Strategien um Industrielle Steuerungssysteme vor Cyberattacken zu schützen

Distributor

tug.at

geautomation.com

Einführung

Cyberattacken auf Infrastruktursysteme kommen immer häufiger vor. Für viele Betriebe mit industriellen Steuerungssystemen (ICSs) stellt sich nicht mehr die Frage, ob ein Cyberangriff auf sie zukommen könnte, sondern nur mehr wann das der Fall sein könnte.

Nach Statistiken des United States Department of Homeland Security (DHS) gab es im Jahr 2015 295 Vorfälle, die dem Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) gemeldet wurden, wobei man davon ausgehen muss, dass viele Vorfälle nicht gemeldet wurden.

Die Cyberattacke auf das ukrainische Energieversorgungsnetz am 23. Dezember 2015 gilt als der erste erfolgreiche Angriff auf ein Hochspannungsnetz. Während dieses Vorfalls ist es Hackern erfolgreich gelungen, Informationssysteme von drei ukrainischen Energieversorgungsunternehmen zu beeinträchtigen und die Stromversorgung bis zu den Endverbrauchern zeitweise lahm zu legen. Das resultierte in einem Verlust von Milliarden von Euros.

Der Umfang, die Häufigkeit und die Schwere von Cyberattacken auf kritische Infrastruktur nehmen zu, da sich auch Steuerungssysteme weiterentwickeln und zunehmend mehr vernetzt sind. Das bisherige Vorgehen um industrielle Steuerungsnetzwerke zu schützen, entweder durch physische Sperren an Kontrollräumen und Schaltschränken, oder durch den Aufbau von Steuerungsnetzwerken mit stärkerem Zugriffschutz durch physische Trennung der Steuerungssysteme und äußerer Kommunikations-Infrastruktur ist nicht länger ausreichend.

Neueste gekoppelte Steuerungssysteme, wie GE´s Industrial Internet Control System (IICS) können Informationen rund um den Globus austauschen. Diese Industrial Internet Systeme erfordern umfassende Cyber Security Ressourcen um mit den sich immer weiter entwickelnden Cyber Security Bedrohungen mithalten zu können.

In dieser Broschüre werden Sie mehr über die sieben Strategien, zusammengefasst unter DHS erfahren, um zukünftig auftretenden Schwächen bei industriellen Kontrollsystemen entgegen wirken zu können. Außerdem wird in dieser Broschüre auf GE´s Defense-In-Depth Ansatz zu Cyber Security eingegangen, der es erlaubt, Cyber-Verteidigungs-Fähigkeiten bei jeder Produktausführung einzusetzen und wie das helfen kann, Benutzer von Industrial Control Systemen zu schützen.

Sieben Strategien um Industrial Internet Control zu schützen

Nach Berichten des Department of Homeland Security hätten 98 Prozent der Vorfälle, die an das ICS-CERT in den Jahren 2014 und 2015 gemeldet wurden, vermieden werden können, wenn sich die Anwender an die folgenden sieben Strategien gehalten hätten. Die verbleibenden zwei Prozent hätten mit einer besseren Überwachung identifiziert werden können. Die sieben Strategien sind:

1. Angewandtes Application Whitelisting
Application Whitelisting (AWL) kann den Versuch und die Ausführung von Hackern, Schadprogramme hochzuladen, erkennen und vorbeugen. Die Statik mancher Systeme, wie Database Server und Human-Machine-Interface (HMI) Computern, macht sie ideal um AWL auszuführen. Betreiber sollen dazu animiert werden, mit Anbietern zusammenzuarbeiten, um den AWL Einsatz messen zu können.

2. Stellen Sie sicher, dass Konfigurations-patch-Management korrekt ausgeführt wird
Das Ziel von Hackern sind ungepatchte Systeme. Ein Configuration/Patch Management Programm, dessen Ziel die sichere Einführung und Implementierung von zuverlässigen Patches ist, kann helfen, Kontrollsysteme sicherer zu machen.

