SIEMENS

White Paper

Schutz industrieller Steuerungen

Herausforderung und praktische Lösungen

Im Zuge der fortschreitenden Verbindung von Operational-Technology-Netzwerken (OT) mit klassischen Information-Technology-Netzwerke (IT) stellen Betreiber industrieller Steuerungssysteme (Industrial Control Systems – ICS) in zahlreichen Branchen ihre Netzwerke zunehmend von serieller Kommunikation auf IP-basierte Kommunikation um, was deutliche Vorteile wie verbesserte Leistung, Zuverlässigkeit und Effizienz mit sich bringt.

Die Konvergenz von OT und IT birgt allerdings auch neue Herausforderungen und Risiken für die Steuerungen selbst. Da ein ICS konkrete technische Abläufe in der realen Welt überwacht und steuert, unterliegt es strengeren Anforderungen hinsichtlich der Deterministik und Echtzeit- Datenübertragung.

Deterministik beschreibt einen bekannten, messbaren Parameter für die Geschwindigkeit und Zuverlässigkeit der Signale im Netzwerk. Ein ICS fordert in diesem Zusammenhang eine extrem niedrige Latenz bei Antwortzeiten und eine extrem niedrige Varianz für diese Antwortzeiten (sprich niedrige „Jitter"-Werte),die bei Null oder nahe Null liegen. Je nach der Branche, in der ein ICS eingesetzt wird, sind in OT-Netzwerken daher andere Aspekte hinsichtlich der Dienstgüte (QoS) als bei IT-Netzwerken zu beachten.

Bisher waren herkömmliche ICS völlig abgeschottete Systeme und damit vor netzwerkbasierten Bedrohungen geschützt.
Die verstärkte Umstellung von seriellen auf IP-basierte Netzwerke bringt jedoch potentielle Schwachstellen und Risiken für industrielle Steuerungen mit sich, sowohl in der verarbeitenden Industrie als auch in den Branchen mit kritischen Infrastrukturen, wie Energieerzeugung und Stromnetze, Transportwesen und moderne Verkehrsleittechnik.

Die industriellen Steuerungen in diesen Bereichen sind in zunehmendem Maße durch Cyberangriffe gefährdet, mit möglicherweise verheerenden Folgen für Marken, Unternehmen und die öffentliche Sicherheit.Die Planung und Inbetriebnahme vieler heutiger Industrieanlagen und Steuerungen fanden zu einer Zeit statt, in der die Notwendigkeit zahlreicher Sicherheitsmaßnahmen noch nicht existierte, die heutzutage aber bereits zum Standard von IT-Netzwerken gehören.

Dazu gehören u. a. Zugangsrichtlinien und entsprechende Maßnahmen, um diese durchzusetzen, Autorisierungs- und Authentifizierungsverfahren, Richtlinien zur Vereinfachung des Änderungswesens sowie Aktivitäts- oder Auditprotokolle, die forensische Untersuchungen bei Sicherheitsverletzungen ermöglichen.

Potentielle Ausworkungen

Ein Einbruch in das IT-Netzwerk eines Unternehmens kann das operative Tagesgeschäft massiv beeinträchtigen. Beispiele hierfür sind Diebstahl von geistigem Eigentum oder Kundendaten, oder auch das Blockieren der öffentlich zugänglichen Website eines Unternehmens. Demgegenüber kann ein Angriff auf ein ICS zu einem Produktionsausfall, Schäden an Anlagen und Infrastruktur oder sogar zu Gefahren für Leib und Leben von Mitarbeitern oder der Allgemeinheit führen. Diese potentiellen Auswirkungen verstärken sich um ein Vielfaches, wenn kritische Infrastrukturen angegriffen werden.

Cyberattacken nehmen zu

Laut einer Studie von Booz Allen Hamilton aus dem Jahr 2016 (“Industrial Cybersecurity Threats are on the Rise”) nehmen Cyberangriffe auf Steuerungssysteme zu und werden wahrscheinlich auch weiterhin zunehmen.

