xtechnik
VORSPRUNG DURCH KNOW-HOW

AUTOMATION

DAS FACHMAGAZIN FÜR MASCHINENBAU, ANLAGENBAU UND PRODUZENTEN | 7/NOV. 24 | AUTOMATION.AT

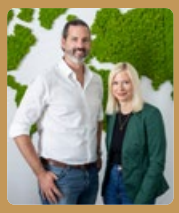
Special
sps
123 – 157

Österreichische Post AG – MZ 02Z034671 M – x-technik GmbH, Schöneringer Str. 48, 4073 Wilhering

KUKA

AUTOMATISIERTER FORTSCHRITT AUF DER BAUSTELLE 10

SPS-SPECIAL 123 – 157
Vom 12. bis 14. November öffnen sich die Messetore der SPS in Nürnberg. Einen Einblick in die Messe-Highlights haben wir im Special zusammengestellt.



DOPPELINTERVIEW 92
Energiemonitoring und Energieeffizienz sind das A und O der Industrie. Microtronics weiß, worauf es dabei ankommt und diskutierte im #VIDEOCAST-Gespräch die Herausforderungen.

Es stellt sich die Frage, welche Methoden es konkret gibt, um eine dynamische Bedrohungslandschaft und ihre Risiken in den Griff zu bekommen. Die Antwort wäre ein ganzheitliches Risikomanagement, bestehend aus proaktivem Monitoring und kontinuierlicher Risikobeurteilung mitsamt Milderungsmaßnahmen.

Andreas Willert, BSc MSc Head of Industrial Security bei Pilz Österreich

AKTIVES GANZHEITLICHES RISIKOMANAGEMENT

Bedrohungslage versus Sicherheitsgegenmaßnahmen: Nichts ist so beständig wie der Wandel (Heraklit von Ephesus) – dies gilt auch zweieinhalbtausend Jahre später in der IT- und OT-Security. Kaum glaubt man, die Risiken in den Griff bekommen zu haben, tauchen noch kreativere Angriffsmethoden und neue Schwachstellen auf, die die eigene Produktion und Produkte gefährden. Ein kontinuierliches Monitoring ist essenziell, um Informationen zu erhalten. Und es bedarf technischer und organisatorischer Maßnahmen für den eigenen Betrieb. Mit ganzheitlichem Risikomanagement lassen sich die in einer dynamisch bewegenden Bedrohungslandschaft befindlichen Ziele im Visier behalten, meint Andreas Willert, BSc MSc, Head of Industrial Security bei Pilz Österreich.

Wie wird die bestehende OT eines Betreibers oder die neu zu entwickelnde Maschine/Anlage eines Herstellers sicher im Sinne von „secure"? Sowohl bei bestehenden Topologien – sei es eine existierende Maschine oder eine bestehende Produktion – als auch bei Neuentwicklungen: Es ist nicht mehr zeitgemäß, Systeme als – vom Rest der Welt unabhängige Inseln – zu entwickeln und im Anschluss die Security „drüberzustülpen". Die internationale Normenreihe der IEC 62443 „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme" gibt ganzheitliche Herangehensweisen technischer und organisatorischer Art, sowohl für Hersteller und Integratoren als auch für Betreiber, vor.

Normen und Gesetze

Unabhängig von Normen und Good-Practices sowie gesetzlich-extrinsischer Motivation zur Anwendung dieser, wird folgend ein Mindset adressiert. Zweifelsfrei gilt dies nicht für alle Unternehmen, dass die Prioritäten in der Instandhaltung einer Produktionsinfrastruktur und in der Entwicklung einer neuen Maschine/Anlage liegen und dass die Anforderungen hinsichtlich Betriebsfähigkeit, Funktionalität und Leistung kostenoptimiert erfüllt werden sollen. Die Mechanik soll mit geringstmöglichem Material- und Fertigungsaufwand den zu erwartenden Lasten standhalten können. Dies gilt analog auch für die Elektrik, die Automatisierung, die Software u.v.m. Sofern etablierte Vorgänge bestehen, auf denen eine Evolutionsstufe aufbaut, soll möglichst viel Bestand übernommen werden. Frei nach dem Motto „Never touch a running system" gilt dies oftmals nicht nur bei Betreibern/Endanwendern, sondern auch bei Entwicklungen. In Folge bleibt es bei einer flachen Netzwerkstruktur, Default-Passwörtern und bei Konfigurationsfehlern, die niemand hinterfragt.

