Cybersicherheit industrieller Anlagen

Internationale Partnerbehörden veröffentlichen Grundsatzpapier zur OT- Cybersicherheit

Der sichere Betrieb von Prozessleit- und Automatisierungstechnik (Operational Technology, OT) stellt Organisationen vor große Herausforderungen hinsichtlich der Cybersicherheit — auch, weil sie häufig sehr lange Lebenszyklen hat, und insbesondere, wenn sie in kritischen Infrastrukturen eingesetzt wird. Dabei ist ihre Bedeutung aus Sicht des BSI nicht zu unterschätzen: OT-Produkte tragen dazu bei, die Sicherheit von Menschen, Produktionsanlagen und nicht zuletzt der Umwelt zu gewährleisten.

©greenbutterfly - stock.adobe.com

Kritische Infrastrukturen sind für die Aufrechterhaltung und Verbesserung unserer Lebensweise unverzichtbar. Die Betriebstechnologie (OT) innerhalb unserer kritischen Infrastruktur kontrolliert viele wichtige Dienste wie das Wasser, das wir trinken, die Energie, auf die wir angewiesen sind, und die Transportmittel, die uns alle bewegen. Berichten zufolge nehmen weltweit böswillige Cyberaktivitäten gegen OT-Ressourcen zu.

Das Australian Cyber Security Centre hat gemeinsam mit internationalen Partnerbehörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) das Dokument „Principles of Operational Technology Cyber Security“ veröffentlicht. Das englischsprachige Dokument hilft Betreibern mit grundsätzlichen Fragestellungen und hat zum Ziel, den Betrieb von OT resilienter zu gestalten und ist kostenlos verfügbar.

> *Die steigende Tendenz, OT stärker zu vernetzen, erfordert eine Vorstellung von potenziellen Cyber-Angriffsszenarien.*

Sechs Grundsätze für die OT-Cybersicherheit

Die steigende Tendenz, OT stärker zu vernetzen, erfordert neben dem Verständnis für die Systeme, Prozesse und deren Integration in eine bestehende Infrastruktur auch eine Vorstellung von potenziellen Angriffsszenarien. Aus Sicht des BSI ist es zwingend notwendig, dass OT-spezifische Notfallpläne und Playbooks in andere Notfall- und Krisenmanagementpläne sowie Business-Continuity-Pläne von Organisationen integriert werden. Da in der OT zunehmend auch IT-Komponenten aus der Office-IT eingesetzt werden, ist von einem ähnlich hohen Gefährdungsgrad auszugehen. Jedoch weist die OT gegenüber der klassischen IT wesentliche Unterschiede auf, die es erschweren, etablierte Sicherheitsverfahren anzuwenden.

Die sechs Grundsätze für die OT-Cybersicherheit sollen Betreiber unterstützen, fundierte und umfassende Entscheidungen zu treffen, um die Sicherheit und Kontinuität des Geschäftsbetriebs bei der Planung, Implementierung und Verwaltung von OT-Systemen sicher zu stellen. Sie sollen alle Mitarbeitenden einer Organisation ansprechen – unabhängig davon, ob es sich um operative, taktische oder strategische Entscheidungen handelt. Mithilfe der Grundsätze kann OT-Cybersicherheit ganzheitlich gestaltet werden. Die Grundsätze zur Schaffung und Aufrechterhaltung einer sicheren OT-Umgebung lauten:

- Safety (Funktionale Sicherheit) ist oberstes Gebot
- Profunde Kenntnisse der Geschäftsprozesse und Technik sind entscheidend
- OT-Daten sind äußerst wertvoll und müssen geschützt werden
- OT muss von allen anderen Netzwerken segmentiert und getrennt sein
- Die Lieferkette muss sicher sein
- Menschen mit ihrer Erfahrung und Expertise sind für die Cybersicherheit in der OT unerlässlich.

Safety ist oberstes Gebot

Stellen Sie sicher, dass das System sicher ist! Funktionale Sicherheit ist in physischen Umgebungen von entscheidender Bedeutung. Dazu gehören die Sicherheit von Menschenleben, die Sicherheit von Anlagen, Geräten und der Umwelt sowie die Zuverlässigkeit des Prozesses. Safety und Cybersecurity müssen Hand in Hand gehen, denn funktionale Sicherheit kann durch Cybereingriffe kompromittiert werden.

Die NAMUR hat dazu bereits in 2017 das NA163 „IT-Risikobeurteilung von sicherheitsrelevanten PLT-Einrichtungen“ veröffentlicht, welches sich in der Folge zum Referenzdokument für Betreiber und Behörden entwickelt hat. Im November 2024 wurde in einer überarbeiteten Fassung auch die Bewertung von Systemen, deren Logiksysteme (Controller, SSPS) oder Programmiergeräte (Engineering Station) sowohl für betriebliche Automatisierungstechnik als auch für funktionale Sicherheit (SIL1 – SIL3) genutzt werden, integriert. Das Arbeitsblatts soll so ein hinreichendes Niveau an Cyberresilienz für Safety-Systeme sicherstellen, eine IT-Risikobeurteilung für einen Betrieb auch ohne spezielle Cybersecurity-Expertise innerhalb eines Tages sowie den Nachweis der Konformität zu TRBS 1115-1 und KAS 51 ermöglichen.