Diese Studie referenziert auf öffentlich zugängliche Daten von 314 Organisationen weltweit, wobei 34 Prozent der ICS-Betreiber von mehr als zwei Einbrüchen in ihre Systeme während der vorangegangenen zwölf Monate berichteten. In 44 Prozent der Fälle konnte die Quelle nicht identifiziert werden.

In einem auf den Energiesektor bezogenen Artikel von 2016 aus dem U.S. News & World Report (“Cyberattacks Surge on Energy Companies, Electric Grid”) meldeten 150 Energie- und Stromversorgungsunternehmen erfolgreiche Angriffe auf ihre Netzwerke in den letzten zwölf Monaten, und nahezu die Hälfte gab an, dass die Angriffe in letzter Zeit häufiger geworden seien. Über 80 Prozent gingen davon aus, dass im kommenden Jahr physische Schäden an Einrichtungen zu erwarten seien. „Angreifer konnten eine oder auch mehrere Firewalls, Antivirenprogramme und andere Schutzvorkehrungen überwinden“, wie das Magazin berichtete.

Ein Analyst bei SecurityWeek nannte kürzlich die drei größten Bedrohungen für industrielle Steuerungssysteme (“The Top 3 Threats to Industrial Control Systems”): 1. äußere Bedrohungen durch Staaten, Terroristen oder Hacker, 2. innere Bedrohungen durch unzufriedene Mitarbeiter und 3. menschliches Versagen – vielleicht die häufigste und gefährlichste Bedrohung überhaupt.

Was bedeutet das für Ihr Unternehmen?

Cyberangriffe auf industrielle Steuerungssysteme sind mittlerweile fester Bestandteil des Geschäftslebens. Nach Ansicht zahlreicher Experten muss diesen Bedrohungen mit gesundem Menschenverstand und den aktuell bekannten Methoden begegnet werden – denn ein Cyberangriff auf Ihr Unternehmen ist keine Frage des „Ob“, sondern des „Wann“.

Laut einem Trendbericht von Mandiant bleiben Hacker oder Malware durchschnittlich 101 Tage unentdeckt. wobei es einige weitere Tage dauert, bis ein solcher Angriff abgewehrt wurde. Rund 38 Prozent der betroffenen Unternehmen erfuhren erst von einer externen Stelle wie dem Justizministerium, dem Bundesamt für Sicherheit in der Informationstechnik oder einer anderen nationalen Sicherheitsbehörde von dem Angriff.

Natürlich lassen sich nicht alle diese Bedrohungen ausschalten, vor allem angesichts der Tatsache, dass der Faktor Mensch eine Hauptfehlerquelle darstellt und böswillige Attacken immer ausgefeilter werden und immer häufiger auftreten. Allerdings können wirksame Strategien – gestützt durch erprobte Sicherheitsmaßnahmen – dazu beitragen, menschliches Fehlverhalten zu vermeiden, schädliche Attacken zu erkennen und zu isolieren, deren Auswirkungen zu minimieren und ICS widerstandsfähiger gegen Cyberangriffe zu machen.

Ein gemeinsames Anliegen

Für ICS verantwortliche Führungskräfte und Manager führen oft an, ihre größte Sorge sei die fehlende Kenntnis der Teilnehmer und der Abläufe in ihren Netzwerken. Ähnliche Bedenken äußern sie hinsichtlich unbeabsichtigter oder vorsätzlicher Verstöße gegen die Netzwerksicherheit, Problemen mit der Einhaltung gesetzlicher Bestimmungen und der Gesamtverantwortung für die Sicherheit der Steuerungen.

Glücklicherweise können gut eingeführte Strategien, bewährte Technologien und ein zuverlässiger Beratungspartner, der über langjährige Erfahrungen im Aufbau, Betrieb und Schutz von ICS verfügt, diese und andere Bedenken zerstreuen.

