Keine Angst vor der Maschinenverordnung

Security einfacher als gedacht?

Bild 1: Sieben Maßnahmen der IEC 62443 mit der die notwendigen Safety Level erreicht werden können. © Indu-Sol

Autoren:
Dipl.-Ing. (FH) Nora Crocoll;
Dipl.-Wirt. Ing. Alex Homburg
Redaktionsbüro Stutensee
http://www.rbsonline.de

Indu-Sol GmbH
info@indu-sol.com
www.indu-sol.com

Security ist ein Thema, das den Maschinenbau seit einiger Zeit aufwirbelt, insbesondere mit Blick auf das Inkrafttreten der Maschinenverordnung am 20.1.2027. Viele sind verunsichert, sehen für die OT-Netzwerkkommunikation herausfordernde Maßnahmen auf sich zukommen und horrende Kosten. Beides kann sich der Maschinenbau hierzulande nicht leisten, will er weiter wettbewerbsfähig bleiben. René Heidl von Indu-Sol zeigt sich von diesem Wirbel überrascht. Er sieht dabei nicht viel „Neues unter der Sonne“, sondern vielmehr die umfangreichen Erfahrungen, an die der Maschinenbau anknüpfen kann. Betrachte man das Thema genauer und aus der richtigen Perspektive, seien in vielen Fällen die Lösungen ebenso einfach wie kostengünstig.

Ziel von Security-Maßnahmen

Was ist das Ziel von Security-Maßnahmen, die in der Maschinenverordnung, dem Cyber Resilience Act oder NIS2 gefordert werden? Viele denken schnell an den Schutz vor russischen Hackerangriffen oder Ähnlichem; also an hochkompetente Angreifer mit einer hohen Motivation, Schaden anzurichten. Dieses Szenario führt zu Angst und diese eher zu einem Erstarren als zu positivem Handeln. Ein genauerer Blick in die Maschinenverordnung zeigt allerdings, dass diese Angst in der Regel unbegründet ist, weil sie den Großteil der Maschinenbauer nicht betrifft.

Raus aus der Kaninchenstarre

Das Thema Security ist an sich nichts Neues. Ähnliches hat der Maschinenbau bereits erlebt in Bezug auf die elektrische Sicherheit von Maschinen oder die Safety von Industrieanlagen. Bevor es hier rechtliche Vorgaben gab, wurde elektrische Sicherheit bzw. Safety bei der Entwicklung von Maschinen und Anlagen kaum berücksichtigt. Es kam zu Schäden, Verletzungen oder gar Todesfällen. Diese führten einerseits zu Forderungen von Ausgleichszahlungen, andererseits aber auch zur Verbesserung der Sicherheit. Diese wurde unter anderem von Versicherungen vorangetrieben, deren Interesse am Auszahlen von Schadensersatzzahlungen naturgemäß gering ist. Es entstand über Richtlinien, Gesetze und Verordnungen ein Stand der Technik, an den sich Maschinenbauer fortan halten mussten.

Risikobetrachtung

Eine Risikobetrachtung in Bezug auf die elektrische Sicherheit oder die Safety einer Maschine oder Anlage zum Abschätzen benötigter Schutzmaßnahmen ist für einen Maschinenbauer heute nichts Fremdes, ebenso wie das Einhalten von Performance Leveln (PL a bis e) oder Safety Integrity Leveln (SIL 1 bis 4). Sehr ähnlich verhält es sich im Grunde ab Januar 2027 mit den Security Leveln. Bislang führten mangelnde Security-Maßnahmen nicht zu rechtlichen oder finanziellen Konsequenzen bei Maschinenbauern. Die Versicherungen übernahmen die Schadensersatzzahlungen.

Bild 2: René Heidl, Geschäftsführer Technik & Entwicklung bei der Indu-Sol GmbH. „Die Angst vor der Maschinenverordnung halte ich für überzogen. Oft sind die notwendigen Security Level deutlich geringer, als befürchtet.“ © Indu-Sol

Mit Inkrafttreten der Maschinenverordnung tun sie das nur noch dann, wenn der Maschinenbauer nachweisen kann, dass er in Bezug auf seine Security-Maßnahmen nicht grob fahrlässig gehandelt hat. Das schafft ein Maschinenbauer aber leichter als gedacht.

