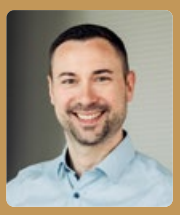
xtechnik
VORSPRUNG DURCH KNOW-HOW

AUTOMATION

DAS FACHMAGAZIN FÜR MASCHINENBAU, ANLAGENBAU UND PRODUZENTEN | 5/SEPT. 24 | AUTOMATION.AT

PILZ: WIE SICHER IST „SICHER“? 10

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



PLUG & PRODUCE MIT MTP? 24

Immer kürzere Produkt- und Innovationszyklen verlangen nach hoch automatisierten Produktionsanlagen mit maximaler Flexibilität. GF Johannes Petrowisch von Copa-Data CEE/ME erläutert den Einsatz von MTP.

LEBENSMITTELINDUSTRIE 62 – 79

Die Lebensmittelindustrie boomt und verlangt gleichzeitig den Einsatz smarter und automatisierter Lösungen. Deren Vielfalt zeigen wir im Schwerpunkt auf.

WIE SICHER IST „SICHER“?

Vollumfängliche Maschinensicherheit ist für Maschinenhersteller und -betreiber nur mit Industrial Security-Maßnahmen möglich. Diese schützen Maschinen vor möglichen Cyberangriffen, menschlicher Fehlbedienung oder gar Manipulation und werden mit der Maschinenverordnung zur Einhaltung der CE-Konformität verlangt. Doch wie stark ist die individuelle Maschine von Angriffen gefährdet? Die Frage nach geeigneten Vorsorgemaßnahmen stellt sich mehr denn je. Pilz kennt die Antworten. **Von Stephanie Englert, x-technik**

Sie erinnern sich? Vor einigen Jahren ist das Unternehmen Pilz selbst durch einen Cyberangriff massiv im täglichen Arbeitsalltag gestört worden – für mehrere Wochen. Die Lehre aus diesem unerwarteten Angriff ist nicht nur eine interne verbesserte Security, sondern auch eine massive Steigerung der Sensibilität für die Ungewissheit hinter jedem Mail, USB-Stick, SMS und mehr. Der Vorteil nach den harten, arbeitsintensiven „Wochen danach“ ist, dass jeder einzelne Pilz-Mitarbeiter inzwischen weiß, was ein Angriff durch lückenhafte Security bedeuten kann. „Das war uns nicht nur eine Lehre, sondern auch eine Verbesserung unserer eigenen Security“, hieß es vonseiten Pilz.