© BSI

Die Cybersicherheitslage stets im Blick: Im 24/7-Betrieb werden im Nationalen IT-Lagezentrum im BSI aktuelle Beobachtungen und Vorkommnisse der Cybersicherheitslage aufgenommen und bewertet. Es verfügt jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland, um den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen sowohl auf staatlicher Ebene als auch in der Wirtschaft schnell und kompetent einschätzen zu können.

Profunde Kenntnisse der Geschäftsprozesse

Kennen und schützen Sie wichtige Systeme! Wenn ein Unternehmen das Geschäft kennt und weiß, wie Prozesse funktionieren, wo Verbindungen sind und welche Teile kritisch sind, kann es die effektivsten Cybersicherheitskontrollen und Reaktionsmöglichkeiten für die verfügbaren Ressourcen entwickeln und implementieren. Unternehmen sollten in der Lage sein, wichtige Systeme zu identifizieren und eine Architektur zu haben, die sie schützt, sowie einen Wiederherstellungsprozess einbinden, der die erforderlichen Geschäftsergebnisse erzielen kann.

OT-Daten schützen

OT-Daten sind äußerst wertvoll und müssen geschützt werden! Für einen böswilligen Cyberakteur ist das Wissen, wie ein System eingerichtet ist, wie das Netzwerk aufgebaut ist, wie die Controller konfiguriert sind, welche Anbieter und Geräte verwendet werden und mit welchen Protokollen sie kommunizieren praktisch wie eine Schatzkarte, um Schaden anrichten zu können. Setzen Sie Prozesse ein, um den Zugriff auf und die Verbreitung von OT-Daten zu minimieren und gleichzeitig die Integrität der OT-Daten sicherzustellen.

Segmentieren und trennen

Segmentieren und trennen Sie OT von allen anderen Netzwerken! Halten Sie alle Hintertüren geschlossen! Die Segmentierung und Trennung von Netzwerken – einschließlich Peers, IT und dem Internet – wird seit langem als eine der wichtigsten Möglichkeiten zur Reduzierung des Cyberrisikos in OT-Umgebungen empfohlen. Neben den eher traditionellen Aspekten der physischen und logischen Trennung gehören dazu auch die Zuweisung von Verwaltungs- und Managementrollen in OT-Umgebungen. Unternehmen sollten das Risiko einer unzureichenden Trennung von Verwaltungs- und Managementsystemen und -diensten in OT-Umgebungen regelmäßig bewerten.

> *Die sechs Grundsätze für die , OT-Cybersicherheit sollen Betreiber unterstützen, die Sicherheit von OT-Systemen zu erhöhen.*

Die Lieferkette muss sicher sein

Sichern Sie die Cyber-Lieferkette! Die Sicherheit der Lieferkette geht über Software und Geräte von großen Anbietern hinaus. Berücksichtigen Sie alle Software, Geräte und Managed Service Provider in OT, einschließlich deren Support, Management und Wartung, vom Einkauf und der Integration bis hin zur Außerbetriebnahme und Entsorgung.

Menschen sind für die OT-Cybersicherheit unverzichtbar

Menschen mit ihrer Erfahrung und Expertise sind die erste Verteidigungslinie! Ein Cyber-bezogener Vorfall in OT kann nicht rechtzeitig verhindert, abgewehrt, identifiziert, beantwortet und behoben werden, ohne dass Menschen mit den erforderlichen Tools und der erforderlichen Schulung danach suchen und in der Lage sind, kompetent darauf zu reagieren. Eine Investition in Personal, um ein kollaboratives Team aus geschulten und qualifizierten Mitarbeitern mit den erforderlichen Tools aufzubauen, unterstützt durch eine ausgereifte und organisationsweite Cybersicherheitskultur, ist für die Cyberabwehr eines Unternehmens von großer Bedeutung.

> *Die Cyber-Bedrohungslage bleibt angespannt, aber die Resilienz gegen Angriffe steigt.*

BSI-Bericht zur Lage der IT-Sicherheit in Deutschland

Die Bedrohungslage bleibt angespannt, aber die Resilienz gegen Angriffe steigt Das ist das Resümee des BSI in seinem Lagebericht im November 2024. Danach bleibt Ransomware weiterhin die größte Bedrohung im Cyberraum. Zugleich stellen sich Staat, Wirtschaft und Gesellschaft stärker als bisher auf die Bedrohungen ein und haben ihre Resilienz erhöht.

Im Berichtszeitraum von Mitte 2023 bis Mitte 2024 wurden täglich durchschnittlich 309.000 neue Schadprogrammvarianten bekannt – das entspricht einem Anstieg von 26 % im Vergleich zum Vorjahr. Besonders Android-Schadprogrammvarianten legten im Berichtszeitraum überdurchschnittlich zu.