Defense in Depth – Tiefengestaffelte Verteidigung

Auf begrifflicher Ebene weisen Experten auf den bedeutsamen Unterschied zwischen Compliance und Security hin. Compliance lässt sich definieren als Konformität mit Regelwerken und Normen, nachgewiesen durch ein Audit, womit eine Untersuchung oder Überprüfung durch Dritte oder eine Behörde gemeint ist.

Demgegenüber gilt Security als Umsetzung technischer und administrativer Maßnahmen sowie von Kontrollmechanismen zur Gewährleistung von Geheimhaltung, Systemintegrität und Verfügbarkeit. In diesem Kontext können die administrativen Maßnahmen auch Rechenschaftspflichten und Verantwortungszuweisung beinhalten. Einfacher ausgedrückt: „Compliance" ist nicht gleich „Security". Compliance stellt lediglich eine Momentaufnahme dessen dar, ob bzw. wie Schutzprogramme bestimmte Sicherheitsanforderungen erfüllen, die von Aufsichtsstellen zu einem bestimmten Zeitpunkt festgelegt wurden. Security dagegen ist wesentlich breiter angelegt und erfordert neben Compliance und der Abarbeitung von Checklisten mit Aktionen und Maßnahmen eine ganzheitliche Herangehensweise auf mehreren Ebenen.

Das in der Praxis bewährte Konzept „Defense in Depth" bietet Schutz auf mehreren Ebenen, um menschliches Fehlverhalten und böswillige Eingriffe aufzudecken, zu verhindern oder deren Folgen einzudämmen. Eine tiefengestaffelte Verteidigung zum Schutz von ICS stützt sich auf das Prinzip, nach dem ein Angriff allmählich an Wucht verliert. Diese Strategie kann Schutz gegen die häufigsten Angriffe oder gegen menschliches Fehlverhalten bieten, aber auch gezielte, ausgefeilte Angriffe zumindest so lange aufhalten bis Gegenmaßnahmen zur Eindämmung des Risikos eingeleitet werden können.
Als hilfreiche Analogie können Vorkehrungen und Maßnahmen beim Einbruchsschutz dienen, die Menschen zum Schutz ihres Eigenheims vornehmen. Zunächst wird die Haustür verschlossen; aber diese einzelne, rein mechanische Maßnahme reicht oftmals nicht aus, um einen Einbruch zu verhindern. Erweitert wird die Sicherung des Hauses durch mehrere Schutzebenen, die ein Eindringen erschweren, so dass genug Zeit bleibt, den Einbruch zu erkennen und zu stoppen. Bewegungsmelder, ein bellender Hund und eine Alarmanlage, die der Polizei den Einbruch meldet, tragen zur Abwehr verschiedener Gefahren und zur Risikominimierung bei.

Um die zahlreichen Angriffsvarianten auf ein ICS abzuwehren, erfordert eine Defense in Depth-Strategie Maßnahmen für die Anlagensicherheit (wie physischen Zutrittsschutz, Prozesse und Richtlinien, ganzheitliche Überwachung), Netzwerksicherheit (wie Zellenschutz, Schutz des Perimeternetzwerks, Firewalls, VPN) sowie Systemintegrität (wie Systemhärtung, Patch-Management, Erkennung von Angriffen, Authentifizierung und Zugriffsschutz).

Die meisten Unternehmen implementieren zwar Gegenmaßnahmen für mindestens eine Angriffsvariante, doch reichen solche Maßnahmen in der Regel nicht aus, um allen Angriffen in einer ganzheitlichen Strategie angemessen entgegenzutreten. Einzelmaßnahmen wie Kennwörter oder Firewalls allein können also den Bedrohungen der Cybersicherheit nicht standhalten. Stattdessen kann die tiefengestaffelte Verteidigung durch Einrichten von Verfahren und Technologien auf allen diesen Ebenen gegebenenfalls Ausfallzeiten minimieren und potentielle Gefahren durch Cyberattacken abwehren.