Hinterfragen ist das, was einen weiterbringt

Mechanik-Entwickler fragen sich, wie sie das Bauteil noch leichter/fertigungseinfacher/günstiger gestalten können. Automatisierungsspezialisten fragen sich, wie sie den Prozess optimieren können. Die Aufzählung lässt sich beliebig fortsetzen. Doch wer fragt sich Folgendes: „Wenn jemand von einem Tag auf den anderen ‚böse' wird, wie könnte die Person in mein System eindringen und was könnte sie mit dem Zugang oder Daten anstellen? Welcher (maxi- >>

Security-Risikobeurteilungen sind komplexer als Safety-Risikobeurteilungen, da sie eine breitere und dynamischere Bedrohungslandschaft berücksichtigen müssen. (Bild: Stock-Illustration/antoniokhr)

male) Schaden könnte verursacht werden? Welcher Schaden könnte bei meinen Zulieferern oder Kunden passieren, für den ich dann verantwortlich bin?" Dies sind zentral wichtige Fragen. Zweifelsfrei stehen dahinter demnächst gesetzliche sowie vertragliche Anforderungen und es ist die Essenz des Risikomanagements aus zahlreichen Normen und Good-Practices. Vor allem ist es auch eine Denkweise, die einen ständig begleiten sollte. Idealerweise lassen sich Gefährdungsereignisse als Business-Cases mit monetärem Verlust darstellen. Erst dann ist es möglich die Risiken zu bewerten, die von Angriffsvektoren oder Schwachstellen ausgehen und die individuellen Assets – gleich ob digital oder physisch – gefährden. Im darauffolgenden Schritt kann man es wagen, diese Risiken zu bewerten, zu priorisieren und danach zielgerichtete Milderungsmaßnahmen umzusetzen. Im vorläufig letzten Schritt werden die Maßnahmen validiert – bis ein Trigger auslöst, der den Prozess von vorne startet. Solch ein Trigger ist beispielsweise eine Änderung der Bedrohungslage, eine politische Änderung gegenüber dem Unternehmen, die Erweiterung des Portfolios oder Kundenkreises. Erst dann kennt man die verbleibenden Risiken und die Einschätzung darüber, wie schwerwiegend die Folgen sein könn(t)en.

An Cyber-Risiken kann man sich nicht nur die Finger verbrennen

Risikomanagementgrundsätze, Risikomanagementmaßnahmen, Risikoanalyse und Risikobeurteilung – gleich ob NIS2, Cyber Resilience Act oder Maschinenverordnung: Security Risk Assessments sind überall grundlegende Anforderungen. Dabei ist es essenziell, die vorhin ausgeführten Gefährdungsereignisse und Risiken zu kennen. Insbesondere für Industrieunternehmen, die bei funktionaler Maschinensicherheit im Sinne von Safety zwar routiniert sind, bisher aber keine intrinsische oder gesetzlich induzierte Notwendigkeit hatten, IT- und OT-basierte Risiken zu beurteilen, ist dies eine sogenannte „neue Realität". Und: Security-Risikobeurteilungen sind meist aufwendiger als Safety-Risikobeurteilungen. Das liegt an der Komplexität und Vielfalt der Risiken. In der Safety liegen in der EN ISO 12100 Beispiele für Gefährdungsereignisse vor – weder vollständig noch priorisiert, doch ist die Richtung der Betrachtung und Denkweise erkennbar.

Angriffsmethodiken

Es gilbt unterschiedlichste mechanische, elektrische, thermische Gefährdungen sowie Gefährdungen durch Lärm und Strahlung als übergeordnete Gruppen. Aus der Perspektive der Security betrachtet könnte man beispielsweise bei einem Frequenzumrichter und dessen Steuerung Folgendes fragen: Was gilt es hier zu bewerten/schützen (= Asset)? Wichtig sind das Programm, die Firmware, der Prozess selbst, die Datenflüsse, die Logs etc. Welchen Bedrohungen ist man in Folge ausgesetzt? Die Anwendung des Akronyms S.T.R.I.D.E. ist dabei international üblich. Es steht für Spoofing (Identitätsverschleierung), Tampering (Manipulation), Repudiation (Nichtanerkennung), Information disclosure (Veröffentlichung von Informationen), Denial of Service (Verweigerung des Dienstes) sowie Elevation of privilege (Erhöhung von Rechten). Zudem gibt es noch 47 elementare Gefährdungen der IT-Grundschutz-Methodik des deutschen Bundesamtes für Sicherheit in der Informationstechnik. Und das ist nicht alles. Die Common Attack Pattern Enumeration and Classification (CAPEC) von MITRE, ebenfalls branchenweit anerkannt, umfasst derzeit 559 Angriffsvektoren. Davon werden mindestens 46 „Attack Pattern" direkt industriellen Steuerungssystemen zugordnet.