3. Reduzieren Sie Angriffsflächen, die attackiert werden könnten
Trennen Sie ICS Netzwerke von allen unsicheren Netzwerken. Versperren Sie alle ungenützten Eingänge. Schalten Sie alle nicht genutzten Services aus. Erlauben Sie nur Echtzeit Verbindung mit externen Netzwerken, wenn es bestimmte Geschäftsvorgaben oder Kontrollfunktionen gibt.

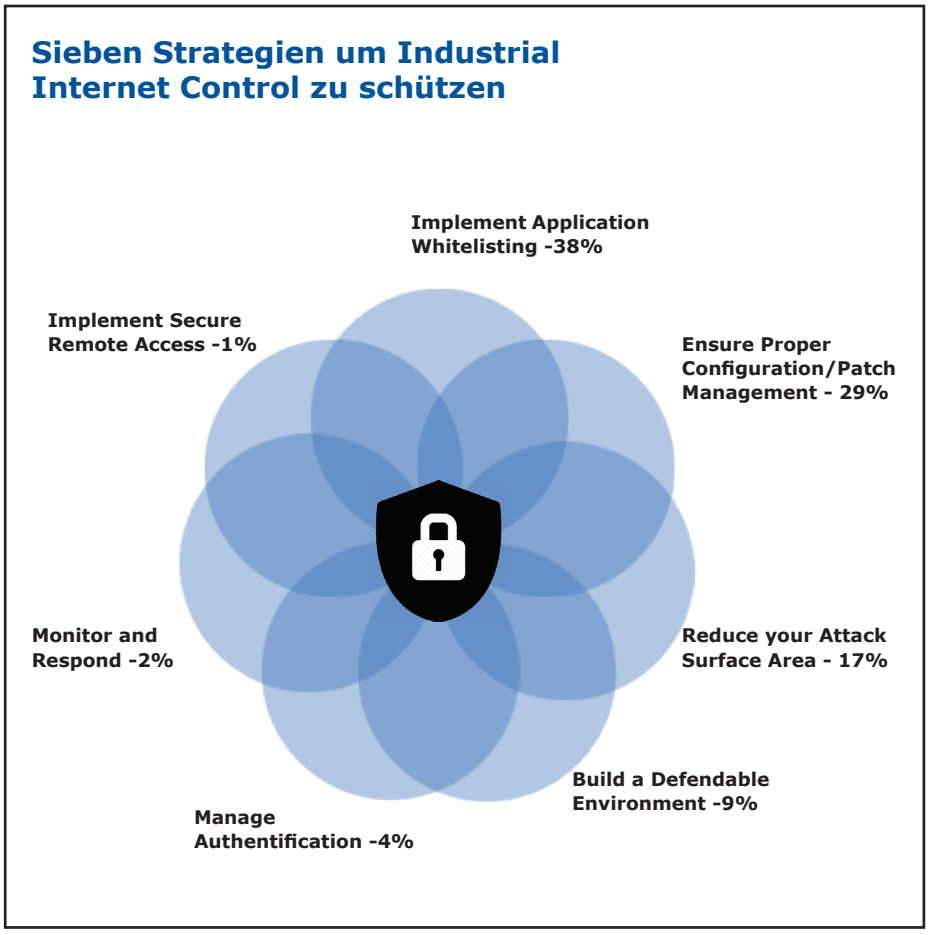
4. Schaffen Sie ein zu verteidigendes Umfeld
Vermindern Sie Schäden durch Netzwerk Perimeter Lücken. Unterteilen Sie Netzwerke in logische Segmente und schränken Sie host-to-host Kommunikationspfade ein. Das kann Hacker vom Ausweiten ihres Zugriffes abhalten, während die normale Systemkommunikation weiterlaufen kann.

5. Regeln Sie Authentifizierungen
Hacker sind zunehmend auf das Erlangen von Kontrolle von rechtmäßigen Zertifikaten fokussiert, vor allem an solchen Accounts, die mit großen Berechtigungen ausgestattet sind. Das Kompromittieren solcher Zertifikate erlaubt es Hackern, sich als normale Benutzer auszugeben und so hinterlassen sie weniger Spuren und können Schwachstellen ausnutzen oder Schadprogramme ausführen. Authentifizierungen so zu regeln, dass Benutzer nur solche Rechte haben, die sie auch wirklich benötigen, vermindert diese Gefahren.

