Neue Regeln, bekannte Maßnahmen

Security for Safety: Wie Betreiber ihre Systeme gegen Cyberattacken absichern können

In Sachen Cybersicherheit von automatisierten Systemen sorgt die TRBS 1115-1 (Technische Regel Betriebssicherheit) seit einigen Monaten für Gesprächsstoff unter Sicherheitsexperten. Dabei ist die neue Regel lediglich ein anderer Blickwinkel auf die Cybersicherheit von OT-Systemen – und die Maßnahmen gegen Hackerangriffe bleiben dieselben.

Die im März 2023 veröffentlichte TRBS 1115-1 „Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen“ schlug hohe Wellen. Nicht etwa, weil das Regelwerk an sich besonders viel Neues in Sachen Cybersicherheit forderte – diese ist längst Gegenstand vieler Vorschriften und Normen. Die Aufregung war deshalb groß, weil eine große zugelassene Überwachungsstelle (ZÜS) in der Folge Sicherheitsbeauftragte dazu aufgefordert hatte, durch Unterschrift zu bestätigen, dass die Dokumentation zur Durchführung von Cybersicherheitsmaßnahmen durch die ZÜS eingesehen werden kann.

Technische Maßnahmen alleine reichen nicht aus – auch die Organisation muss gehärtet werden.

Erwin Kruschitz, Anapur

Betriebe und die für Sicherheitsmaßnahmen zuständigen Personen in der Chemie sehen sich in Sachen Cybersecurity inzwischen einer ganzen Reihe an Anforderungen aus verschiedenen Regelwerken gegenüber. Aus Sicht der Kommission für Anlagensicherheit (KAS) nennt der seit November 2019 gültige Leitfaden KAS51 die Grundpflichten im Hinblick auf die Störfallverordnung, um Eingriffe Unbefugter als Gefahrenquelle zu berücksichtigen – darunter auch Gefahren durch Cyberangriffe und Drohnen. IEC 61511 beschreibt die funktionale Sicherheit von sicherheitsinstrumentierten Systemen (SIS) für die Prozessindustrie und fordert IT- Risikobeurteilungen für PLT Sicherheitseinrichtungen. Wie das geht, hat die NAMUR im Arbeitsblatt NA 163 beschrieben. Und schließlich ist da noch die Sicht des Gesetzgebers in Form der Richtlinie (EU) 2016/1148 zur Netzwerk- und Informationssicherheit (NIS-Richtlinie), die in 2023 von der EU als (EU) 2022/2555 neu gefasst wurde (NIS-2) und die bis Oktober 2024 in nationales Recht umgesetzt werden soll.

Ein Problem – unterschiedliche Perspektiven

Im Fall der Cybersicherheit kristallisieren sich erst nach und nach Checklisten und Prüfprozedere heraus – allerdings unter unterschiedlichen Prämissen. So fordern zugelassene Überwachungsstellen heute zum Teil die Dokumentation der Cybersicherheit von Sicherheitseinrichtungen auf Basis einzelner Sicherheitsfunktionen – analog zur in der funktionalen Sicherheit gängigen Praxis, wonach SIL-Werte für einzelne Sicherheitskreise berechnet werden. Das hat bspw. zur Folge, dass ein Logic Solver (Sicherheitssteuerung), der 100 Sicherheitsfunktionen steuert, auch 100-mal geprüft werden muss – eine im Hinblick auf die Cybersicherheit wenig sinnvolle Vorgehensweise.

Dabei wollen alle Beteiligten eigentlich das Gleiche: Die Cybersicherheit industrieller Anlagen stärken. Und um dies zu erreichen, gilt es nach wie vor, die wichtigsten Grundregeln zu beachten, die für Betreiber von Prozessanlagen im aktuellen NA 163 beschrieben sind. Zu den wesentlichen Grundregeln gehören organisatorische und technische Maßnahmen und eine dreistufige Vorgehensweise.

Risiken bewerten, Zonen definieren, Maßnahmen ergreifen

An der ersten Stelle steht die Bewertung von Risiken: Wie wahrscheinlich ist es, dass ein Cyberangriff Einrichtungen der funktionalen Sicherheit betreffen bzw. beeinträchtigen kann? An zweiter Stelle steht Zoneneinteilung, die allerdings mit fortschreitender Digitalisierung zwischen Automatisierungsstruktur und Sicherheitssystemen nicht mehr scharf getrennt ist. Und an dritter Stelle folgen Maßnahmen gegen Cyberbedrohungen.

