Analyse von Cybersicherheitsbedrohungen in modernen elektrischen Steuerungssystemen

28.02.2025, 11:00 Uhr
Kommentare: 0
Sicher arbeiten



Die Komplexität moderner Steuerungssysteme erfordert einen proaktiven Ansatz in der Cybersicherheit. (Bildquelle: : PUGUN SJ/iStock/Getty Images Plus)

Die zunehmende Digitalisierung und Vernetzung von industriellen Steuerungssystemen stellt Elektrofachkräfte vor neue Herausforderungen im Bereich der Cybersicherheit. Industrial Control Systems (ICS) und Distributed Control Systems (DCS) sind zentrale Bestandteile kritischer Infrastrukturen – von der Energieversorgung über die Wasseraufbereitung bis hin zur industriellen Fertigung. Diese Systeme wurden ursprünglich für maximale Zuverlässigkeit entwickelt, jedoch nicht mit Blick auf moderne Cyberbedrohungen. Das Ergebnis ist eine große Angriffsfläche, die durch veraltete Protokolle und fehlende Sicherheitsmechanismen begünstigt wird.

Versteckte Schwachstellen in ICS- und DCS-Systemen

Elektrofachkräfte müssen sich der Tatsache bewusst sein, dass ICS- und DCS-Komponenten häufig mit Standardbenutzernamen und -passwörtern ausgeliefert werden, die Angreifer leicht kompromittieren können, wenn Verantwortliche der Anlagen sie nicht ändern. Da diese Systeme in der Regel nicht mit herkömmlicher Endgeräteschutz- oder Firewall-Software kompatibel sind, ist eine robuste Netzwerkarchitektur von entscheidender Bedeutung. Netzwerksegmentierung, zum Beispiel durch VLANs oder Software-defined Networks, minimiert das Risiko unbefugter Zugriffe. Sinnvoll ist ein Zero-Trust-Ansatz, der grundsätzlich keinem Benutzer und keinem Gerät vertraut und ständige Überprüfungen erfordert.

Ein weiteres Risiko liegt in der Verwendung veralteter Kommunikationsprotokolle wie Modbus und DNP3, die ursprünglich nicht für sicherheitskritische Anwendungen entwickelt

wurden. Diese Protokolle bieten keine integrierten Verschlüsselungs- oder Authentifizierungsmechanismen und sind daher anfällig für Man-in-the-Middle-Angriffe. Elektrofachkräfte sollten sich der Notwendigkeit bewusst sein, solche Protokolle entweder durch sicherere Alternativen zu ersetzen oder durch zusätzliche Schutzmaßnahmen abzusichern.

Zunehmende Bedrohung durch gezielte Angriffe

Die steigende Anzahl von Cyberangriffen auf OT-Systeme verdeutlicht die Dringlichkeit. Angriffe erfolgen häufig über Phishing-Kampagnen oder unsichere Fernzugriffe und können schwerwiegende Folgen wie Produktionsausfälle, die Zerstörung von Anlagen oder sogar die Gefährdung von Menschenleben haben. Die Bedrohung durch spezialisierte Malware wie Triton oder Industroyer nimmt zu und unterstreicht die Notwendigkeit einer kontinuierlichen Überwachung und schnellen Reaktionsfähigkeit.

Ein besonders gefährliches Szenario ist der Einsatz von Ransomware in OT-Umgebungen. Während solche Angriffe in IT-Systemen „nur“ zu Datenverlusten führen, können sie in industriellen Steuerungssystemen physischen Schaden anrichten, indem Maschinen manipuliert oder Produktionsprozesse gestört werden. Elektrofachkräfte sollten daher in der Lage sein, sowohl vorbeugende Maßnahmen zu ergreifen als auch Notfallpläne für den Ernstfall zu entwickeln.

Tipp der Redaktion



Sicheres Arbeiten an elektrischen Anlagen

- E-Learning-Kurs für Fachkräfte der Elektrotechnik
- Mit Wissenstest und Teilnahmebestätigung
- Sorgen Sie für ein sicheres elektrotechnisches Arbeiten in Ihrem Betrieb.

Jetzt mehr erfahren

Technische Schutzmaßnahmen

Verantwortliche für solche Anlagen sollten deshalb nicht nur technische Schutzmaßnahmen umsetzen, sondern auch ein tiefes Verständnis für die Sicherheitsarchitektur entwickeln. Ein vollständiges und aktuelles Asset-Register ist die Basis für ein effektives Schwachstellenmanagement. Ein solches Verzeichnis sollte sicher gespeichert und regelmäßig aktualisiert werden, um Manipulationen frühzeitig zu

erkennen. Die Integration von Bedrohungsdatenbanken speziell für ICS- und DCS-Umgebungen hilft, aktuelle Angriffsmuster zu erkennen und gezielte Abwehrstrategien zu entwickeln.

Darüber hinaus sollten Intrusion Detection Systems (IDS) und Intrusion Prevention Systems (IPS) in industrielle Netzwerke integriert werden, um verdächtige Aktivitäten frühzeitig zu erkennen und abzuwehren. Diese Systeme lassen sich speziell an die Anforderungen von OT-Umgebungen anpassen, um Fehlalarme zu minimieren und gleichzeitig eine hohe Sensibilität für Bedrohungen zu gewährleisten.