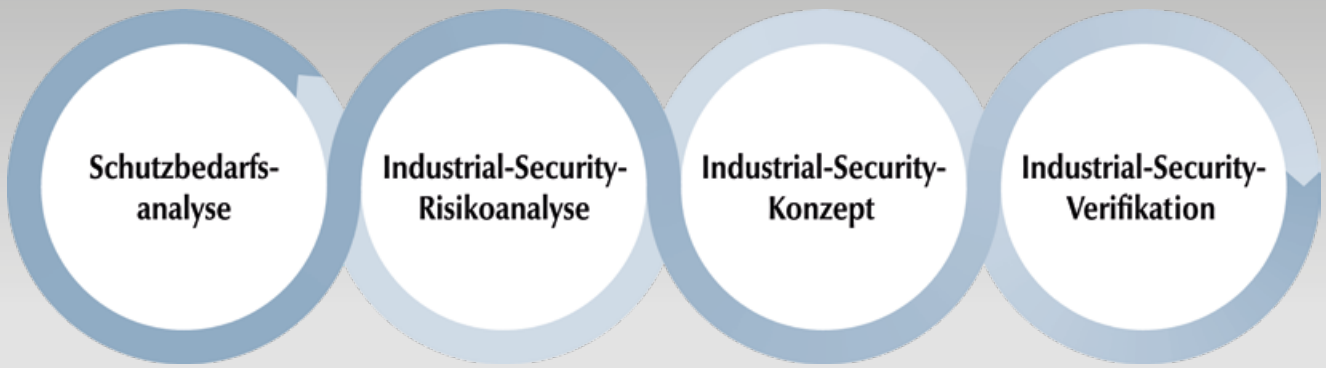
Security als „Must-have“

Was gehört also zu einer an die 100 %-Marke „kratzenden“ Top-Security für den eigenen Betrieb? Wie man am besten bei der Beantwortung dieser Fragen vorgeht, weiß Pilz wie kein anderer. Denn der Industrial Security Consulting Service (ISCS) des Automatisierungsexperten setzt genau hier an. „Wir identifizieren Gefährdungen durch Security-Schwachstellen, analysieren und beurteilen sich daraus ergebende Risiken, definieren Schutzziele, quantifizieren Security Levels, stellen passende Lösungsschritte zusammen und überprüfen die getroffenen Maßnahmen. Der ISCS erhöht dadurch die Cybersicherheit und sorgt dafür, dass Sie normative und gesetzliche Vorgaben korrekt umsetzen sowie Security-Vorfälle an der Maschine mildern und abwehren können“, betont Andreas Willert, BSc MSc Head of Industrial Security bei Pilz Österreich, der neben seiner praktischen Expertise zudem einen CMSE – Certified Machinery Safety Expert (TÜV Nord) und CESA – Certified Expert for Security in Automation vorweisen kann. Willert verstärkt seit Mai 2022 den Automatisierer Pilz in Österreich im Consulting Service und übernahm 2023 die Leitung der damals neu ins Leben gerufenen Abteilung „Industrial Security“. Er ergänzt: „Security ist kein statisches, sondern ein sich dynamisch bewegendes Ziel. Es ist nichts, was man einmal macht und dann einen Haken dahinter setzt.“

Andreas Willert, BSc MSc Head of Industrial Security bei Pilz Österreich und verantwortlich für den Industrial Security Consulting Service aus dem Consultingangebot von Pilz sieht nicht nur den Mehrwert durch eine optimierte Security.

Maßnahmenpakete schnüren

Auf der Hand liegt, dass Maschinen und Anlagen kein CE erhalten, ohne dass Security-Risiken analysiert worden sind. „Keine Safety ohne Security“ ist jedoch nur ein Teilbereich mehrerer umfassender gesetzlicher Maßnahmenpakete, wie auch Willert betont. Diese betreffen nun eine bedeutende Mehrzahl an Branchen, wie das verarbeitende/herstellende Gewerbe. Somit sind auch der Maschinenbau, Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, elektrischer Ausrüstungen sowie Hersteller von Kraftwagen, Kraftwagenteilen und sonstiger Fahrzeugbau gemeint, die zuvor keine gesetzlich induzierte Notwendigkeit betraf, Cybersecurity-Maßnahmen umzusetzen. „Diese Branchen sehen sich künftig durch die Maschinenverordnung (MVO) EU 2023/1230, dem Cyber Resiliance Act (CRA) und der Richtlinie für Netzwerk- und Informationssicherheit 2 (NIS 2) EU 2023/2555 mit erstmaligen Verpflichtungen konfrontiert“, so Willert, und genau hier greifen die Consultingmaßnahmen – von Experten für Experten.



Vier Schritte zur sicheren Maschine

Der Industrial Security Consulting Service aus dem Consultingangebot von Pilz setzt sich dabei aus vier aufbauenden Modulen zusammen. Nach Durchführung der einzelnen Schritte ist aufgrund des Moving-Target-Prinzips eine regelmäßige Neuüberprüfung des Industrial Security Status der Maschinen notwendig, um neuesten Cyberangriffmethoden oder Schwachstellen permanent entgegenzuwirken. Doch was decken die einzelnen Module ab?