6. Regeln Sie den sicheren Fernzugriff
Manche Hacker erlangen erfolgreich Zugang zu Kontrollsystemen, in dem sie verworrene Zugangsvektoren finden, sozusagen versteckte Hintertüren, die unabsichtlich von den Systemanwendern geschaffen wurden. Entfernen Sie solche Verbindungen wo immer es möglich ist - vor allem bei Modems, da diese grundsätzlich als unsicher gelten. Wenn Sie alle verbleibenden Zugänge limitieren und sichern, vermindern sich auch die Gefahren.

7. Überwachung und Rückmeldung
Soll ein Netzwerk gegen moderne Bedrohungen verteidigt werden, ist aktive Überwachung im Fall von feindlichem Eindringen und das schnelle Ausführen einer vorbereiteten Rückantwort erforderlich. Machen Sie einen Plan, wie Sie im Fall von feindlicher Aktivität vorgehen wollen. Dieser Plan sollte das Trennen aller Internetverbindungen, die genaue Suche nach Schadprogrammen, das Sperren von betroffenen Benutzerkonten, die Isolation verdächtiger Systeme und einen sofortigen Austausch aller Passwörter beinhalten. Außerdem sollte dieser Plan Eskalationsauslöser und Aktionen definieren und auch eine Rückmeldung zu Vorfällen, eine genaue Untersuchung und PR Aktivitäten beinhalten. Machen Sie einen Plan zur Wiederherstellung, der das schnelle Wiederverwenden des Systems auf dem letzten Stand ermöglicht.

Erfahren Sie mehr über diese Strategien unter diesem Link:
https://ics-cert.us-cert.gov/



GE’s Vorgehen zum Thema Cyber Security

GE ist engagiert, sichere und zuverlässige Produkte zu entwickeln und will helfen, sich Attacken energisch in den Weg zu stellen. GE nutzt ein Defense-In-Depth Vorgehen, das es erlaubt, Cyber-Verteidigungs-Fähigkeiten bei jeder Produktausführung einzusetzen. Der weitere Text soll verdeutlichen, wie GEs Defense-in-Depth Ansatz die sieben Strategien, definiert vom Department of Homeland Security, zur Verteidigung von industriellen Internet Kontrollsystemen umsetzt.

Schaffen Sie ein zu verteidigendes Umfeld:

Um Anwendern zu helfen, böswilligen Zugang zu ihrem System einzuschränken und ihnen zu zeigen, wie sie ein segmentiertes Kontrollnetzwerk erstellen, bietet GE Secure Deployment Guides zu jedem Produkt an. Diese Guides skizzieren kommende Entwicklungen im Sicherheitsbereich und beinhalten Firewalls und Segmentierung, um ungebetenen eintreffenden Verkehr zu blocken und Netzwerke isolieren zu können, um den Datentransfer auf Geräte zu begrenzen, die auch wirklich verwendet werden. Industrie Router können angewendet werden, um Datentransaktionen zwischen diesen isolierten Netzwerken durchzuführen. Alle Secure Deployment Guides bieten Muster Checklisten um Kunden durch diesen Prozess zu helfen:

• Legen Sie ein Netzwerk Diagramm an.

• Identifizieren und zeichnen Sie benötigte Kommunikationspfade zwischen Knotenpunkten auf.

• Identifizieren und zeichnen Sie benötigte Protokolle für jeden Pfad auf, in denen Sie die Rolle eines jeden Knotenpunktes einfügen.

• Ändern Sie Ihr Netzwerk, sodass es Ihren Anforderungen entspricht, um genaue Partitionierung sicherzustellen, indem Sie Firewalls oder andere Netzwerksicherheitsmaßnahmen hinzufügen. Halten Sie das Netzwerk Diagramm auf dem neuesten Stand!

• Konfigurieren Sie Firewalls und andere Methoden, um Ihr Netzwerk sicherer zu machen.

• Verwenden und/oder konfigurieren Sie die entsprechenden Sicherheits-Features bei jedem GE Produkt.

• Ändern Sie bei jedem Ihrer GE Produkte das voreingestellte Passwort.