Die Rolle der Zusammenarbeit von IT und OT

Ein weiteres zentrales Element ist die enge Zusammenarbeit zwischen IT- und OT-Teams. Unterschiedliche Prioritäten und technologische Anforderungen führen häufig zu Kommunikationsproblemen. IT-Teams konzentrieren sich in der Regel auf den Schutz von Daten und Netzwerken, während OT-Teams der Geschäftskontinuität und der Sicherheit physischer Prozesse Priorität einräumen. Diese unterschiedlichen Perspektiven können zu Konflikten führen, wenn die Sicherheitsstrategien nicht aufeinander abgestimmt sind.

Fachkräfte, die ein Verständnis für beide Bereiche mitbringen, können als Brücke fungieren und zur Entwicklung ganzheitlicher Sicherheitsstrategien beitragen. Dabei ist es wichtig, nicht nur auf technische Lösungen zu setzen, sondern auch das Sicherheitsbewusstsein im Unternehmen zu stärken. Regelmäßige Schulungen und Sensibilisierungsmaßnahmen sind entscheidend, um menschliche Fehler zu minimieren, die nach wie vor eine der größten Schwachstellen darstellen.

Proaktive Cybersicherheitsstrategien in der Praxis

Die Komplexität moderner Steuerungssysteme erfordert einen proaktiven Ansatz in der Cybersicherheit. Mitarbeiter, die in der Lage sind, Risiken zu erkennen, Schutzmaßnahmen zu implementieren und schnell auf Sicherheitsvorfälle zu reagieren, sind für den Schutz kritischer Infrastrukturen unverzichtbar. Durch kontinuierliche Weiterbildung und den Einsatz spezialisierter Sicherheitslösungen können sie einen entscheidenden Beitrag zur Resilienz von Unternehmen leisten.

Wichtige Elemente eines proaktiven Ansatzes sind regelmäßige Sicherheitsüberprüfungen, Penetrationstests und die Simulation von Angriffsszenarien. Diese Maßnahmen helfen, Schwachstellen zu identifizieren und die Wirksamkeit bestehender Sicherheitsstrategien zu überprüfen. Darüber hinaus sollten Notfallpläne und Wiederherstellungsstrategien entwickelt werden, um im Falle eines Angriffs schnell reagieren zu können.

Downloadtipps der Redaktion

E-Book: Prüfprotokolle für die Elektrofachkraft

Hier gelangen Sie zum Download.

E-Book: Haftung der Elektrofachkraft

Hier gelangen Sie zum Download.

Mess- und Prüfprotokoll

Hier gelangen Sie zum Download.

Gefährdungsbeurteilung: Gefahrenarten (Gefährdungsfaktoren)

Hier gelangen Sie zum Download.

Wichtige Aspekte bei der Absicherung von DCS-Systemen

Gerade in DCS-Umgebungen, die aufgrund ihrer verteilten Architektur oft schwer zu überblicken sind, ist eine systematische Sicherheitsstrategie notwendig. Die Vielfalt der verwendeten Protokolle wie Modbus, DNP3 oder proprietäre Lösungen erschwert die Standardisierung von Schutzmaßnahmen. Verantwortliche sollten sicherstellen, dass alle Schnittstellen von den Feldgeräten bis zu den HMI-Workstations auf Sicherheitslücken überprüft und abgesichert werden.

Besonderes Augenmerk ist auf die Engineering-Arbeitsplätze zu legen, da Änderungen in der Steuerungslogik direkte Auswirkungen auf den Produktionsprozess haben können. Hier sind strenge Zugriffskontrollen und Protokollierungen erforderlich, um unbefugte Manipulationen zu verhindern. Auch Historian-Server, die Prozessdaten speichern, müssen vor Angriffen geschützt werden, da manipulierte Daten zu Fehlentscheidungen im Betrieb führen können.

Sicherheitsaspekte bei der Nutzung von Cloud-Services

Mit der zunehmenden Integration von Cloud-Diensten in industrielle Steuerungssysteme entstehen neue Angriffsvektoren. Daten, die zwischen lokalen Steuerungssystemen und Cloud-Servern ausgetauscht werden, müssen verschlüsselt und durch strenge Zugriffskontrollen gesichert werden. Besondere Vorsicht ist bei der Fernüberwachung und -steuerung von Anlagen über das Internet geboten. Verantwortliche sollten darauf achten, dass sichere Protokolle verwendet und unsichere Verbindungen vermieden werden.

Ein weiterer kritischer Punkt ist die Verwaltung von Zugriffsrechten in Cloud-Umgebungen. Es muss sichergestellt werden, dass nur autorisierte Personen Zugriff auf sensible Steuerungsdaten haben und die Berechtigungen regelmäßig überprüft werden. Der Einsatz von Multi-Faktor-Authentifizierung kann hier zusätzliche Sicherheit bieten.

