14. Datenschnittstellen von Drittanbietern einschränken

Schränken Sie die Art der Verbindungen und die verfügbaren Daten für 3rd-Party-Schnittstellen ein. Die Verbindungen und/oder Datenschnittstellen sollten klar definiert und so eingeschränkt sein, dass nur Lese-/Schreibfähigkeiten für die erforderliche Datenübertragung möglich sind.

Sicherheitsziel	Zilegruppe
Härten	Integrator / Wartungsdienstleister

Anleitung

In einigen Fällen stellen aufgrund langer Kabelwege oder eines großen Datenaustauschs Schnittstellendatenverbindungen einen besseren Geschäftsfall dar als ein fest verdrahteter Datenaustausch zwischen zwei separaten Parteien.

Die folgenden Richtlinien sollten beim Entwerfen und Implementieren einer Datenaustauschschnittstelle eines Drittanbieters berücksichtigt und befolgt werden, sofern dies praktikabel ist:

- Verwenden Sie ein dediziertes Kommunikationsmodul, das entweder direkt mit der SPS oder den Datenaustauschgeräten des Drittanbieters verbunden ist, oder verwenden Sie dedizierte Netzwerkgeräte, die physisch vom Kernnetzwerk jeder Partei getrennt sind.
- Die MAC-Adresse der angeschlossenen Geräte ist in der Regel in Systemvariablen für jedes ICS verfügbar Ethernet-fähiges Gerät, das es ermöglicht, die Geräteidentität mit einem Multi-Faktor-Ansatz zu überprüfen (IP-Adresse + MAC-Maker-Code = vertrauenswürdiges Gerät). Diese Praxis ist sicherlich nicht narrensicher, da MAC- und IP-Adressen gefälscht werden können, aber sie dient dazu, die Messlatte in Bezug auf die Kommunikation zwischen vertrauenswürdigen ICS-Systemen und -Geräten höher zu legen.
- Wählen Sie bei der Auswahl eines Protokolls für 3rd-Party-Schnittstellen ein Protokoll, das die Fähigkeit des Dritten, Daten in das System des Eigentümers zu schreiben.
- Wählen Sie eine Verbindungsmethode und einen Verbindungsport, der verhindert, dass der Drittanbieter in der Lage, die SPS oder die Datenaustauschgeräte des Eigentümers zu konfigurieren.
- Der Dritte sollte nicht in der Lage sein, Daten zu lesen oder zu schreiben, die nicht ausdrücklich definiert und zur Verfügung gestellt werden.
- Verwenden Sie einen Watchdog-Timer zur Überwachung der Kommunikation, damit keine Befehle an eine SPS im Fehlermodus.
- Serielle Verbindung: Verwenden Sie ein dediziertes Kommunikationsmodul für jede 3rd-Party-Schnittstelle mit Ein eingeschränktes Array von Daten. Stellen Sie sicher, dass die Seite des Besitzers der Verbindung der Initiator und der Drittanbieter der Responder ist.
- Ethernet/IP: Einige SPSen ermöglichen die Funktion von Kommunikationsmodulen als Firewall und können Deep Packet Inspection (DPI) durchführen oder die Schnittstellen der Kommunikationsmodule auf eine Begrenzung beschränken den Datenaustausch zu einer vordefinierten Teilmenge. Wenn diese Funktionen verfügbar sind und ein Ethernet/IP-Protokoll verwendet wird, stellen Sie sicher, dass die Funktionen aktiviert und konfiguriert sind.
- Wenn betriebliche oder vertragliche Anforderungen den Eigentümer daran

hindern, die vorherigen Punkte zu erfüllen, sollten Sie die Verwendung einer separaten "Datenkonzentrator"-SPS (auch bekannt als Proxy/DMZ) in Betracht ziehen, um die Daten zu puffern und den Eigentümer vor unerwünschten Schreibvorgängen/Programmierungen durch die Drittpartei zu schützen. Stellen Sie sicher, dass die Backplane dieser SPS nicht vom 3rd-Party-Netzwerk aus durchquert werden kann.