Zu den technischen Maßnahmen gehört bspw. die Netzwerksegmentierung: Dabei wird der Zugriff auf Sicherheitseinrichtungen beschränkt, indem das PLT-Netzwerk in verschiedene Segmente unterteilt wird. Weil in einem segmentierten Netzwerk nur wenige Geräte und Systeme für Angreifer zugänglich sind, wird es diesen erschwert, Schwachstellen zu finden und auszunutzen. Dadurch wird die Angriffsfläche kleiner und die Ausbreitung der Angriffe wird begrenzt. Zudem kann der Datenverkehr in segmentierten Netzen einfacher überwacht werden, sodass sich verdächtige Aktivitäten schneller erkennen lassen.

Zwischen den Netzwerksegmenten sowie nach außen hin dienen Firewalls dazu, den Zugriff auf Sicherheitseinrichtungen zu kontrollieren. So bleibt der Zugriff auf ein Netzwerk oder auf Systeme im Netzwerk auf bestimmte IP-Adressen oder Ports beschränkt, wodurch Hacker daran gehindert werden, auf ungeschützte Geräte oder Dienste zuzugreifen. Firewalls können zudem den Datenverkehr filtern – bspw. indem bekannte Exploits (Angriffswerkzeuge) oder Angriffssignaturen erkannt werden, und sie können bei verdächtigen Aktivitäten warnen. Moderne Firewalls können auch situationsspezifisch Kommunikationsverbindungen freischalten oder sperren und erzielen folglich einen enormen Sicherheitsgewinn.

Weitere technische Maßnahmen sind die Verschlüsselung von Datenverbindungen zu Sicherheitseinrichtungen sowie die Zugangskontrolle: Der Zugriff auf Sicherheitseinrichtungen sollte durch starke Authentifizierung und Autorisierung beschränkt werden. Und schließlich dürfen auch Softwareupdates nicht vergessen werden – denn die Auswertung von Schadensereignissen durch Cyberangriffe zeigt, dass Sicherheitslücken in der eingesetzten Software häufig das Einfallstor für Angreifer sind. Je länger eine Sicherheitslücke bekannt ist, desto größer ist die Gefahr, dass Angreifer diese auch ausnutzen.

Maßnahmen können selbst zum Einfallstor werden

In der Praxis wird in diesem Zusammenhang häufig unterschätzt, dass jede Maßnahme wiederum Risiken birgt: Sei es das Patchen von Software, das Key- und User-Management, die Administration der Firewall, Datenmonitoring, Log- oder Incident-Management – jede Maßnahme erfordert den Zugriff auf oder durch die Firewall und schafft wiederum Einfallstore für Angriffe. Und je mehr Softwarekomponenten eine Sicherheitsfunktion enthält, desto größer die Exposition gegenüber Cyberangriffen.

In Sachen Cybersecurity gibt es eine ganze Reihe an Anforderungen aus verschiedenen Regelwerken.

Spätestens hier wird deutlich, dass technische Maßnahmen alleine nicht ausreichen – auch die Organisation muss „gehärtet“ werden: Dies geschieht in erster Linie durch das Schulen der Mitarbeiter, die mit Sicherheitseinrichtungen arbeiten. Und nicht zu vergessen: Unternehmen und die für die Sicherheit der OT-Systeme zuständigen Mitarbeiter sollten auch für den Fall der Fälle Vorsorge treffen. Dazu hilft es, einen sog. „Incident-Response-Plan“ zu erstellen, in dem niedergelegt wird, was im Falle eines Cyberangriffs geschehen soll.

Enthaltsamkeit zahlt sich aus

Interessant ist im Zusammenhang mit Sicherheitsmaßnahmen gegen Cyberangriffe, dass in der Öffentlichkeit sehr viel über organisatorische und noch viel mehr über technische Maßnahmen diskutiert wird, aber die wichtigste Maßnahme überhaupt wenig populär ist: der Verzicht. Die günstigste und erste Maßnahme sollte es immer sein, Geräte und Systeme zu härten. Da – wie oben gezeigt – jede Software und jede Verbindung nach draußen ein Sicherheitsrisiko darstellt, das mit Maßnahmen reduziert werden muss, hilft es, auf alle Soft- und Hardwarekomponenten sowie auf Dienste zu verzichten, die nicht unbedingt benötigt werden. So sollten sich Anlagenbetreiber bspw. fragen, ob Software aus der Office-Welt auf eine Engineering-Workstation des Safety-Systems gehört. Von USB-Verbindungen und permanent offenen Fernwartungsverbindungen ganz zu schweigen. Letztere sollten allenfalls temporär im Wartungsfall freigeschaltet werden.

In diesem Zusammenhang ist eine akribische Bestandsaufnahme des Safety-Inventars – ob Soft- oder Hardware – wichtig. Denn nur was bekannt ist, kann gehärtet oder gepatcht werden. NA 163 enthält eine Checkliste, die verwendet werden kann, um die Wirksamkeit der getroffenen Schutzmaßnahmen zu beurteilen und den Aufwand für die Risikoanalyse zu reduzieren, sodass ein Risk Assessment in der Regel in einem Tag durchgeführt werden kann.