Security Level verstehen

Auch in Bezug auf die Security steht eine Risikobewertung am Anfang und zwar nach der IEC 62443. Diese ermittelt ein Target Security Level (SL-T), also das Schutzniveau, das von dem System mindestens gefordert ist. Ähnlich wie beim SIL definieren auf der anderen Seite Hersteller für ihre Komponenten eine Security-Level-Capability (SL-C), also welches Niveau die Komponente in Bezug auf Security erreichen kann. Dann schlägt die IEC 62443 sieben Maßnahmen vor, mit deren Hilfe die geforderten Security-Level erreicht werden können (Bild 1). Die Komponente allein muss es allerdings nicht „richten", sondern sie ist wiederum Teil des gesamten Systemdesigns (Achieved Security Level – SL-A), das ebenfalls Einfluss nehmen kann auf die Security. Kurz gesagt:Der geforderte Target-Security-Level muss vom Achieved-Security-Level abgedeckt werden. Die Komponente spielt dabei eine wichtige, aber nicht die einzige Rolle. René Heidl (Bild 2) fragt: „Was ist denn aber, wenn der geforderte Security-Level deutlich geringer ist, als viele denken? Das eingangs beschriebene Szenario mit den russischen Hackern wäre ein SL 4, die meisten Anwendungen in der Industrie fordern aber höchsten SL 2, manche vielleicht auch SL 3 wie die SL-Grafik in Bild 3 zeigt."

SL 2 als Beispiel

Betrachten wir dazu den SL 2 anhand eines Beispiels. Hier geht es um den „Schutz vor vorsätzlichem Missbrauch" mit folgendem Angreiferprofil: Angreifer mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und niedriger Motivation. „Welchen Grund hätte ein Angreifer, z. B. die Temperatur eines Kessels aufwändig aus einem SPS-Protokoll auszulesen?", fragt Heidl und antwortet gleich darauf: „Vielleicht, um die Temperatur zu manipulieren und damit die Produktionscharge zu zerstören? Aber was hätte er davon? Davon mal abgesehen, gelänge ihm das nicht mit einfachen Mitteln. Er müsste einen Spiegelport an einem Switch einrichten können und sich dann per Wireshark einhacken, um den Datenverkehr auszulesen und anschließend zu manipulieren. Das macht man nicht mit allgemeinen Fähigkeiten, geringen Ressourcen und einfachen Mitteln. Und andersrum gesagt: Wer über die nötigen Mittel verfügt, hätte keinerlei Interesse am Angriff, weil es keinen Nutzen bringt." Die meisten Industrieanlagen sind vor diesem Hintergrund für externe Hacker schlicht uninteressant. Anders sieht das aus, wenn man zum Beispiel wertvolle Rezepte, personenbezogene Daten oder dergleichen stehlen kann. Aber dieses Problem betrifft nur den kleinsten Teil industrieller Anlagen.

Bild 3: Überblick über die Safety-Level und jeweiligen Angreiferprofile © KI-generiertes Bild - ChatGPT, 2026

Schlimmster anzunehmender SL 2-Angreifer

Ohnehin wäre das Absichern eines Angriffs von außen Sache derjenigen, die die Lösung für den Fernzugriff bereitstellen, nicht der internen Netzwerkkommunikation und die Connectivity von „außen" endet heute noch in 95 % aller Fälle an der SPS, ohne direkte Verbindung in das Maschinennetzwerk.