Beispiel

- Pipeline- oder Leasing-Einheiten für den automatischen eichpflichtigen Verkehr (LACT), die Kohlenwasserstoffe oder Wasser, die zwischen einem Upstream-Produktions- oder Pipeline-Unternehmen und einem Midstream-Pipeline-Unternehmen mit Netzwerk- oder seriellen Schnittstellenverbindungen ausgetauscht werden, die Mess-, Zustands- und Freizügigkeitsinformationen zwischen Unternehmen austauschen.
- Regionaler Trinkwasserversorger (Importeur) teilt die gelieferte Wasserdurchflussmenge an der Weiche an das Wasserwerk einer örtlichen Gemeinde

Begründung

Vorteilhaft für	Begründung
Sicherheit	1. Begrenzen Sie die Gefährdung durch Netzwerke und Geräte von Drittanbietern. 2. Authentifizieren Sie externe Geräte, um Spoofing zu verhindern., besteht darin, sie vollständig zu deaktivieren.
Zuverlässigkeit	Schränkt die Möglichkeit für absichtliche oder unbeabsichtigte Änderungen oder den Zugriff von Standorten oder Geräten von Drittanbietern ein.
Instandhaltung	./.

Referenzen

Standard / Framework	Mapping
MITRE ATT&CK für ICS	**Taktik** : TA0105 Impair Process Control **Technik:** T0836 Modify Parameter
ISA 62443-3-3	**SR 7.6**: Netzwerk- und Sicherheitskonfigurationseinstellungen **SR 7.7:** Geringste Funktionalität
ISA 62443-4-2	**SR 7.6:** Netzwerk- und Sicherheitskonfigurationseinstellungen **CR 7.7:** Geringste Funktionalität
ISA 62443-4-1	**SD-4:** Best Practices für sicheres Design **SI-1:** Überprüfung der Sicherheitsimplementierung **SVV-1:** Testen von Sicherheitsanforderungen

15. Definieren Sie einen sicheren Prozesszustand im Falle eines SPS-Neustarts

Definieren Sie sichere Zustände für den Prozess bei SPS-Neustarts (z. B. Kontakte einschalten, stromlos schalten, vorherigen Zustand beibehalten).

Sicherheitsziel	Zilegruppe
Resillienz	Produktlieferant Integrator / Wartungsdienstleister

Anleitung

Wenn irgendetwas einer SPS befiehlt, mitten in einem Arbeitsprozess neu zu starten, sollten wir erwarten, dass das Programm reibungslos und mit minimaler Unterbrechung des Prozesses aufgenommen wird. Stellen Sie sicher, dass der von ihm gesteuerte Prozess neustartsicher ist.

Wenn es nicht praktikabel ist, die SPS so zu konfigurieren, dass sie einen sicheren Neustart ermöglicht, stellen Sie sicher, dass sie Sie auf diese Tatsache hinweist und keine neuen Befehle ausgibt. Stellen Sie in diesem Fall außerdem sicher, dass die Standardarbeitsanweisungen (SOP) sehr klare Anweisungen zum Einstellen der manuellen Steuerungen enthalten, damit die SPS den Prozess ordnungsgemäß startet.

Dokumentieren Sie außerdem alle Vorgänge zum Starten, Herunterfahren, zur stationären Steuerung und zum Neustart des Flugsteuerungssystems.

Beispiel

/

Begründung

Vorteilhaft für	Begründung
Sicherheit	**Eliminiert potenziell unerwartetes Verhalten:** Der grundlegendste Angriffsvektor für eine SPS besteht darin, sie zum Absturz und / oder Neustart zu zwingen. Für viele SPSen ist das gar nicht so schwer, denn viele SPSen kommen mit unerwarteten Eingaben oder zu viel Verkehr nicht gut zurecht. Es gibt zwar mehrere Diagnosen für Controller-Aktionen während der Ausführung, aber es ist in der Regel nicht klar, wie der Start mit einem laufenden Prozess gehandhabt wird. Dies kann dazu führen, dass Es ist ungewöhnlich, aber es ist ein grundlegender Angriffsvektor, wenn wir böswilliges Verhalten eines Angreifers berücksichtigen.
Zuverlässigkeit	**Vermeiden Sie unerwartete Verzögerungen:** Wenn nach dem Einschalten einer SPS die Zustandsmaschine in einen Zustand mit einigen Bedingungen initialisiert wird, die den Prozess nicht starten lassen, und der Bediener das System nicht normalisieren kann, müsste ein Techniker das SPS-Programm eingeben, um zu erzwingen, dass die Bedingungen in den gewünschten Zustand versetzt werden, um den Betrieb starten zu können. Dies kann zu Verzögerungen und Produktionsausfällen führen..
Instandhaltung	./.

Referenzen

Standard / Framework	Mapping
MITRE ATT&CK für ICS	**Taktik** : TA0107 Inhibit Response Function **Technik:** T0816 Device Restart/Shutdown
ISA 62443-3-3	**SR 3.6**: Deterministische Ausgabe
ISA 62443-4-2	**CR 3.6**: Deterministische Ausgabe
ISA 62443-4-1	**SVV-1**: Prüfung der Sicherheitsanforderungen

16. Fassen Sie die SPS-Zykluszeiten zusammen und trenden Sie sie auf dem HMI

Fassen Sie die SPS-Zykluszeit alle 2-3 Sekunden zusammen und melden Sie sie dem HMI zur Visualisierung in einem Diagramm.