Der Trusted Advisor

Aufgrund der umfassenden Erfahrung, die zur Umsetzung der zahlreichen Sicherheitsmaßnahmen einer tiefengestaffelten Verteidigung erforderlich ist, stellen sich nur wenige Unternehmen der Thematik Cybersicherheit im Alleingang. Ein zuverlässiger Beratungspartner (Trusted Advisor) sollte sich zunächst über die vom Unternehmen bereits umgesetzten Maßnahmen zur Cybersicherheit informieren und diese analysieren, bevor er mögliche Lösungen für noch bestehende Schwachstellen im Konzept aufzeigt.
Entwurf und Implementierung von Lösungen auf jeder Ebene der Defense in Depth-Strategie erfordern in der Regel einen Trusted Advisor mit langjähriger Erfahrung im Bereich Industriesteuerungen sowie Fachkompetenz in den Applikationen im industriellen Umfeld, ICS sowie spezifische Branchenkenntnisse. Erfahrung und Fachkompetenz sollten durch gutes Sicherheits-Know-how, robuste Softwarelösungen und zuverlässige, industrietaugliche Hardware untermauert sein.

Eine Liste der Industriezweige, die den Cyber-Bedrohungen begegnen müssen, unterstreicht die Bedeutung der Wahl eines zuverlässigen Beratungspartners, der über ein breites Erfahrungsspektrum, umfassendes Fachwissen und ein Portfolio von Lösungen zur Implementierung von „Defense in Depth" in ICS verfügt. Diese Liste umfasst Branchen wie Fertigung, Nahrungs- und Genussmittel, Pharma, Wasser und Abwasser, Energie und Versorgung, Transport und Logistik, Anlagen zur Nutzung erneuerbarer Energien, Öl und Gas, Pipelines und Raffinerien, Schienenverkehr und intelligente Verkehrssysteme.

In einem umkämpften Markt voller „Lösungen" genügt es nicht, seine Informationen ausschließlich von Anbietern mit IT-Kenntnissen zu beziehen, die sich das relevante Industrie-Know-how zum Schutz von ICS-Netzwerken gerade erst aneignen. Und auch eine simple Investition in Hardware ohne eine übergreifende Strategie zur Cybersicherheit mit entsprechenden Softwarelösungen, die auf dieser Hardware ausgeführt werden können, werden den Anforderungen nicht gerecht.

Ein bewährter Lösungsanbieter und Partner in der Cybersicherheit sollte vielmehr über langjährige Erfahrung in Herstellung, Implementierung und Diagnostik von Applikationen im industriellen Umfeld und in den relevanten Branchen verfügen.

Abbildung 1

Drei Ebenen und Lösungen

Abbildung 1 veranschaulicht die drei Ebenen der ganzheitlichen Defense in Depth-Strategie. Keine einzelne Ebene ist wichtiger als die jeweils anderen; vielmehr tragen alle gemeinsam zum ganzheitlichen Schutz bei. Abbildung 1 verdeutlicht, wie die verschiedenen Ebenen zusammenwirken und das durchgängige Schutzkonzept bilden.

Die zu schützenden Anlagen und Daten sitzen im Kern. Hierbei wird durch Zugriffskontrolle sichergestellt, dass nur befugte Personen mit den entsprechenden Berechtigungen mit dieser Ebene am rechten Ort und zur rechten Zeit interagieren können. Lösungen müssen bewährt, skalierbar und intuitiv für den Endbenutzer sein und dabei die nationalen und globalen Anforderungen und Standards für Industrial Cybersecurity einschließlich Verschlüsselungsstandards erfüllen.

Anlagensicherheit

Die Anlagensicherheit arbeitet Hand in Hand mit der Cybersicherheit. Sie beginnt mit dem herkömmlichen Gebäudezutritt und reicht bis zur Sicherung sensibler Bereiche mittels Codekarten, Sperren und Überwachungskameras. Die Anlagensicherheit umfasst Prozesse und Richtlinien für einen umfassenden Anlagenschutz. Hierzu zählen etwa die Risikoanalyse über die Umsetzung geeigneter Maßnahmen und deren Überwachung bis hin zu regelmäßigen Updates.