• Überdenken Sie die Konfiguration Ihrer GE Produkte, schalten Sie ungenutzte Features, Protokolle und Ports aus.

• Testen, auditieren und qualifizieren Sie das System.

• Erstellen Sie einen Update-Instandhaltungsplan.

Mit diesen Informationen will GE seinen Kunden dabei helfen, ihre Kontrollnetzwerke sicherer zu machen. Zusätzlich beobachtet und adaptiert GE aktiv die Entwicklung von Cyber Security Bedrohungen. GE bietet seinen Kunden ein Center, das 24 Stunden täglich erreichbar ist, das Cyber Aktivitäten beobachtet und falls nötig adaptiert. Außerdem bietet GE viele Cyber Security Ressourcen an.

GEs Automation & Controls Security Webseite:
http://www.geautomation.com/security

Auf dieser Webseite finden Sie weiterführende Links zu:

• GE Product Security Ratgeber

• GE Security Ratgeber Auto-Notification Service

• Third-Party Patch Validation

• Entwicklung von Sicherheitsanforderungen

• Produkt-Anfälligkeit und Sicherheits/ Risiken Reporting

– Email security@ge.com

Vermindern Sie Ihre Angriffsfläche

Cyber Security beginnt bei Kommunikationsverbindungen zwischen den Geräten. Bei GE Control Produkten werden nicht notwendige Ports und Protokolle nicht unterstützt. Station Manager, USB und SD card Ports sind standardmäßig deaktiviert. Zugang zu den Geräten wird auf das beschränkt, was für die unterstützten Kommunikations Protokolle notwendig ist: HTTP Proxy wird unterstützt, für kontrollierten Internetzugang, HTTPS Protokolle mit Zertifikaten für sichere Predix Verbindung zum WAN. Außerdem haben wir ein privates Mobilfunknetzwerk für unsere Field Agent Produkte aufgebaut.

GE reduziert die Angriffsfläche seiner Produkte, indem Zugang zu wesentlichen Ports und Services limitiert wird. GE bietet außerdem Cyber Security Zertifikate für IICS Produkte an. Entweder die allgemein anerkannte Achilles Level 2 Zertifizierung oder die China spezifische TRIMPS Zertifizierung besagen, dass GE Kontrollsysteme weltweiten Security Standards entsprechen.

Achilles Test

Die Wurldtech Achilles Zertifizierung ist ein Kommunikationstest, ausgeführt an Geräten, während bestimmte Leistungsindikatoren überwacht werden. Der Achilles Test ist in drei Hauptgruppen unterteilt:

Achilles Grammar

– Achilles Grammar testet Protokoll Grenzbedingungen in der Systemkommunikation. Es wird systematisch jedes Feld und jede Feldkombination wiederholt, um reproduzierbar und quantifizierbar gängige Implementierungsfehler zu testen. Achilles Grammar sendet ungültige, schädliche oder unvorhergesehene Pakete an das Device under Test (DUT), um Anfälligkeiten in spezifischen Abschnitten des Protokollblocks zu erkennen.