Sicherheitsziel	Zilegruppe
Überwachung	Integrator / Wartungsdienstleister

Anleitung

Zykluszeiten sind in der Regel Systemvariablen in einer SPS und können zur Zusammenfassung in SPS-Code verwendet werden. Die Zusammenfassung sollte durchgeführt werden, um Durchschnitts-, Spitzen- und Mindestzykluszeiten zu berechnen. Das HMI sollte bei diesen Werten einen Trend darstellen und eine Warnung ausgeben, wenn es signifikante Änderungen gibt.

Die Zykluszeit ist die Zeit, die benötigt wird, um jede Iteration der Logik für die SPS zu berechnen. Bei den Iterationen handelt es sich um die Kombination aus Kontaktplandiagrammen (KOP), Funktionsblockdiagrammen (FBS), Anweisungslisten (IL) und strukturiertem Text (ST). Diese Logikkomponenten können mit den sequentiellen Funktionsplänen (SFC) zusammengefügt werden.

Die Zykluszeiten sollten auf einer SPS konstant sein, es sei denn, es gibt Änderungen an z.B.

- Netzwerkumgebung
- SPS-Logik
- Prozess

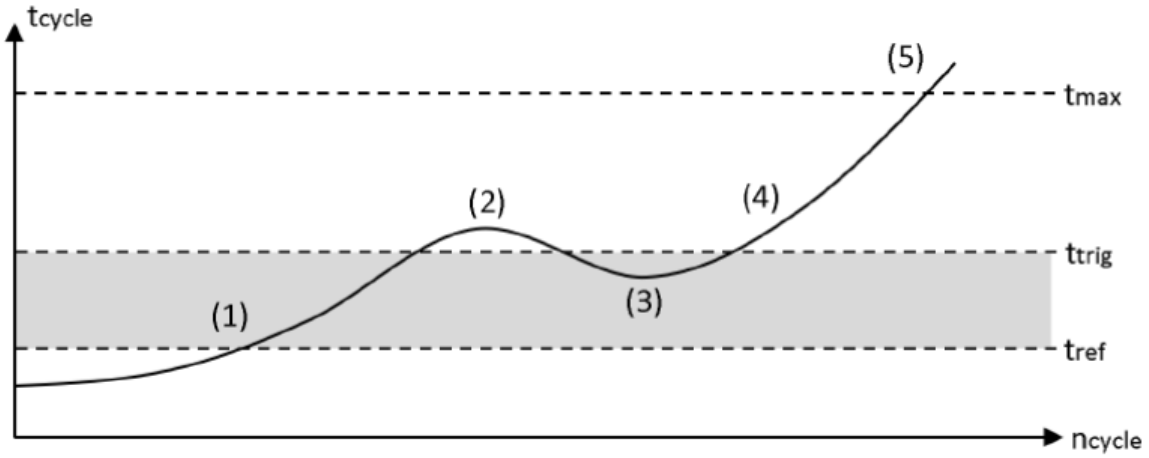
Daher können ungewöhnliche Zykluszeitänderungen ein Indikator dafür sein, dass sich die SPS-Logik geändert hat und somit wertvolle Informationen für Integritätsprüfungen liefern.

Die Visualisierung von Werten im Zeitverlauf mithilfe eines Diagramms bietet eine intuitive Möglichkeit, die Aufmerksamkeit auf Anomalien zu lenken, die mit absoluten Werten schwieriger zu erkennen wären.

Beispiel

Viele SPSen verfügen über eine "maximale Zykluszeit"-Überwachung auf Hardware-Ebene. Überschreitet die Zykluszeit den Maximalwert, setzt die Hardware die CPU auf STOP (5). Natürlich sind sich Angreifer dessen bewusst und werden einen möglichen Angriffscode so schlank wie möglich halten, um die Auswirkungen auf die Gesamtzykluszeit zu minimieren. In einem zusätzlichen Software-Zykluszeitüberwachungsprogramm wird ein Referenzzyklus-t_{ref} als Basiszykluszeit definiert. Da kleine Schwankungen natürlich sind, muss ein akzeptabler Schwellenwert definiert werden (1,3) Die Zyklusüberwachung wird ausgelöst, wenn der Schwellenwert überschritten wird (2,4).