Netzwerksicherheit

Die Netzwerkebene muss durch Firewalls, Virtuelle Private Netzwerke (VPN) und Angriffserkennungssysteme gesichert werden, die mit weiteren Elementen der Defense in Depth-Strategie interagieren. Über Firewalls wird der Netzwerkverkehr gemäß den Sicherheitsregeln überwacht und kontrolliert. Ein VPN verschlüsselt die Datenübertragung zwischen Teilnehmern in einem Netzwerk.

Systemintegrität

Die Sicherung der Integrität Ihres ICS ist sowohl zum Schutz des bestehenden Know-how als auch vor unautorisiertem Zugriff auf Ihre Automatisierungsprozesse unerlässlich. Dem Schutz von Firmware und System-/Hostsoftware kommt eine Schlüsselrolle bei der Aufrechterhaltung der Systemintegrität zu. Erreicht wird dies durch Systemhärtung, regelmäßiges Patch-Management und weiteren Methoden zum Integritätsschutz.

Vielleicht spielt der Faktor Mensch, der an Implementierung, Wartung und Betrieb dieser Systeme beteiligt ist, die wichtigste Rolle bei einer tiefengestaffelten Verteidigung. Fachgerechte Schulungen vermitteln das Bewusstsein für geeignete Maßnahmen und Richtlinien zur Sicherheit in der Belegschaft und bereiten die Mitarbeiter auf die zunehmenden Cyberbedrohungen vor.

Profundes Know-how von Siemens im Bereich ICS-Cybersicherheit

Betriebsverfahren und Industrieautomatisierung – und somit auch Industrielle Steuerungssysteme – sind seit jeher die Stärke von Siemens. Dazu gehören auch profunde Kenntnisse über Cybersicherheit und die jeweiligen Branchen. In der Palette bewährter Lösungen und Services zur Cybersicherheit findet sich für jede Ebene der Defense-in-Depth-Strategie die passende Lösung. Unsere Expertenteams analysieren ICS-Sicherheitslücken, entwerfen maßgeschneiderte Lösungen für den Aufbau eines Verteidigungsrings und kümmern sich auch um deren Umsetzung.

Das Alleinstellungsmerkmal von Siemens liegt in der langjährigen Erfahrung beim Schutz von ICS-Netzwerken und der Unterstützung seiner softwarebasierten Lösungen, kombiniert mit der für Industrieumgebungen entwickelten Hardware. Hierdurch setzt sich Siemens von neueren Marktteilnehmern und deren IT-basierten Angeboten ab.

So bilden die von Siemens angebotenen Tools für Anlageninventur und Anlagenverwaltung eine Lösung für problembewusste ICS-Manager, die genau wissen möchten, welche Geräte in ihrem Netzwerk betrieben werden. Zudem bietet Siemens kompetente Hilfestellung, wenn es um End-to-End-Cybersicherheit geht, und fungiert als Mentor hinsichtlich der Einhaltung gesetzlicher Vorschriften. Falls die stets vorhandene Möglichkeit menschlichen Fehlverhaltens – oder böswilliger Angriffe – Bedenken in Sachen Cybersicherheit auslösen, hält Siemens Lösungen zur Authentifizierung, zum Kennwortmanagement und zur Angriffserkennung bereit, um diese Sicherheitslücken zu schließen.

Im Dialog bleiben

Ihr Ansatz in Sachen Cybersicherheit und ICS basiert vielleicht schon heute auf dem Know-how und der Erfahrung von Siemens mit dem Defense-in-Depth-Konzept und stützt sich auf unsere bewährten Strategien, unsere Software und unsere Hardwareplattformen für die Industrie. Oder aber Sie befassen sich gerade zum ersten Mal mit ICS-Cybersicherheit. In beiden Fällen sollte der Dialog mit einem Trusted Advisor zum Thema Industrial Security ganz oben auf Ihrer Agenda stehen.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit **http://www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

PDF
WhitePaper
BR 0818 / 5 En
Produced in Germany