Achilles Storms

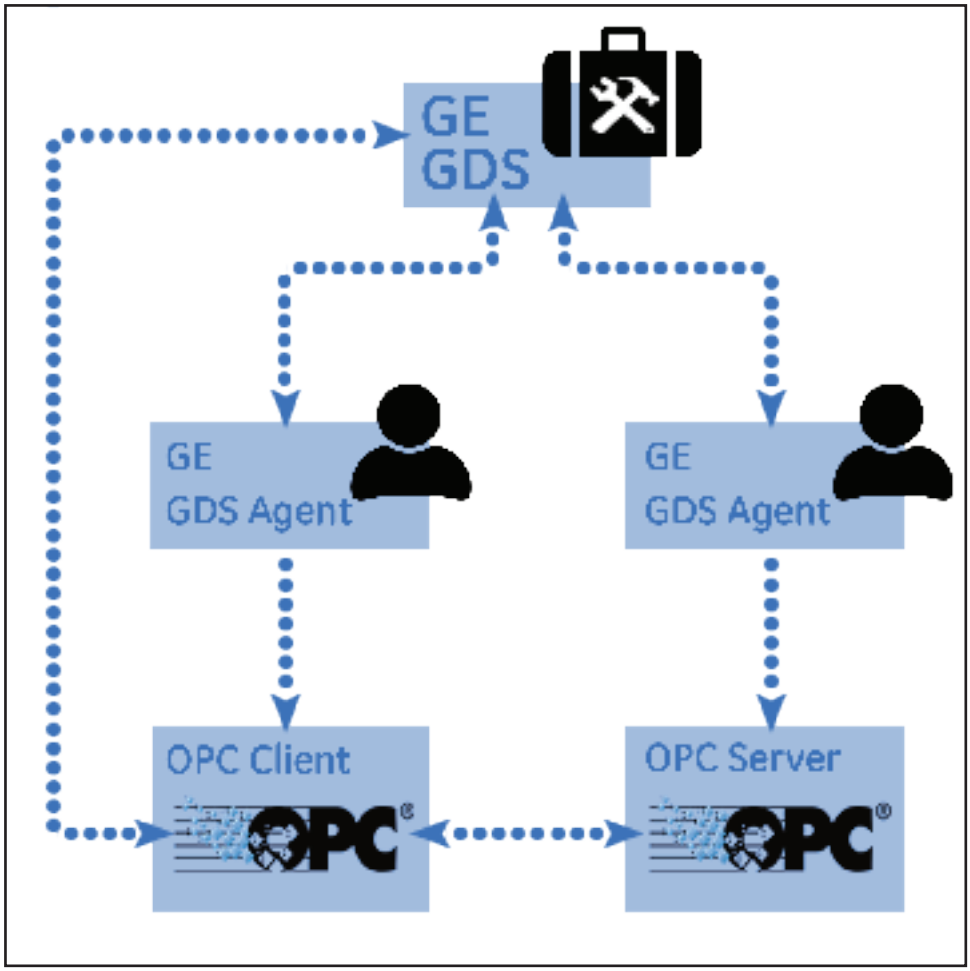
– Achilles Storms generiert große Mengen an Paketen in kurzen Zeitabständen, um die Fähigkeit des DUTs zu untersuchen, wie die unterschiedlichen Protokolle mit der hohen Verkehrsrate zurechtkommen. Über die Achilles Test Plattform kann auch nach dem denial-of-service Grenzwert für einen bestimmten Typ von Storm Traffic gesucht werden – der Wert, ab dem das Gerät nicht länger gängige Anfragen beantworten kann.

Bekannte Schwachstellen – Bei Testfällen mit bekannten Schwachstellen wurde ausschöpfender Traffic generiert, der mit hoher Wahrscheinlichkeit bei Kontrollgeräten vorkommt. Wurldtech bezeichnet den Achilles Grammar Test als „verzerrten Test", bei dem ungültige, unerwartete und zufällige Daten zu den Inputs geliefert werden. Das Programm wird überwacht für Ausnahmen, wie Zusammenbrüche, fehlerhafte built-in Code Einbettung oder für das Finden potenzieller Datenlücken. Während des Achilles Tests wird das Gerät durch Kommunikationsrückmeldung mit diskreten und analogen Signalen überwacht. Das Gerät muss die Anforderungen und Signale innerhalb akzeptierbarer Spezifikationen während der Tests unterstützen.

GE animiert seine Kunden erweiterte Kommunikationsprotokolle zu nutzen. OPC UA ist allgemein akzeptiert für seine sichere Kommunikation zwischen Systemen. OPC UA ist Plattform unabhängig und benötigt nicht länger die Sicherheit von COM/DCOM. OPC UA Security lässt den Austausch von gelenkten Zertifikaten zwischen Client und Server zu. Dieses Zertifikat ist eine elektronische ID, ausgewiesen von der Applikation, die die Identität des Anwenders bestimmt. Diese Zertifikate sind konform zur X509 Spezifikations. Die Daten werden zwischen den Endpunkten des OPC UA Austausches verschlüsselt, um den Zugriff Dritter zu unterbinden. Sogar mit diesen erweiterten Features ist OPC UA netzwerkfreundlich und kommuniziert über Standard HTTP oder UA TCP Ports. OPC UA kann sicher über VPN und durch Firewalls verbinden.