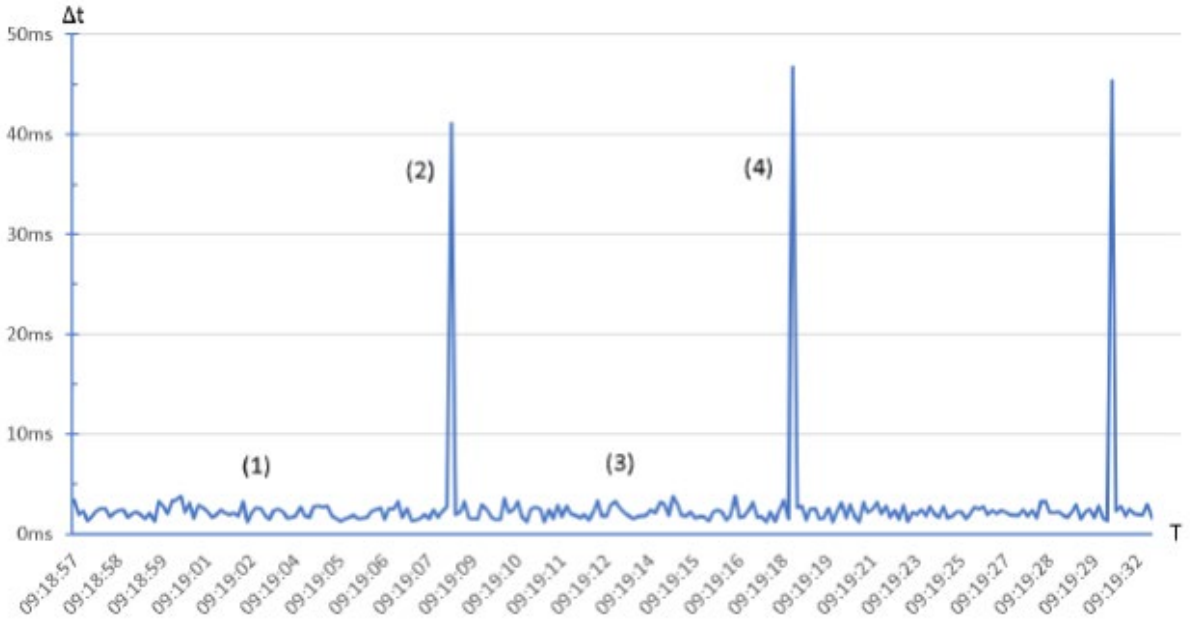
Wenn die Zykluszeiten auf das HMI zugeführt werden, sind hohe CPU-Lasten auf einen Blick sichtbar. Das folgende Beispieldiagramm zeigt ein SPS-Programm mit periodisch ausgeführtem Schadcode. (1,3) im Normalbetrieb akzeptable Zykluszeitschwankungen ("Rauschen") aufweisen, wird auf (2,4) Angriffscode ausgeführt, der die Zykluszeit erhöht.



Jede Abweichung von der Referenzzeit kann wie folgt in einem Logfile gespeichert werden:

SeqNo	Date	UTC Time	Abweichung
1	2019-11-22	09:05:50.021	40,821ms
2	2019-11-22	09:06:00.069	44,391ms
3	2019-11-22	09:06:10.120	44,994ms
4	2019-11-22	09:06:20.166	40,561ms
5	2019-11-22	09:06:30.211	40,725ms

Wenn die Zykluszeiten auf das HMI zugeführt werden, sind hohe CPU-Lasten auf einen Blick sichtbar. Das folgende Beispieldiagramm zeigt ein SPS-Programm mit periodisch ausgeführtem Schadcode. (1,3) im Normalbetrieb akzeptable Zykluszeitschwankungen ("Rauschen") aufweisen, wird auf (2,4) Angriffscode ausgeführt, der die Zykluszeit erhöht.



Begründung

Vorteilhaft für	Begründung
Sicherheit	Zu den Angriffen auf SPS gehören das Ändern der Logik, das Aktivieren eines neuen Programms, das Testen von neuem Code, das Laden eines neuen Prozessrezepts, das Einfügen von Hilfslogik , um Nachrichten zu senden oder eine Funktion zu aktivieren. Für die meisten SPS sind herkömmliche kryptografische Integritätsprüfungen nicht durchführbar. Es ist jedoch gut, Warnung, wenn eine der oben genannten logischen Änderungen eintritt. Da die Zykluszeiten Unter normalen Umständen eher konstant, sind Änderungen der Zykluszeiten ein guter Indikator dafür, dass sich die Logik in einer der oben genannten Logikkomponenten geändert hat.
Zuverlässigkeit	Siehe Sicherheit, aber aus nicht böswilligen Gründen.
Instandhaltung	/