Ausblick: neue Herausforderungen und neue Technologien

Die fortschreitende Entwicklung von Technologien wie dem industriellen Internet der Dinge (Industrial Internet of Things, IIoT) und der künstlichen Intelligenz bringt sowohl Chancen als auch Risiken für die Cybersicherheit in industriellen Steuerungssystemen mit sich. Während IIoT die Effizienz und Transparenz in der Produktion erhöht, vergrößert es

gleichzeitig die Angriffsfläche. KI-gestützte Systeme können helfen, Anomalien frühzeitig zu erkennen und Sicherheitsvorfälle schneller zu identifizieren.

Elektrofachkräfte sollten sich kontinuierlich mit diesen neuen Technologien auseinandersetzen und deren Sicherheitsimplikationen verstehen. Die Kombination aus traditionellem technischen Wissen und dem Verständnis moderner IT-Technologien wird entscheidend sein, um den steigenden Anforderungen an die Cybersicherheit gerecht zu werden.

Cybersicherheit in der Automobilindustrie: Schutz von Steuergeräten

Die Prinzipien und Strategien der Cybersicherheit, die für industrielle Steuerungssysteme entwickelt wurden, lassen sich auch auf andere Branchen übertragen, die von vernetzten Steuerungssystemen abhängig sind. Ein besonders relevantes Beispiel ist die Automobilindustrie, die mit der zunehmenden Vernetzung von Fahrzeugen und der Verbreitung von Elektrofahrzeugen vor ähnlichen Herausforderungen steht.

Mit der zunehmenden Verbreitung von Elektrofahrzeugen und vernetzten Fahrzeugen hat die Cybersicherheit in der Automobilindustrie eine neue Dringlichkeit erreicht. Fahrzeuge sind heute mobile IP-Adressen und damit potenzielle Angriffsziele. Die elektronischen Steuergeräte (ECU) steuern zentrale Fahrzeugfunktionen und sind ohne geeignete Sicherheitsmaßnahmen anfällig für Manipulationen. Elektrofachkräfte, die in der Automobiltechnik tätig sind, müssen die besonderen Herausforderungen verstehen, die mit der Absicherung dieser Systeme verbunden sind.

Die Integration von Hardware-Sicherheitsmodulen (HSM) bietet einen wirksamen Schutz gegen unbefugten Zugriff. Diese Module ermöglichen die sichere Speicherung von Schlüsseln und die Authentifizierung von Kommunikationsnachrichten im Fahrzeugnetzwerk. Moderne Fahrzeuge verwenden CAN-FD-Protokolle, deren Nachrichten durch kryptografische Verfahren geschützt werden können. Die Kombination von Digital Signal Controllers (DSC) mit Sicherheits-ICs gewährleistet, dass kritische Steuerungsfunktionen vor externen Eingriffen geschützt sind.

Bei Cyberattacken versuchen Angreifer häufig, durch gezielte Befehle die Kontrolle über das Fahrzeug zu übernehmen, indem sie beispielsweise den Motor abstellen oder die Geschwindigkeit unkontrolliert erhöhen. Ohne geeignete Sicherheitsmechanismen könnten solche Angriffe zu gefährlichen Situationen im Straßenverkehr führen. Der Einsatz von Echtzeitüberwachung und Authentifizierungsverfahren verhindert solche Manipulationen, indem verdächtige Befehle erkannt und blockiert werden.

Hier ist es entscheidend, die spezifischen Anforderungen automobiler Steuerungssysteme zu verstehen und geeignete Schutzmaßnahmen zu implementieren. Die Einhaltung von Standards wie AUTOSAR und die Verwendung von Sicherheitsframeworks sind wesentliche Elemente, um die Integrität und Sicherheit moderner Fahrzeuge zu gewährleisten.

Darüber hinaus sollten Over-the-Air-(OTA-)Update-Mechanismen mit sicheren Authentifizierungs- und Verschlüsselungsverfahren integriert werden, um Manipulationen der Fahrzeugsoftware zu verhindern. Angesichts der zunehmenden Vernetzung von Fahrzeugen ist es für Elektrofachkräfte unerlässlich, sich mit den neuesten Entwicklungen im Bereich der Cybersicherheit von Fahrzeugen vertraut zu machen und sich kontinuierlich weiterzubilden.

Weitere Beiträge zum Thema

Künstliche Intelligenz (KI)

KI-Verordnung (AI-Act): Anwendungsbereich und verbotene KI-Anwendungen

KI-Verordnung (AI-Act): Das sollten auch Elektrofachkräfte wissen

Einsatz von Augmented Reality bei Wartung und Prüfung von Schaltanlagen

Einsatz von Künstlicher Intelligenz zur Fehlerdiagnose in elektrischen Anlagen

Autor:

Thomas Joos

freiberuflicher Publizist



Thomas Joos ist freiberuflicher Publizist und veröffentlicht neben seinen Büchern auch Artikel für verschiedene Medien wie dpa, Computerwoche und C't.

Seit seinem Studium der medizinischen Informatik berät er auch Unternehmen im Bereich IT, Security und Absicherung von Rechenzentren.