Abonnement für den Schutz von Cyber-Anlagen für die Stromerzeugung

Überblick

In einer komplexen Welt mit sich ständig ändernden Technologien erkennt GE an, dass sehr wichtig ist, einen erfahrenen Partner zu haben, der Sie erfolgreich durch die Umsetzung von Cyber-Sicherheit führt. Als ein weltweit führendes Unternehmen im Bereich industrielle Bedienelemente verfügt GE über die Fachkompetenz zur Verbesserung der Sicherheit seiner Kunden und zur Unterstützung bei der Einhaltung von Vorschriften. Wir haben bei unseren Lösungen den Schwerpunkt auf Sicherheit gelegt und sie lassen sich gut in umfassendere Systeme auf Anlagenebene und in IT-Architekturen integrieren.

Das Abonnement von GE zum Schutz von Cyber-Anlagen ist eine zentrale Lösung für das Sicherheitsmanagement und ein wesentlicher Bestandteil von Systemen mit gestaffelten Sicherheitsebenen für Turbinen-, Anlagen- und Generatorsteuerungen. Der Aboservice umfasst das Betriebssystem und Anwendungs-Patches sowie Antivirus-/Angriffserkennungs-Signaturen und deckt Updates für HMI, Server, Switches und Vorrichtungen zur Erkennung von Angriffen auf Netzwerke ab. Monatliche Updates können auf einzelne HMI oder über SecurityST* für den Einsatz im gesamten Netzwerk durchgeführt werden.

Das Abonnement von GE zum Schutz von Cyber-Anlagen gehört zu SecurityST Mark* VIe Lösung und Serviceleistungen für die Inbetriebnahme, die nach Achilles® Practices – Bronze zertifiziert sind. Das bezeugt, dass die Lösung die optimalen Verfahren für eine hohe Cyber-Sicherheit einhält und zeigt dem Kunden auf, dass die Systeme sicher entwickelt und umgesetzt werden. Das Abonnement zum Schutz von Cyber-Anlagen wurde entwickelt, um Unternehmen bei der Einhaltung der Normen und Richtlinien für die Cyber-Sicherheit wie NERC CIP, NEI 08-09 und ISA99/IEC 62443 durch die Anlagen zu unterstützen.

Warum sind Patches kritisch?

Die Aktualisierung Ihrer Systeme mit Patches ist eines der besten Verfahren zum Schutz Ihrer Anlagen und sie gewährleisten, dass das Betriebssystem und die Programme die Updates erhalten, die den neuesten Schutz gegen Bedrohungen bieten, ohne Ihren Betrieb zu gefährden. Die Aktualisierung mit Patches wird vom SANS Institute, einer renommierten Autorität auf dem Gebiet der Informationssicherheit und Schulungen zur Cyber-Sicherheit, als zwei der „First Five Quick Wins" aufgeführt. Die Aktualisierung von Anwendungen und Systemsoftware mit Patches ist für die Verbesserung und Beibehaltung eines hohen Sicherheitsniveaus kritisch.

Wie funktioniert es?

Das Cyber Asset Protection-Abonnement liefert monatliche Updates für Ihre HMI, Historian-Funktionen, Switches, Firewalls, OSM und RSG. Die Software-Updates umfassen:

- Betriebssystem Windows®
- GE Cimplicity (ICS-CERT-spezifisch)
- Angriffserkennungs-Signaturen
- Antivirus-Signaturen
- Switch-Updates
- System 1*

Der Aboservice liefert auch einen monatlichen Bericht mit den Patches, die installiert werden müssen und die Bereiche, denen unbedingt Beachtung geschenkt werden muss.

Vorteile

- Lieferte geprüfte Updates, um Ihre kritische Alt-Infrastruktur am Laufen zu halten
- Reduziert Stillstandszeiten durch die Bereitstellung von validierten Patches, die in einem Umfeld getestet werden, um die Anwendbarkeit und die Kompatibilität zu gewährleisten
- Hält Ihr Risikoprofil auf dem neuesten Stand und erhöht Ihre Sicherheit durch den Schutz Ihrer kritischen Anlagen vor bekannten Anfälligkeiten auf einer monatlichen Basis

- Hilft Ihnen bei der Erfüllung der gesetzlichen Vorschriften und dabei, Geldstrafen zu vermeiden
- Verbessert die Sicherheit und Zuverlässigkeit, indem es der Verlust der Sichtbarkeit verhindert
- Eigener Service-Manager für Cyber-Angelegenheiten

Die Bedeutung der Validierung

Mit dem validierten Patch-Management können die Updates in einem Labor validiert werden, in dem die Bedingungen der Anlage nachgestellt werden, um vor der Verwendung des Patch zu ermitteln, ob eine Inkompatibilität vorliegt. Damit kann der Betreiber bestimmten, welche Änderungen erforderlich sind, um die Verfügbarkeit und den Schutz gegen Cyber-Bedrohungen zu gewährleisten, ohne dass sie selbst Simulatoren erstellen müssen. Unsere Tests werden in einem gesicherten Labor sowohl mit Hardware als auch mit Software durchgeführt. Es handelt sich dabei um das beste Verfahren, um zu gewährleisten, dass industrielle Bedienelemente auf monatlicher Basis maßgeschneiderte Patches und einen Anwendungsbericht erhalten.