Referenzen

Standard / Framework	Mapping
MITRE ATT&CK für ICS	**Taktik** : TA0104 Execution **Technik:** T0873 Project File Infection
ISA 62443-3-3	**SR 3.4**: Software- und Informationsintegrität
ISA 62443-4-2	**EDR 3.2**: Schutz vor Schadcode
MITRE CWE	**CWE-754:** Unsachgemäße Prüfung auf ungewöhnliche oder außergewöhnliche Bedingungen

17. Protokollieren Sie die SPS-Betriebszeit und trenden Sie sie auf dem HMI

Protokollieren Sie die Betriebszeit der SPS, um zu wissen, wann sie neu gestartet wurde. Trend- und Protokollverfügbarkeit auf dem HMI für die Diagnose.

Sicherheitsziel	Zilegruppe
Überwachung	Integrator / Wartungsdienstleister

Anleitung

Behalten Sie den Überblick über die SPS-Betriebszeit

- in der SPS selbst (wenn die Betriebszeit eine Systemvariable in der SPS ist.
- in der SPS selbst, wenn diese über MIB-2 / eine beliebige SNMP-Implementierung verfügt
- extern mittels z.B. SNMP

Wenn die SPS SNMP mit MIB-2 hat, was sehr häufig vorkommt, ist die OID für die Betriebszeit "sysUpTimeInstance(0)" 1.3.6.1.2.1.1.3. Das Zurücksetzen der Betriebszeit ist ein wichtiger Indikator für SPS-Neustarts. Stellen Sie sicher, dass das HMI bei jeder Art von SPS-Neustart warnt.

Die Betriebszeit mit Fehlercodes zu korrelieren, ist eine gute Diagnosemethode.

Beispiel

/

Begründung

Vorteilhaft für	Begründung
Sicherheit	Der grundlegendste Angriffsvektor für eine SPS besteht darin, sie zum Absturz und / oder Neustart zu zwingen. Für viele SPSen ist das gar nicht so schwer, denn viele SPSen kommen mit unerwarteten Eingaben oder zu viel Verkehr nicht gut zurecht. So können unerwartete Neustarts ein Indikator dafür sein, dass die SPS auf ungewöhnliche Aktionen.
Zuverlässigkeit	SPS-Neustarts eignen sich auch gut für die Diagnose bei Ausfällen und für die Überwachung, an welcher SPS zu welchem Zeitpunkt gearbeitet wird.
Instandhaltung	/

Referenzen

Standard / Framework	Mapping
MITRE ATT&CK für ICS	**Taktik** : TA0107 Inhibit Response Function **Technik:** T0816 Device Restart Shutdown
ISA 62443-3-3	**SR 7.6**: Netzwerk- und Sicherheitskonfigurationseinstellungen
ISA 62443-4-2	**CR 7.6**: Netzwerk- und Sicherheitskonfigurationseinstellungen
MITRE CWE	**CWE-778:** Unzureichende Protokollierung

18. Protokollieren Sie SPS-Hardstopps und trenden Sie sie auf dem HMI

Speichern Sie SPS-Hard-Stop-Ereignisse von Fehlern oder Abschaltungen für den Abruf durch HMI-Alarmsysteme, um sie vor dem Neustart der SPS zu konsultieren. Zeitsynchronisierung für genauere Daten.

Sicherheitsziel	Zilegruppe
Überwachung	Integrator / Wartungsdienstleister

Anleitung

Fehlerereignisse zeigen an, warum eine SPS heruntergefahren wurde, damit das Problem vor einem Neustart behoben werden kann.

Einige SPS haben möglicherweise Fehlercodes aus dem letzten Fall, in dem die SPS fehlerhaft war oder nicht ordnungsgemäß heruntergefahren wurde. Notieren Sie diese Fehler, und löschen Sie sie dann. Es kann eine gute Idee sein, diese Fehler als Informationsdaten an das HMI oder vielleicht an einen Syslog-Server zu melden, wenn diese Funktionen und diese Infrastruktur vorhanden sind.

Die meisten SPSen verfügen auch über eine Art First-Scan-Funktion, die Ereignisse generiert. Es ist ein Verhalten, das fast alle SPS-Geräte in irgendeiner Form haben. Es handelt sich im Grunde um ein oder mehrere Flags oder eine bestimmte Routine, die beim ersten Scan einer SPS ausgeführt wird, nachdem sie "aufgeweckt" wurde. Dieser erste Scan sollte protokolliert und nachverfolgt werden.