Definieren Sie Berechtigungen und wenden Sie sicheren Fernzugriff an

GE bietet seinen Kunden erweiterte Sicherheitsfunktionalität, die die Anwender zu einem besseren Umgang mit Passwörtern für ihr Equipment fordert, ebenso wie mehrfache Passwort geschützte Zugangslevel mit umfangreicheren Berechtigungen. GE stellt ebenso verschlüsselte Passwörter bereit, welche sichere Fernzugangsprotokolle nutzen, die helfen, unbefugten Zugriffen von Dritten vorzubeugen.



GE's OPC-UA Global Discovery Server

Secure Remote Password Protocol (SPR6a) benötigt Benutzer Authentifikation zwischen Client Applikationen und dem Server. SPR6a erlaubt es einer Client Applikation Authentifizierungs Sequenzen an einen Server zu übermitteln, wobei das aktuelle Passwort nie offengelegt wird. Alles was am Server offengelegt wird, wird mit einem einmaligen Wert, abgeleitet vom Benutzer Passwort verschlüsselt. Wenn ein Lauscher oder Dritter versucht zwischen Client und Server zu kommen, gibt es für ihn keinen Weg das Passwort zu erlangen. SRP6a gehört zu einer neuen Klasse von starken Authentifizierungs Protokollen, die allen bekannten passiven und aktiven Netzwerkangriffen standhalten. Informationen über letzte Zugänge und letzte Updates werden aufgezeichnet.

Überwachung und Rückmeldung

GE erkannte, dass der erste Schritt um sich gegen moderne Bedrohungen zu verteidigen, aktive Überwachung von feindlichem Eindringen ist. Die Funktionalität von IICS versorgt die Kunden mit Informationen über letzte Zugänge und letzte Updates für Prüfungszwecke, sodass die Benutzer jegliche verdächtige Aktivität überwachen können. Zusätzlich verfügt IICS über eingebaute Software Firewalls die dafür ausgelegt sind, das Aufdecken und Verhindern von Denial-of-Service und Distributed-Denial-of-Service Angriffen durch Drosseln der Eingangs-/Ausgangs-Kommunikation und Alarmierungsoperatoren zu ermöglichen. GE unterstützt ebenfalls Netzwerkkommunikations-Port Überwachung, die unerwartete Netzwerkprotokolle, Verbindungen oder Kommunikationstypen überprüft.

Betreiben Sie Applikations-Whitelisting

GE empfiehlt seinen Kunden Host Level Application Whitelisting anzuwenden, wobei eine der drei unten erklärten Strategien für HMI/SCADA Server angewendet werden kann:

1. Wenden Sie Anti-Virus-Software auf dem HMI/SCADA Server an.

2. Verwenden Sie zentralisierte Anti-Malware-Software für Ihre Anlage.

3. EDR – Endpoint Detection and Response Software für Ihre Anlage.

Abhängig von der Komplexität und Größe Ihrer Applikation, sollten Sie als Anwender einen oder mehrere der im vorherigen Absatz definierten Ansätze von Host Level Application Whitelisting verfolgen, um die volle Sichtbarkeit und Kontrolle über die Applikation auf den HMI/SCADA Servern zu gewährleisten.

Zusätzlich führt die GE HMI/SCADA Software umfangreiches Applikations Whitelisting durch, wobei Anwender die Funktion haben, Zugangsbeschränkungen bei verschiedenen Projekten innerhalb ihrer SCADA Applikation einzurichten.

Stellen Sie korrektes Konfigurations- und Patch Management sicher!

GE erkannte, dass Kontrollsysteme „secure by design" sein müssen und dass die Hardware einen vertrauensvollen Ursprung haben sollte, da dies die Grundlage für alle Sicherheitskonstruktionen innerhalb des Kontrollsystems ist. Für das IICS Portfolio sind alle Steuerungen jetzt mit Trusted Platform Module (TPM) Technologie ausgestattet, die einen vertrauensvollen Hardwareursprung ermöglicht. Jede Firmware wird bei GE mit einem Schlüssel signiert, der im TPM Modul abgespeichert wird, um sicherzustellen, dass nur von GE signierte Firmware an der Hardware ausgeführt wird. Von GE unterstützte Patches sind ebenso signiert für Verifizierungszwecke vorrangig für den Ladevorgang.