Den Cyber-Reifegrad in zehn Minuten bestimmen

Um den Reifegrad der eigenen Organisation im Hinblick auf Cyberbedrohungen in kürzester Zeit zu bestimmen, empfiehlt Anapur einen einfachen Test, dessen vier Schritte verantwortliche Manager in weniger als zehn Minuten durchführen können:

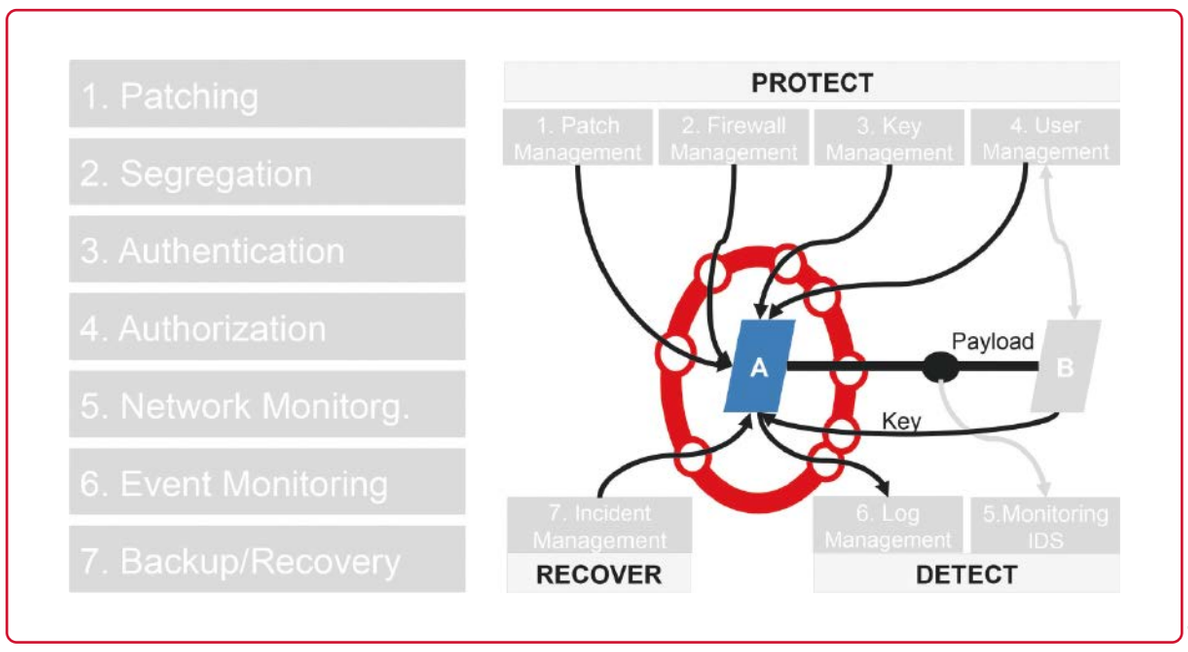
- 1. Fordern Sie ihre Mitarbeiter auf, sich vorzustellen, dass es einen Angriff gab, der Umwelt- und Gesundheitsschäden hervorrufen könnte.
- 2. Lassen Sie die Frage beantworten, wer dafür verantwortlich ist, so einen Vorfall zu managen, d.h., die Produktion zu stoppen, oder Kommunikationsverbindungen nach draußen zu kappen.
- 3. Messen Sie die Zeit, wie lange es dauert, bis Sie die richtige Antwort erhalten.
- 4. Berechnen sie den Reifegrad (Maturity Level): ML = 5 - t, wobei t die Zeit bis zur Antwort in Minuten ist. Je höher der resultierende ML, desto höher der Reifegrad der Organisation.

Fazit

Ob TRBS 5111-1, KAS 51, IEC 61511 oder NIS – die aktuellen Vorschriften zielen darauf, die Sicherheit von Automatisierungssystemen und Systemen der funktionalen Sicherheit gegenüber Cyberangriffen zu stärken. Auch wenn sich Interpretation und Prüfpraxis unterscheiden – zum Schluss sind es dieselben Maßnahmen, die zu einer größeren Resilienz gegenüber Bedrohungen und Angriffen von Hackern führen. Eine praktikable Vorgehensweise für die in der Prozessindustrie eingesetzten Einrichtungen der funktionalen Sicherheit beschreibt das NAMUR Arbeitsblatt NA 163, welches demnächst in der Version 2.0 erscheinen wird.

Erwin Kruschitz,
CEO, Anapur AG, Frankenthal

- www.anapur.de
- e.kruschitz@anapur.de



Auch Maßnahmen zur Sicherung von automatisierungstechnischen Komponenten können wiederum zu einem Sicherheitsrisiko werden, weil sie den Zugriff durch eine Firewall verlangen.