Beispiel

/

Begründung

Vorteilhaft für	Begründung
Sicherheit	Protokolle ermöglichen die Fehlerbehebung im Falle eines Vorfalls. Bevor eine SPS in Betrieb genommen wird, insbesondere nach aufgetretenen Problemen, ist es wichtig, sicherzustellen, dass sie vertrauenswürdig ist.
Zuverlässigkeit	Protokolle sind auch gute Quellen für das Debuggen, wenn das Ereignis nicht böswillig verursacht wurde.
Instandhaltung	/

Referenzen

Standard / Framework	Mapping
MITRE ATT&CK für ICS	**Taktik** : TA0107 Inhibit Response Function **Technik:** T0816 Device Restart Shutdown
ISA 62443-3-3	**SR 7.6**: Netzwerk- und Sicherheitskonfigurationseinstellungen
ISA 62443-4-2	**CR 7.6**: Netzwerk- und Sicherheitskonfigurationseinstellungen
MITRE CWE	**CWE-778:** Unzureichende Protokollierung

19. Überwachen Sie die SPS-Speicherauslastung und zeigen Sie einen Trend auf dem HMI

Messen und stellen Sie eine Baseline für die Speicherauslastung für jeden Controller bereit, der in der Produktionsumgebung eingesetzt wird, und stellen Sie einen Trend auf dem HMI bereit.

Sicherheitsziel	Zilegruppe
Überwachung	Integrator / Wartungsdienstleister Asset Owner

Anleitung

Da die Zunahme von Codezeilen in der Logik auch zu einem erhöhten Speicherverbrauch zur Laufzeit führen kann, empfiehlt es sich für SPS-Programmierer, jede Abweichung von der Baseline zu verfolgen und diesem Ereignis eine Alarmklasse zu widmen.

Beispiel

In Rockwell Allen Bradley-SPSen kann eine Baseline auf einer Steuerung erstellt und die Speicherauslastung mit dem RSLogix 5000 Task Monitor Tool verfolgt werden. Nicht nur der Hauptspeicher, sondern auch der I/O-Speicher und der Ladder/Tag-Speicher können anhand von Trends verfolgt werden.

Begründung

Vorteilhaft für	Begründung
Sicherheit	Eine erhöhte Speicherauslastung kann ein Indikator dafür sein, dass die SPS geänderten Code ausführt
Zuverlässigkeit	Die Verfolgung der Speicherauslastung für die laufenden Programme kann nützlich sein, um den Gesamtspeicherverbrauch und einen eventuellen Fehlerzustand für die SPS-Steuerung zu vermeiden.
Instandhaltung	Die Nachverfolgung der Speicherauslastung kann zum Optimieren und Ermitteln der besten Scanzeit für den überwachten Controller, aber auch zur Fehlerbehebung bei Problemen und Problemen im Zusammenhang mit fehlerhaften Zuständen verwendet werden.

Referenzen

Standard / Framework	Mapping
MITRE ATT&CK für ICS	**Taktik** : TA0xx Ausführung
ISA 62443-3-3	**SR 3.4**: Software- und Informationsintegrität
ISA 62443-4-2	**EDR 3.2**: Schutz vor Schadcode

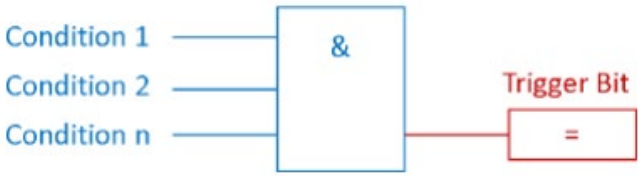
20. Fangen Sie falsch negative und falsch positive Ergebnisse für kritische Warnungen ab

Identifizieren Sie kritische Warnungen und programmieren Sie eine Falle für diese Warnungen. Legen Sie den Trap fest, um die Auslösebedingungen und den Alarmstatus für Abweichungen zu überwachen.