Ein zuverlässiger Partner für Compliance

Als Lieferant von industriellen Bedienelementen übernimmt GE seine Verantwortung gegenüber den Eigentümern von kritischer Infrastruktur gerne und unterstützt sie bei der Verbesserung ihrer Sicherheit und ihren Bemühungen in Bezug auf Compliance für von GE gelieferte Anlagen während des 10- bis 20-jährigen Lebenszyklus des Steuersystems. Zusammen mit Wurldtech Security Technologies kann GE eine Unterstützung für die Sicherheit anbieten, die von der Planung des Systems über die Inbetriebnahme bis hin zu fortlaufendem Support und Wartung reicht.

NERC CIP Rev 5

Viele Stromversorgungsunternehmen in den USA sind jetzt auf Bundesebene zur Einhaltung der Anforderungen von NERC CIP verpflichtet, nach denen bis April 2016/2017 der Einsatz von Technologien für die industrielle Sicherheit und Mängelbeseitigung vorgeschrieben ist. Bei der Anpassung des Betriebs an diese Vorschriften sind die Problematik des Anwendens von Patches auf industrielle Bedienelemente und die häufigen Angriffe auf die Anlagen zu berücksichtigen. Dazu müssen die Kunden bekannte ICS-Anfälligkeiten beheben, ohne den Betrieb zu unterbrechen. Wegen dieser Faktoren benötigen elektrische Versorgungsunternehmen eine Lösung, die einfach umzusetzen ist und einen Einblick in das industrielle Netzwerk und Compliance bringt.

NEI 08-09

Die Betreiber von Kernkraftwerken in den USA sind auf Bundesebene verpflichtet, für einen ausreichenden Schutz von digitalen Computern und Kommunikationssystemen und -netzwerken gegen Cyber-Angriffe zu sorgen. Im Rahmen eines Cyber-Plans müssen die Betreiber bekannte ICS-Anfälligkeiten beheben und u.a. über Lösungen für Updates des Betriebssystems, der Anwendungen und externer Software, Host Intrusion Detection und Nachweisbarkeit verfügen.

IEC 62443-2-4

IEC 62443-2-4 ist eine veröffentlichte internationale Norm, in der Programme zur Cyber-Sicherheit beschrieben werden, die Anbieter von industriellen Automatisierungssystemen (Industrial Automation and Control System - IACS) realisieren und anbieten können. Die Norm kann den Eigentümer von Anlagen bei der Beschaffung und beim Management von Fachkompetenz im Bereich Sicherheit für Steuersysteme behilflich sein. IEC 62443-2-4 wurde vom Technischen Kommitee 65 der IEC in Zusammenarbeit mit International Instrumentation Users Association (vormals WIB) und den Mitgliedern des ISA 99 Komitees erarbeitet. GE stärkt die Systeme seiner Kunden mit einer Kombination aus technischen und verfahrenstechnischen Maßnahmen, die nach der Sicherheitsnorm IEC 62443-2-4 zertifiziert sind. Diese Normen enthalten umfassende Vorgaben von Sicherheitsanforderungen für die Installation und Wartung von industriellen Automatisierungssystemen (IACS).

Weitere Informationen über unser Angebot zur Erfüllung dieser drei Normen und Vorschriften finden Sie auf unserer Website www.gemeasurement.com/machinery-control.

Für weitere Informationen wenden Sie sich bitte an:
GE Oil & Gas
Nordamerika: 1-888-943-2272; 1-540-387-8726
Lateinamerika (Brasilien): +55-11-3958-0098
Europa (Frankreich): +33-2-72-249901
Asien/China (Singapur): +65-6622 1623
Afrika/Indien/Naher Osten (VAE): +971-2-699 7119

E-Mail: ControlsConnect@ge.com
Kunden-Portal: ge-controlsconnect.com

1800 Nelson Road
Longmont, CO, USA 80501
https://www.gemeasurement.com

Für weitere Unterstützung oder technische Informationen wenden Sie sich an ein Verkaufs- oder Servicebüro in Ihrer Nähe oder an einen autorisierten Außendienstmitarbeiter von GE

GEA30382D-DE (06/2016)