» **1. Schutzbedarfsanalyse**
Schritt eins beinhaltet die Schutzbedarfsanalyse. Hier werden zunächst die geltenden Normen und Vorschriften ermittelt. Weiters findet eine Definition der Grenzen des in Betracht zu ziehenden Systems statt. Darüber hinaus werden die sogenannten Schutzziele jedes Assets des Systems anhand der zu erwartenden Schadenshöhen bei einem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit bestimmt. Der Nutzen bei diesem ersten Arbeitsschritt ist, die grundsätzliche Einschätzung des Gefahrenbewusstseins beim jeweiligen Unternehmen zu eruieren.

» **2. Industrial Security-Risikoanalyse**
Im zweiten Schritt findet eine Einschätzung des Risikoausmaßes und des jeweiligen Handlungsbedarfes statt. Die Ermittlung sämtlicher Risiken für jedes Asset innerhalb jeder Lebensphase des Systems hinsichtlich der in Betracht gezogenen Schutzziele gehört zu den Kernelementen der Analyse. Hier wird detailliert eine Analyse aller vorhandener risikosenkender Maßnahmen und deren Auswirkung durchgeführt und eine empfohlene Herangehensweise festgelegt, in dem auch die Schwachstellen dokumentiert werden und die entsprechende Gefährdung.

» **3. Industrial Security-Konzept**
Im dritten Schritt geht es darum, Gegenmaßnahmen zu planen und festzulegen, die einen möglichen Angriff bestmöglich verhindern sollen. Dabei wird etwa der Security-Level für jedes Systemteil festgelegt. Weiters werden eine Definition und Spezifikation möglicher Gegenmaßnahmen zusammengefasst, alles unter Berücksichtigung der Verfügbarkeit und Produktivität. Die detaillierte Zuordnung der Sicherheitsmaßnahmen zu den ermittelten Risiken wird ebenfalls bestimmt und die Regeln und Richtlinien für die Reduzierung des Risikos über den gesamten Maschinenlebenszyklus werden klar definiert. Im Endeffekt steht ein Konzept in Dokumentationsform dem Maschinen- und Anlagenbauer zur Verfügung.

» **4. Industrial Security System-Verifikation**
Im schließlich letzten Schritt fokussiert man sich auf die Überprüfung der Wirksamkeiten der zuvor gesetzten Maßnahmen. Hilfreich ist hierbei die Möglichkeit, einen Testbericht mit Informationen zu den Ergebnissen und eventuellen Abweichungen anzufertigen.

Doch welchen Nutzen hat der Kunde? Das liegt laut Willert auf der Hand: „Zum einen geht es um den Haftungsschutz durch die Einhaltung relevanter Security-Anforderungen, zudem um die Erhöhung des Mitarbeiterschutzes und der Anlagenverfügbarkeit sowie um die gesamte Kostenersparnis, die durch die Abwehr von Cyberattacken zu eruieren wäre. Zum anderen, und das ist nicht unwesentlich, muss auch die so genannte Imagewahrung durch die wirksam getroffenen Vorsorgemaßnahmen definiert werden." Der letztgenannte Aspekt sei dabei kein unwesentlicher, denn er garantiere schlussendlich das Vertrauen vom bzw. zum Kunden.

Consulting als wesentliche Maßnahme

Als Botschafter der Sicherheit weist das Unternehmen Pilz die Weiterentwicklung der Maschinenrichtlinie zur EU-Maschinenverordnung auf die kommenden gesetzlichen und normativen Änderungen (MVO, NIS2, CRA) und den sich daraus ergebenden Herausforderungen an Hersteller, Integratoren und Betreibern von Maschinen sowie Anlagen in die richtigen Bahnen. Jeder, der sich beraten lässt – und das zeitig – kann und wird es, ob der immens zunehmenden Cyberangriffe, nicht „bereuen", dessen sind sich nicht nur die Pilz-Experten rund um Andreas Willert gewiss. Auch Referenzkunden haben bereits in Erfahrung gebracht, dass eine zeitige Ausarbeitung der To-dos für beide Seiten von Vorteil ist.

www.pilz.at

VIDEO

Der Industrial Security Consulting Service aus dem Consulting-angebot von Pilz setzt sich dabei aus vier aufbauenden Modulen zusammen.