterschieden: Die Authentication stellt sicher, dass die Datenverbindung tatsächlich mit der erwarteten Gegenstelle aufgebaut wird. Erst die zusätzliche Encryption macht den Verkehr auch abhörsicher. Es stellt sich daher die Frage: Ist der Inhalt der Kommunikation vertraulich oder genügen Fälschungssicherheit und eindeutige Authentifizierung der Kommunikationsteilnehmer? Die folgenden beiden Anwendungsfälle zeigen, dass beide Lösungen ihre Berechtigung haben.

Anwendungsfall 1: Zugriff auf Daten einer Windturbine

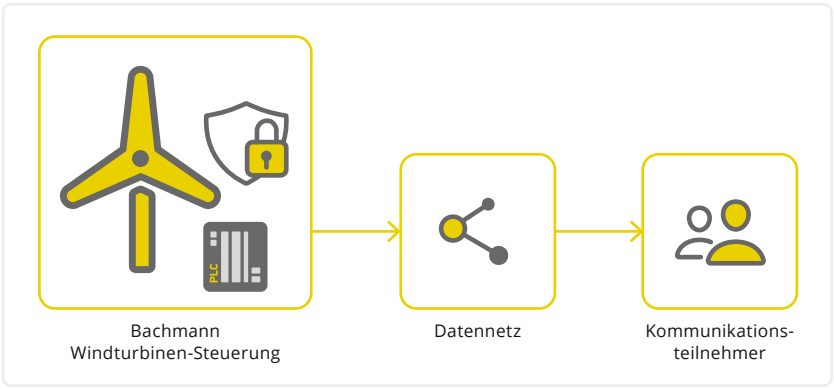

Bild 1: Ende-zu Ende-Verschlüsselung der externen Anlagenkommunikation mit der Bachmann-Steuerung

Zu Beginn der Windkraft-Industrialisierung war die Menge der erfassten Daten sehr gering und der Zugang war meistens nur für den Hersteller möglich. Inzwischen befinden sich in Windparks Turbinen verschiedener Hersteller im Einsatz. Bei Reparaturen beauftragen die Betreiber weitere, unabhängige und wechselnde Servicedienstleister. Diese benötigen Zugriff auf Betriebsstundenzähler und Störungsmeldungen. Teilweise betreffen Störungen unterschiedliche Fachbereiche für Anlagenschutz, Safety oder Einspeiserichtlinien, bei denen jeweils weiterführende Informationen erforderlich sind.

Gleichzeitig können räumlich weit entfernte Direktvermarkter und Energiebroker Zugriff auf die Erzeugungseinheit erhalten, um die verfügbaren Einspeisekapazitäten abzufragen und um Sollwertvorgaben sowie Fahrpläne für Blind- und Wirkleistung zu übergeben. Auch Abrechnungsdaten werden über diese Verbindung transferiert. Dieser Zugriff erfolgt in den meisten Fällen über das vorhandene Internet oder über Satellitenstrecken und muss entsprechend abgesichert werden.

Die SCADA-Schnittstellen der Erzeugungseinheiten sollten sich somit bei wechselnden Sicherheitsanforderungen einfach anpassen lassen. Das Hinzufügen und Entfernen von Usern, das Ändern der Zugriffsrechte oder das Sperren von nicht länger erwünschten Zertifikaten muss einfach im laufenden Betrieb möglich sein; die Änderungen müssen sich leicht ausrollen lassen.

Die MMS-Schnittstelle gemäß der Normenreihe DIN EN IEC 61850 (VDE 0160-850) [1] für die Steuerungsfamilie von Bachmann [2] ermöglicht die Absicherung der Kommunikation über TLS-Zertifikate. Dabei sind die Erkennung der Teilnehmer (Authentication) und der Verschlüsselung der Kommunikation (Encryption) getrennt konfigurierbar. Alle Einstellungen sind in einer XML-Datei zusammengefasst und können somit – vorausgesetzt, der User hat die Rechte – einfach im Windpark oder in der EZA auf viele Geräte verteilt werden (Bild 1). Ab diesem Zeitpunkt ist es nur noch erwarteten und vorgesehenen Teilnehmern möglich, Sollwerte und Schaltbefehle abzusetzen sowie Prozessdaten und Ereignisse „mitzuhören".

Bild 2:
Omicron-StationGuard für die Überwachung der internen Anlagenkommunikation

Anwendungsfall 2: Kommunikation in der Schutz- und Leittechnik

Welche Nachteile bringt nun eine Verschlüsselung mit sich? Oft wird hier als erstes die verzögerte Reaktions- und Übertragungszeit genannt. Mit Schutzrelais der neueren Gerätegenerationen liegen die Zeiten jedoch meist innerhalb des Anforderungsbereichs für die in der Meldung enthaltenen Signale.

Ein weiteres Problem ist die Analysefähigkeit: In der Schaltanlagenautomatisierung ist die Lesbarkeit des Datenverkehrs von großer Bedeutung. Das gilt insbesondere dann, wenn Betriebsstörungen nachträglich analysiert werden müssen. Verschlüsselte Netzwerkkommunikation macht eine Analyse allerdings unmöglich. Dies ist insbesondere bei GOOSE-Telegrammen ein Problem, da sie in Schutzauslösungen oft relevant sind.