Sicherheitsziel	Zilegruppe
Überwachung	Integrator / Wartungsdienstleister

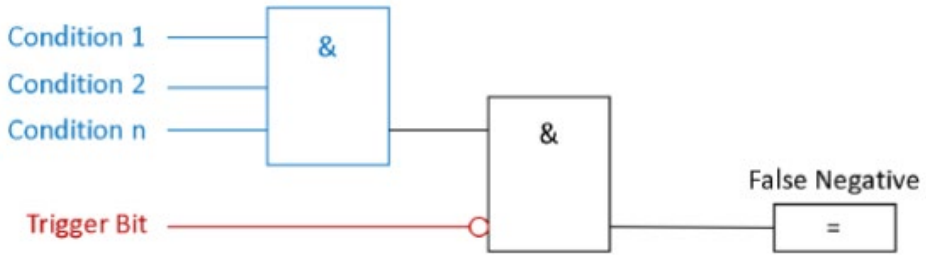
Anleitung

In den meisten Fällen sind Warnungszustände boolesch (True, False) und werden durch bestimmte Bedingungen ausgelöst, wie unten dargestellt. Z.B. wird das Trigger-Bit für den Alarm 'Überdruck' TRUE, wenn Bedingung 1 'Druckschalter 1', Bedingung 2 'Drucksensorwert über kritischer Schwelle' bis n. TRUE sind.



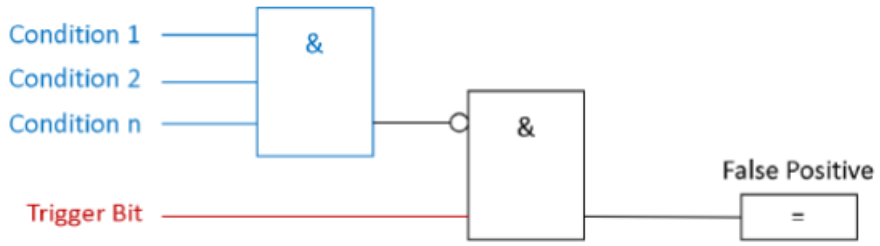
Um einen Angriff zu verschleiern, könnte ein Angreifer das Alert-Trigger-Bit unterdrücken und ein falsch negatives Ergebnis verursachen.

Ein Trap für falsch negative Ergebnisse überwacht die Bedingungen für das Trigger-Bit und das negierte Trigger-Bit selbst. Mit diesem einfachen Aufbau wird ein falsch negatives Ergebnis erkannt. Siehe das folgende Bild:



In anderen Fällen könnte ein Angreifer absichtlich Fehlalarme verursachen, um die Aufmerksamkeit des Prozessbedieners zu beeinträchtigen.

Auf die gleiche Weise wie bei der Falsch-Negativ-Falle können auch Falsch-Positive erkannt werden, indem das Alarm-Trigger-Bit überwacht wird und ob die Trigger-Bedingungen erfüllt sind. Wenn die Bedingungen NICHT erfüllt sind, aber das Trigger-Bit aktiv ist, wird ein falsch positives Ergebnis erkannt: Siehe folgendes Bild:



Beispiel

Beispiel 1: Siemens bietet in seinen Siemens S7-1200/1500 Produkten einen Webserver mit einer Vielzahl von Funktionen, wie z.B. Anzeige des SPS-Zustands, der Zykluszeit oder der Umfangsdatensätze. Es hat auch die Möglichkeit, Datentabellen und Variablen anzuzeigen und zu ändern. Die Zugriffsrechte auf den Webserver können in den SPS-Hardware-Einstellungen geändert werden. Bei falsch konfigurierten Zugriffsrechten könnte sich ein Angreifer Zugriff auf die SPS-Variablen und Datenblöcke verschaffen. Um ein falsch positives Ergebnis zu erzeugen, wählt der Angreifer ein Alert-Trigger-Bit aus und ändert den Zustand.

Beispiel 2: Bei der Triton/Trisys/HatMan-Attacke unterdrückte bösartiger Code die Warnzustände.

Beispiel 3: Ein Bus-Injection-Angriff könnte eine falsch positive Warnung an einen übergeordneten SCADA-Client senden.

Begründung

Vorteilhaft für	Begründung
Sicherheit	Mindert falsch negative oder falsch positive Ergebnisse kritischer Warnmeldungen, die durch einen Angreifer verursacht werden, der seinen Angriff verschleiert (z. B. nicht autorisierter Code, Bus-Injection, Manipulation von zugänglichen SPS-Statustabellen auf ungesicherten Webservern).
Zuverlässigkeit	/
Instandhaltung	/

Referenzen

Standard / Framework	Mapping
MITRE ATT&CK für ICS	**Taktik :** TA0107 Inhibit Response Function **Technik:** T0878 Alarm Suppresion, T0838 Modify Alarm Settings
ISA 62443-3-3	**SR 3.5**: Eingabe-Validierung
ISA 62443-4-2	**CR 3.5**: Validierung der Eingaben
ISA 62443-4-1	**SI-1**: Überprüfung der Sicherheitsimplementierung
MITRE CWE	**CWE-754:** Unsachgemäße Prüfung auf ungewöhnliche oder außergewöhnliche Bedingungen