Interessanter ist es daher, einen Blick auf den schlimmsten anzunehmenden Level-2-Angreifer zu werfen. Der kommt nämlich nicht von außerhalb des Unternehmens, sondern von innen. Heidl beschreibt: „Denken Sie an einen Mitarbeiter, dem aus seiner Sicht zu Unrecht gekündigt wurde und der nun sauer ist. Ihm ist es ein Leichtes, sich über den USB-Port seines Handys, oder mit einem Laptop, ans Maschinennetzwerk anzuschließen und unbewusst (da SL 2, „allgemeine Mittel und Fähigkeiten") z. B. einen Windows-Wurm einzuschleusen, welcher den Visualisierungs-PC lahmlegt."

Anders als in der Büro-Welt ist es in der OT-Welt nämlich kaum möglich, den Zugang zum Netzwerk physisch zu unterbinden. Switches sitzen in Schaltschränken, die sich per Schaltschrankschlüssel einfach öffnen lassen (Bild 4) und an den Enden von Linien sitzen an vielen Stellen in der Maschine/Anlage, PROFINET-Geräte mit einem offenen Port. Heidl ergänzt: „Anhand des Beispiels wird deutlich, wie wenig Sinn es ergibt, in trusted zones und untrusted zones zu unterscheiden. Viel wichtiger ist es, solche Eingriffe von Internen ins Netzwerk zu erkennen und darauf rechtzeitig zu reagieren."

Bild 4: Anders als in der Büro-Welt ist es in der OT-Welt kaum möglich, den Zugang zum Netzwerk physisch zu unterbinden. © Indu-Sol

Gefahr erkannt, Gefahr gebannt?

Diese Erkenntnisse führen zu einer zweiteiligen Lösung. Erstens müssen Maschinenbauer in Bezug auf ihre OT-Netzwerkkommunikation glaubhaft nachweisen können, dass sie eine Security-Risikoanalyse durchgeführt haben, die zur Erkenntnis führt, dass im konkreten Fall z. B. ein Security Level 2 benötigt wird. „Das ist kein Hexenwerk“, berichtet Heidl. „Dennoch unterstützen wir unsere Kunden gern auch beim Erstellen des Nachweises.“ Zweitens müssen dann die notwendigen Maßnahmen umgesetzt werden.

Im beschriebenen Fall ginge es dabei um Lösungen, die den Angreifer zeitnah entdecken und aufgreifen lassen, um im besten Fall den Schaden zu vermeiden und im schlimmsten Fall für einen Schaden haftbar machen zu können. „Auch das ist leichter als gedacht“, weiß Heidl. „Ich kann ja sehr genau sagen, welche Geräte Teil meines Netzwerks sind und welche neu hinzukommen. Jeder Managed Switch hat einen Überblick über alle vergebenen MAC-Adressen im Netzwerk. Derzeit sind unsere Switches jedoch die einzigen am Markt, die eine Meldung absetzen können, wenn eine neue MAC-Adresse im Netzwerk auftaucht. Natürlich können wir das auch mit unserer Software PROmanage oder dem PROFINET-INspektor überwachen, samt weiterer interessanter Informationen.

Bild 5: Der PROmesh Diagnose-Switch ist derzeit der einzige managed OT-Switch am Markt, der eine Meldung absetzen kann, wenn eine neue MAC-Adresse im Netzwerk auftaucht. © Indu-Sol

In den meisten Fällen ist aber ein PROmesh Diagnose-Switch die ausreichende und kostengünstigste Lösung (Bild 5). Genau genommen entstehen keine zusätzlichen Kosten, weil ein Switch für die Netzwerkkommunikation ohnehin benötigt wird.“

Security einfach mal einfach

Die vorherrschende Angst in Bezug auf die Maschinenrichtlinie ist, dass eine Anlage durch die Umsetzung von Security-Maßnahmen im fünfstelligen Bereich teurer wird. Da in einem Großteil der Maschinenbauanwendungen aber keine personenbezogenen Daten oder wertvolle Informationen wie patentierte Rezepte übertragen werden, ist das meist nicht der Fall. Heidl resümiert: „Es ergibt ja keinen Sinn, eine Latzhose mit Hosenträger und Gürtel abzusichern. Wichtig ist jedoch, dass Maschinenbauer jetzt endlich aus dem Knick kommen und konkrete Lösungen entwickeln. ◄