Die Zahl der Opfer von Datenleaks nach Ransomware-Angriffen ist weiter gestiegen. Gleichzeitig ist der Anteil der Ransomware-Opfer, die Lösegeld bezahlen, gesunken. Betroffene, die über funktionierende Sicherungskopien (Back-ups) ihrer Daten verfügen, sind nicht auf die Entschlüsselung ihrer Systeme durch die Angreifer angewiesen. Zudem gehen immer mehr Unternehmen transparent mit Cyberangriffen um, informieren die Öffentlichkeit und ihre Kunden. Dies trägt dazu bei, dass potenzielle Schwachstellen schneller geschlossen und Schäden von weiteren Unternehmen abgewendet werden können.

Vor dem Hintergrund geopolitischer Konfliktlagen sind professionelle und oftmals staatlich gelenkte Angriffe durch APT-Gruppierungen (Advanced Persistant Threats) weiterhin zu beobachten. So hat Cyberspionage zum Nachteil von Behörden, Parteien, politischen Institutionen und Unternehmen an Bedeutung gewonnen.

Cybersicherheit von Wahlen

Im Jahr 2024 haben weltweit mehr als 70 Wahlen stattgefunden. Für deutsche Staatsbürger standen die Europawahl, drei Landtagswahlen und neun Kommunalwahlen an. Diese Wahlen sind ohne nennenswerte Cybersicherheitsvorfälle abgelaufen. Mit Blick auf anstehende Wahlen findet derzeit eine angepasste und situativ verstärkte Lagebeobachtung statt. Das BSI steht in kontinuierlichem Austausch mit seinen Partnerbehörden und ist in die Strukturen der Bundesregierung zum Schutz von Wahlen eingebunden. Zudem unterstützt das BSI Wahlbehörden und politische Zielgruppen durch Beratungsangebote zur Sensibilisierung für Informationssicherheit.

Volker Oestreich, CHEManager

■ www.bsi.bund.de

Herausforderungen in der Prozessautomatisierung sind komplexer und vernetzter geworden

NAMUR Hauptsitzung 2024: Agilere und intelligentere Produktionsprozesse

Die NAMUR Hauptsitzung 2024 am 21. und 22. November in Neuss stand unter dem Thema “Boundless Automation for Ecosystems in Action” – und im Zeichen von personellen Veränderungen im Vorstand. Nach sieben Jahren als Vorstandsvorsitzender der NAMUR übergab Felix Hanisch, Bayer, sein Amt an Tobias Schlichtmann, BASF. Die NAMUR hat unter Hanisch wegweisende Impulse in der Prozessautomatisierung gesetzt und die Zusammenarbeit innerhalb der Branche sowie mit Partnerorganisationen auf ein neues Level gehoben. Mit Tobias Schlichtmann übernimmt ein erfahrener Branchenexperte, der die digitalisierte Automatisierung in der Prozessindustrie weiter vorantreiben wird. Dem neuen NAMUR Vorstand gehören auch Carlos Hedler (Bayer), Nils Kiupel (Evonik), Sebastian Mahler (Covestro), Rene Neijts (Dow) und Michael Pelz (Heubach) an.

In seinem Plenarvortrag stellte Peter Zornio, CTO von Emerson, mit „Boundless Automation“ die Vision einer Automatisierungsarchitektur der nächsten Generation vor, mit der Datensilos beseitigt, eine einfache Bereitstellung von Software und KI-Anwendungen ermöglicht und so für einen agilen und leistungsstarken Betrieb gesorgt werden soll. Indem der Wert von OT-Daten voll ausgeschöpft wird, können Unternehmen die scheinbar widersprüchlichen Ziele von Produktion, Kosten, Zuverlässigkeit und Nachhaltigkeit balancieren und optimieren.

Process-X und KI

In Datenräumen können Unternehmen und Organisationen Daten miteinander austauschen und gemeinsam nutzen, ohne die Kontrolle über ihre eigenen Daten zu verlieren. So werden kooperative Geschäftsmodelle möglich. Process X ist der Datenraum für die Prozessindustrie; er kann z.B. als Grundstein für vernetztes Energiemanagement dienen und einen wichtigen Beitrag zur Erreichung der Klima- und Energieziele liefern.

Die Digitalisierung der Produktion steht vor der Herausforderung, KI sinnvoll zu integrieren und Anlagen im Zuge der ökonomischen und demografischen Herausforderungen möglichst autonom und vollautomatisch zu betreiben. Über das „Ob“ und „Wie“ sind die Meinungen noch geteilt, aber in einem Jahr wird man dazu weiter sein: Die NAMUR Hauptsitzung 2025 findet am 27. und 28. November unter dem Leitthema „Milestones towards Autonomous Plants“ wiederum in Neuss statt; Sponsor der Veranstaltung ist Krohne Messtechnik. (vo) ■