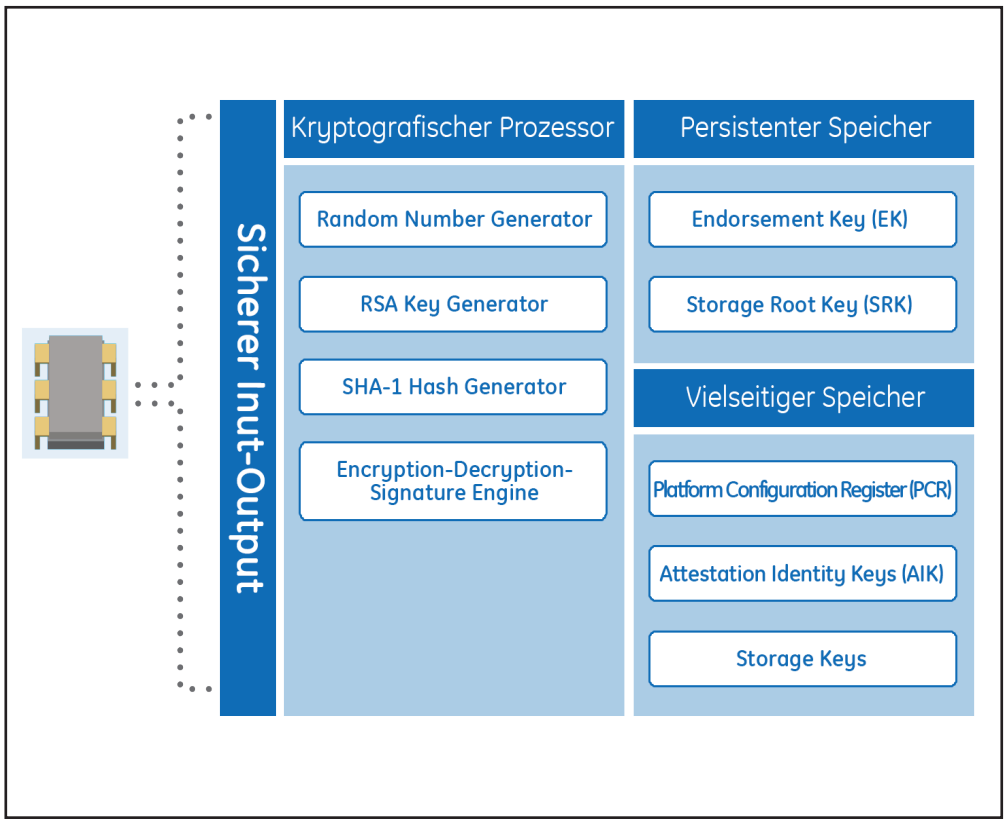
Trusted Platform Module (TPM)

Das Trusted Platform Module ist ein separates Hardwaremodul mit einer zugehörigen Microsteuerung, die die kryptographische Schlüssel Generation und die Schlüssel Speicherfähigkeit unterstützt. Seit jeder TPM Chip ein eigenes und geheimes RSA Schlüsselpaar hat, kann es Plattform Authentifizierung durchführen. Software kann das TPM benutzen, um andere Hardwaregeräte zu authentifizieren.

Das TPM kann für Ver- und Entschlüsselungsvorgänge verwendet werden und ist eine ausgezeichnete Entropiequelle für zufällige Nummerngenerationen. Der zufällige Nummerngenerator macht es für jedes andere System virtuell unmöglich, die generierte Sequenz zu erraten. Diese Fähigkeit, kombiniert mit dem Serverschlüssel, kreiert eine verschlüsselte Verbindung zwischen zwei Punkten. Das TPM generiert eine nicht wiederholbare Nummer, die es für äußere Einflüsse schwer macht, die übermittelten Daten zu entschlüsseln.

Das TPM kann an jedem Computer ausgeführt werden und ist vom United States Department of Defense (TPM Version 1.2 oder höher) für viele Geräte vorgeschrieben, dazu gehören beispielsweise Telefone und Computer. TPM schafft in Kombination mit BIOS eine „hardware root-of-trust".