Sichere SPS-Codierungspraktiken: Top-20 Liste

Version 1.0 (15. Juni 2021/Deutsch 28.März 2024)

Über das Projekt "Sichere SPS-Programmierung"

Seit vielen Jahren sind speicherprogrammierbare Steuerungen (SPS) von Haus aus unsicher. Nach mehreren Jahren der Anpassung und Anwendung von Best Practices aus der IT entstanden sichere Protokolle, verschlüsselte Kommunikation, Netzwerksegmentierung usw. Bisher wurde jedoch nicht darauf geachtet, die charakteristischen Merkmale von SPS (oder SCADA/DCS) für die Sicherheit zu nutzen oder SPS unter Berücksichtigung der Sicherheit zu programmieren. Dieses Projekt – inspiriert von den bestehenden Secure Coding Practices für die IT – füllt diese Lücke.

Wer sollte die Secure PLC Coding Practices lesen und implementieren?

Diese Praktiken wurden für Ingenieure geschrieben. Das Ziel dieses Projekts ist es, Ingenieuren, die Software (Kontaktplanlogik, Funktionsdiagramme usw.) erstellen, Richtlinien zur Verfügung zu stellen, um die Sicherheitslage industrieller Steuerungssysteme zu verbessern. Diese Praktiken nutzen die nativ verfügbaren Funktionen in der SPS/DCS. Für die Implementierung dieser Praktiken sind wenig bis gar keine zusätzlichen Softwaretools oder Hardware erforderlich. Sie alle lassen sich in den normalen SPS-Programmier- und Betriebsablauf integrieren. Für die Umsetzung dieser Praktiken ist mehr als Sicherheitsexpertise erforderlich, sondern auch eine gute Kenntnis der zu schützenden SPSen, ihrer Logik und des zugrunde liegenden Prozesses.

Was ist der Geltungsbereich dieser Liste / wie definiert man SPS-Codierung?

Um in den Umfang der Liste der 20 besten sicheren SPS-Codierungspraktiken zu passen, müssen die Praktiken Änderungen beinhalten, die direkt an einer SPS vorgenommen werden. Was Sie in diesem Dokument sehen, ist eine Top-20-Auswahl einer größeren Anzahl potenzieller sicherer SPS-Codierungspraktiken. Es gibt auch zusätzliche Entwurfspraktiken, die sich auf die Gesamtarchitektur, HMIs oder die Dokumentation beziehen. Diese passen nicht in den Bereich der sicheren SPS-Codierung, könnten aber auf einer zukünftigen Liste für sichere SPS-Umgebungen stehen.

Was sind die Vorteile der Anwendung von Secure PLC Coding Practices?

Die Verwendung dieser Praktiken hat eindeutig Sicherheitsvorteile – in der Regel wird entweder die Angriffsfläche reduziert oder eine schnellere Fehlerbehebung ermöglicht, wenn ein Sicherheitsvorfall auftreten sollte. Viele Praxen haben jedoch über die Sicherheit hinaus weitere Vorteile. Einige machen den SPS-Code auch zuverlässiger, einfacher zu debuggen und zu warten, einfacher zu kommunizieren und möglicherweise auch schlanker. Darüber hinaus helfen die sicheren SPS-Codierungspraktiken nicht nur den Benutzern im Falle eines böswilligen Angreifers, sondern machen den SPS-Code auch robuster, um versehentlichen Fehlkonfigurationen oder menschlichem Versagen standzuhalten.

Wer steckt hinter diesem Projekt?

Angefangen hat alles mit Jake Brodskys S4x20-Vortrag "Secure Coding Practices for PLC's".

Im Anschluss an die Konferenz initiierte Dale Peterson das Top-20-Projekt. Jake Brodsky und Sarah Fluchs verbrachten mehrere Stunden am Telefon, um Jakes vorgeschlagene sichere SPS-Codierungspraktiken zu Papier zu bringen.
Danach richteten Dale, Jake und Sarah mit Unterstützung der ISA GCA eine Plattform bei top20.isa.org ein, um zu strukturieren und zusätzlichen Input aus den ICS-Sicherheits- und Ingenieursgemeinschaften zu sammeln.

Die Diskussionen und die Konsolidierung der Praxistexte sowie die Zusammenstellung einer Liste der relevantesten Top-20-Praxen dauerten etwa ein Jahr; Der Prozess wurde

Deutsche Übersetzung:

Rudolf Preuß Koordinator IT/OT

rudolf.preuss@actemium.de

Actemium Controlmatic West GmbH

www.actemium.de