Auch hinsichtlich der Sicherheit kann Verschlüsselung nachteilig sein: Weder Firewalls noch Angriffserkennungssysteme können verschlüsselte Kommunikation auf Bedrohungen hin analysieren. Es gäbe zwar theoretische Möglichkeiten, dass Sicherheitssysteme die Verschlüsselung öffnen können, diese würden aber im Schaltanlagen- und Steuerungsumfeld wiederum andere Risiken und Aufwände mit sich bringen.

Wird ein Angriffserkennungssystem (Intrusion Detection System) wie StationGuard von Omicron [3] zur Überwachung der Kommunikation innerhalb der Anlage eingesetzt (Bild 2), ergeben sich zahlreiche Vorteile für die Sicherheit sowie die Diagnose und Überwachung der Anlage: Einzelne Aktivitäten in der MMS-, GOOSE- und IEC 60870-5-104-Kommunikation (DIN EN 60870-5-104 [4]) können genau auseinandergehalten und beurteilt werden. Ebenso kann festgelegt werden, welche Geräte beispielsweise Schalthandlungen oder Konfigurationsänderungen durchführen dürfen und welche nicht. Hier kann StationGuard auch zwischen Wartungssituationen und dem Normalbetrieb unterscheiden.

Im Normalbetrieb der Anlage ist es beispielsweise nicht üblich, dass der Engineering-PC Schalthandlungen durchführt. Die Konfiguration von StationGuard ist einfach gehalten und kann durch das Importieren von SCL-Projektdateien (Substation Configuration Language) bzw. Anlagenbeschreibungen im CSV-Format zu großen Teilen automatisiert ablaufen. Aufgrund der detaillierten Überprüfung durch StationGuard werden nicht nur Bedrohungen für die Cyber-Sicherheit, wie manipulierte Pakete oder unzulässige Steuervorgänge, erkannt, sondern auch Kommunikationsfehler, Probleme mit der Zeitsynchronisation und damit auch möglicherweise bevorstehende Geräteausfälle.

Auf diese Weise lassen sich bereits bei der Erstinbetriebnahme von StationGuard verschiedene Security-Bedrohungen, aber auch Konfigurationsfehler in der Leit- und Netzwerktechnik auffinden. Omicron bietet solche Cyber-Security-Assessments für Energieversorger kostenlos an.

Fazit

Die Authentifizierung und Integritätssicherung bei MMS und GOOSE-Kommunikation ist in jedem Fall empfohlen. Mit den in der Normenreihe DIN EN IEC 62351 (VDE 0112-351) [5] beschriebenen Methoden kann sichergestellt werden, dass Absender und Empfänger die erwarteten Geräte sind, und dass die Nachrichten auf dem Kommunikationsweg nicht manipuliert wurden. Die Voraussetzung hierfür ist ein System zur Schlüssel- bzw. Zertifikatsverteilung, also ein weiterer Server im Anlagennetzwerk, der über kurz oder lang in allen Schaltanlagen, Umspann-, Kraft- und Steuerungsnetzwerken zur Verfügung stehen muss.

Die optional zuschaltbare Verschlüsselung ist dort sinnvoll, wo der Kommunikationsinhalt geheim gehalten werden muss. Dies ist beispielsweise bei vertraulichen Zählerinformationen der Fall, kann aber auch grundsätzlich notwendig sein, wenn die Kommunikation teilweise über einen öffentlichen Kanal wie ein Mobilfunknetzwerk (Stichwort: 5G) läuft. Hier empfiehlt es sich, eine Kanalverschlüsselung am Übergang zwischen privatem und öffentlichem Kanal zu schalten. Damit lassen sich die Nachteile der Verschlüsselung im privaten Netz vermeiden und trotzdem das Mithören auf dem öffentlichen Kanal verhindern.

AUTOREN

Helmut Ritter
Product Line Manager Kommunikation und Vernetzung
Bachmann Electronic GmbH in Feldkirch/Österreich

Andreas Klien
Business Area Manager Power Utility Communication
Omicrons Electronics GmbH in Klaus/Österreich

Details zur Security-Normenreihe

Die Security-Normenreihe DIN EN IEC 62351 fordert die Anwendung von sicheren Transportprotokollen mittels krypto- grafischer Methoden auf allen Schalt-, Schutz-, Mess- und Steuergeräten. An der Authentifizierung der Kommunikationsteilnehmer mittels kryptografischer Zertifikate und Nachrichtensignaturen führt kein Weg vorbei. Eine zusätzliche Verschlüsselung der Kommunikation ist in der Norm jedoch optional und hängt vom Anwendungsfall ab.

Einen technischen Lösungsvorschlag unterbreitet die Normenreihe mit Transport Layer Security (TLS) in Version 1.2, die eine Verwendung von TLS mit Integritätsprüfung, jedoch ohne Verschlüsselung erlaubt. Im aktuellen Protokoll TLS 1.3 ist dies grundsätzlich nicht mehr möglich, in der Internet Engineering Task Force (IETF) gibt es jedoch eine Initiative (RFC 9150), die solche „integrity-only cypher suites“ auch für den Nachfolger TLS 1.3 ermöglicht.

MEHR ERFAHREN:

Fernwirkprotokolle

KONTAKT

Helmut Ritter
Product Line Manager Kommunikation und Vernetzung

info@bachmann.info

bachmann.

www.bachmann.info

© 11/2022 by Bachmann electronic | Technische Änderungen vorbehalten