Root of Trust (RoT) umfasst eine Reihe von Funktionen im gesicherten EDV Modul, das immer durch das Operationssystem des Computers geschützt ist. Das RoT dient als separater Computer, das den gesicherten EDV Plattform Verschlüsselungsprozessor auf dem Gerät überwacht, in dem es eingebettet ist.



TPM erlaubt eine sichere Speicherung und Berichte von Sicherheits-Metriken, die verwendet werden können, um die Systemkonfiguration zu validieren und um sicherzustellen, dass keine Veränderungen passiert sind.

Remote Attestation, ein Authentifizierungsprozess, kann erleichtert werden, wenn das TPM einen fälschungssicheren Hash Key kreiert, der eine Signatur der Hardware und Software Konfiguration ist. Das kann es Drittsystemen ermöglichen nachzuweisen, dass die Software nicht verändert wurde.

Secure Boot

Mit Secure Boot prüft die System Firmware, ob der System Boot Ladevorgang mit einem von GE autorisiertem und verschlüsseltem Key in einer Datenbank gespeichert wird, die in der Firmware enthalten ist. Das wird bei UEFI (Unified Extensible Firmware Interface) in Kombination mit BIOS für einen kontrollierten Boot verwendet, um der Ausführung von unsignierten Programmen vorzubeugen.

Trusted Boot

Trusted Boot übernimmt, wo Secure Boot endet. Trusted Boot verifiziert die digitale Signatur des OS. Das OS wiederum verifiziert die Komponenten, die es im Startup Prozess nutzt, wie die Startup Files und Boot Driver. Wenn ein File verändert wurde, findet der Boot Loader diese Veränderung und lehnt dann das Laden dieser Komponente ab.

Trusted Boot verwendet nur vertrauenswürdige Software, die oft ausgeführt wird, wenn signierte und zertifizierte Software vom Hersteller verwendet wird. Das resultiert in korrektem Konfigurations- und Patch Management.

Zusammenfassung

Verteidigung gegen moderne Cyber Angriffe setzt die Anwendung von Schutzmaßnahmen nicht nur für das externe, sondern auch für das interne Kontrollsystem voraus. Mit dem industriellen Internet Kontrollsystem hat die nächste Entwicklung der Kontrolltechnologie begonnen, die Kraft von verbundenen und optimierten Anlagen und Systemen nutzbar zu machen.

Die Vorteile beim Übernehmen von IICS Technologie können nicht ignoriert werden, wenn Unternehmen in der heutigen Weltwirtschaft wettbewerbsfähig bleiben wollen. GE arbeitet daran, sichere Produkte anzubieten, um es Kunden zu ermöglichen, Teil dieser neuen Entwicklung zu werden.

Bei GE ist Sicherheit nicht etwa ein nachträglicher Einfall, sondern „built in". Die laufende Überprüfung und Verbesserung der Produktsicherheit unter Verwendung von regulärer Bewertung und Penetration ist ein kritisches Element des Produkts-Designs Lebenszyklus.

GE Partner wollen zusammen mit Kunden, Industrie, Arbeitsgruppen, Normungsorganisationen und Regierungsagenturen kontinuierlich die Sicherheit von industriellen Steuerungssysteme und globaler Infrastruktur verbessern. Wir sind engagiert, die Vollständigkeit, Verfügbarkeit und Vertraulichkeit von Kundensystemen und -Daten aufrechtzuerhalten.

Da Cyber Security Bedrohungen sich immer weiter entwickeln, werden GE Sicherheitsexperten weiter daran arbeiten, die Sicherheits Features unserer Produkte weiterzuentwickeln.

Bild: GE A&C

COMPETENCE IN AUTOMATION

Taschek & Gruber Automatische Datenverarbeitungs gmbH

Pallstr. 2, 7503 Großpetersdorf, T +43 (0) 3362 21012, F DW-90, E-Mail: office@tug.at
www.tug.at

T&G Solutions GmbH

Kaiser-Friedrich-Promenade 85, 61348 Bad Homburg v.d. Höhe,
T +49 (0) 6172 981 9342, E-Mail: office@tug.at