Komplexität beachten

Security-Risikobeurteilungen sind komplexer als Safety-Risikobeurteilungen anzusehen, da sie eine breitere und dynamischere Bedrohungslandschaft berücksichtigen müssen. Die Breite spiegeln die Assets, Bedrohungen und Schwachstellen wider. Die Dynamik wird beeinflusst durch die Gefahr von un-/absichtlichen, zufälligen/böswilligen Korrumpierungen/Angriffen gepaart mit der Unvorhersehbarkeit und der vorherrschenden Vielfalt. Die Bedrohungslandschaft erfordert daher eine kontinuierliche Überwachung und Anpassung der Sicherheitsmaßnahmen. Security-Risikobeurteilungen müssen zudem oft komplexe IT-Infrastrukturen und Netzwerke miteinbeziehen, was zusätzliche technische Expertise und Ressourcen erfordert.

Automatisiertes versus manuelles Risikomanagement

Mit „Security ist ein moving target" wurde ich des Öfteren zitiert. Es stellt sich die Frage, welche Methoden es konkret gibt, um diese dynamische Bedrohungslandschaft und

die Risiken in den Griff zu bekommen. Die Antwort wäre ein ganzheitliches Risikomanagement, bestehend aus proaktivem Monitoring und kontinuierlicher Risikobeurteilung mitsamt Milderungsmaßnahmen. Dies kann man als vierphasigen Regelkreis beschreiben, bei dem die Phasen miteinander in Verbindung stehen. Und: Ein Asset Inventory, oder das darauf aufbauende Asset Management, sind nicht mit ganzheitlichem Risikomanagement gleichzusetzen. Dies ist eines der ersten Schritte und ein Teilgebiet eines ganzheitlichen Risikomanagements.

Erste Phase

Die erste Phase ist eine Datenerfassung in Form eines aussagekräftigen Asset Inventory. Das reicht von manuellen Prozessen mittels Schaltplänen und Tabellenkalkulationsprogrammen über Traffic-Capture mit Analyse- und Export-Scripts bis hin zu Asset Management-Lösungen, die das Netzwerk scannen und überwachen. Für Maschinentopologien, die nicht verändert werden, mag ein Tabellenkalkulationsprogramm auf den ersten Blick akzeptabel wirken. Allerdings müssen neu entdeckte Schwachstellen manuell recherchiert, zugewiesen und das Risiko neu beurteilt werden. Diese kontinuierlich durchzuführenden Nacharbeiten resultierten bei manuellen Tools in massivem Aufwand.

Zweite Phase

In der zweiten Phase ist die Topologie zu modellieren. Aus der Inventarauflistung wird eine Art Landkarte, in der ersichtlich wird, welche Komponenten über welche Protokolle miteinander kommunizieren. Möglich ist die statische Modellierung ebenso mit Office-üblichen Tools. Asset Management Tools können hierbei deutlich komfortabler unterstützen, jedoch bieten auch diese meist keine Möglichkeit, die Architektur mitsamt Konsequenzen im Zuge von Risikomilderungsmaßnahmen zu remodellieren und vorausblickend neu zu beurteilen.

Dritte Phase

Die dritte Phase ist die Risikobeurteilung. Es werden Angriffswege ermittelt, analysiert und beurteilt sowie die Auswirkungen und das Schadensausmaß bei erfolgreicher Korrumpierung festgestellt. Bei nicht akzeptablen Risiken werden Milderungsmaßnahmen im Modell implementiert, die Angriffsvektoren erneut beurteilt und das gemilderte Risiko quantifiziert sowie dokumentiert. Schon wenige Geräte ergeben viele Hunderte Risiken. Die Automatisierung dieser Phase trägt am wesentlichsten zur Effizienzsteigerung bei und ist daher von immensem Wert.

Vierte Phase

In der vierten Phase widmet man sich der Überwachung, was die Ermittlung von Zuständen, Kommunikationen, Auslastungen, also Operabilität im Allgemeinen, beinhaltet. Zusätzlich zu den operativen Kennwerten wird kontinuierlich die Angriffsoberfläche im Auge behalten. Als Erweiterung zu generischen Bedrohungen und Schwachstellen werden bei der Überwachung reale Exploits aus Datenbanken, auch gegebenenfalls aus im Darknet umlaufenden Informationen, auf die individuell im Einsatz befindlichen Komponenten übertragen. So wird ein reales Bedrohungsbild dargestellt, das stets mit den Risikobeurteilungen abgeglichen wird. Industrial Security Risk Assessments können schon bei einer Hand voll Geräten sehr umfangreich werden.

www.pilz.at