MEINUNGEN

INDUSTRIE 5.0: UND WAS IST MIT DER CYBERSICHERHEIT?

Khobeib Ben Boubaker
Head of Industrial Security Business Line, Stormshield

Menschlich, nachhaltig, resilient: Während sich die Industrie 4.0 bei ihrer Einführung auf die Steigerung der Produktivität mittels Big Data, IoT und intelligenten Maschinen konzentrierte, verspricht die Industrie 5.0, sich wieder auf den Menschen und die Gesellschaft zurückzubesinnen. Was bedeutet dies für die Cybersicherheit?

Zehn Jahre nach der offiziellen Einführung des Begriffs Industrie 4.0 wird mit Industrie 5.0 der Weg für eine neue industrielle Revolution bereitet. Sie konzentriert sich darauf, **den Menschen wieder in den Mittelpunkt der heute weitgehend digitalisierten industriellen Prozesse zu rücken**. Die Interaktion zwischen Mensch und Maschine setzt jedoch den Einsatz von starken Sicherheitsmaßnahmen in industriellen Umgebungen voraus. Welche Position nimmt dann die Cybersicherheit ein? Und in welchem Zeithorizont? Erfahren Sie mehr.

DIE VERHEISSUNGEN DER INDUSTRIE 5.0

Die Vorstellung, dass Maschinen und Technologien letztendlich dazu führen werden, dass der Mensch in den Fabriken und im Zentrum der industriellen Prozesse nicht länger gebraucht wird, ist heute eine überholte Vision der Industrie. Mit dem Fokus auf Produktivitätssteigerungen hatte die Industrie 4.0 das Ziel, Fabriken „*intelligent*" zu machen, indem die Produktion aus der Ferne gesteuert und überwacht werden kann.

Aber **was ist dann die Industrie 5.0?** Das neue Paradigma der Industrie 5.0 soll sich wieder mehr auf den Menschen konzentrieren. „*Der erste Schwerpunkt ist die Verbesserung der Arbeitsbedingungen von Arbeitnehmern durch neue technische Lösungen und leistungsfähige Roboter*", betont **Vincent Nicaise**, Manager für Industriepartnerschaften und das industrielle Ökosystem bei Stormshield. Er hebt noch eine weitere Dimension hervor: „*Das Ansehen der industriellen Tätigkeit in einem Kontext, der für das Thema der Reindustrialisierung in Europa günstig ist, soll wiederhergestellt werden. Es geht also auch darum, einer Branche, die seit mehreren Jahren leidet, neue Attraktivität zu verleihen, indem die Arbeitskräfte von morgen, aber auch ingenieurtechnisches Know-how angezogen werden.*" **Den Arbeitnehmern, den Unternehmen, aber auch dem Planeten zugleich zu nutzen, das ist das Credo der Industrie 5.0.** Es geht also darum, „*neue Technologien zu nutzen, um Arbeitsplätze und Wachstum zu sichern, aber auch und vor allem die Grenzen der Produktionskapazität des Planeten zu berücksichtigen*", betont **Stéphane Potier**, Leiter des Angebots für OT- & IT-Cybersecurity bei Advens. In dieser Hinsicht bildet dieses neue industrielle Paradigma den Gegenpol zum Schreckgespenst einer zu 100 % automatisierten Fabrik, die Arbeitsplätze vernichtet. Roboter werden nicht als eigenständige Einheit betrachtet und ersetzen nicht das Fachwissen des Menschen. „*Roboter sind kollaborativ – sie entlasten den Bediener bei mühsamen Aufgaben*", fährt er fort. Die Maschine soll in erster Linie dazu dienen, Bediener bei ihrer Arbeit zu unterstützen, indem sie ihnen durch die Integration von künstlicher Intelligenz, Augmented Reality, Robotik sowie IoT neue funktionelle Fähigkeiten verleiht. Die Industrie 5.0 strebt eine nachhaltige Produktion an, die dem Klimawandel Rechnung trägt und neue Kriterien, wie die Energieeffizienz von Technologien, die Priorisierung erneuerbarer Energien sowie einen Autonomieansatz, einbezieht. Die Energiefrage ist für die Industrie 5.0 von größter Bedeutung. Dabei muss nicht nur der Energieverbrauch der Maschinen, sondern auch der gesamten Produktionsanlage berücksichtigt werden. „*Die Frage der seltenen Erden, die in vielen Industriekomponenten und Maschinen enthalten sind, wird somit entscheidend sein*", erklärt Stéphane Potier. „*Beispielsweise benötigen die heute hergestellten Motoren deutlich weniger seltene Erden und werden aus leichter verfügbaren Materialien hergestellt.*"

Der Faktor der Resilienz ist auch für die Industrie 5.0 von grundlegender Bedeutung – in einem makroökonomischen und geopolitischen Kontext, der jeden Tag die Notwendigkeit zeigt, sich an Schocks anpassen zu können. Für **Marc Bagur**, Head of Human-Machine Performance bei Airudit, ist dies eine großartige strategische Chance für die Industrie. „*Diejenigen, die sich dafür entscheiden, menschlichen Werten*

den Vorrang vor Technologien zu geben, verfolgen einen ganzheitlichen Ansatz und ein langfristig erfolgreicheres Organisationsmodell." Es gehe nicht länger nur darum, das industrielle Umfeld um jeden Preis zu digitalisieren, sondern darum, „*eine systemische Robustheit anzustreben, die sozial, menschlich und ökologisch akzeptabel ist*". Er weist darauf hin, dass diese Forderung „*perfekt zu den Forderungen der neuen Generationen von Ingenieuren und Arbeitern passt, für die die Ausrichtung an ökologischen Werten, die Frage der Energieressourcen und die soziale Stabilität heute entscheidende Themen sind*".

Da der Reifegrad der verschiedenen Industriesysteme jedoch heterogen ist, bleibt es schwierig, genau abzuschätzen, wann dieses neue Paradigma tatsächlich einsatzbereit sein wird. Und die Industrie 4.0 ist noch relativ jung…

INDUSTRIE 4.0 VS. INDUSTRIE 5.0: ERSATZ ODER ERGÄNZUNG?

Industrie 5.0 stellt keine weitere Iteration im Gewaltmarsch des Fortschritts dar. **Dieses neue Paradigma ist als Ergänzung zu Industrie 4.0 zu sehen und zielt darauf ab, die Frage der technologischen Innovation in einem präzisen Rahmen wiederzugeben, der sich auf die Dreieckskonstellation aus Mensch-Nachhaltigkeit-Resilienz fokussiert**. Um dies zu erreichen, baut die Industrie 5.0 auf der Effizienz der Technologien der Industrie 4.0 auf, z. B. um Probleme im Zusammenhang mit dem Kriterium der Nachhaltigkeit zu lösen. „*Um den Energieverbrauch einer Maschine zu senken, ob neu oder alt, muss man zunächst in der Lage sein, den Verbrauch zu messen. Die Industrie 4.0 liefert uns dank Sensoren, Zählern und IoT-Systemen die nötigen Tools dafür*", betont daher Stéphane Potier. „*Ergänzend kann man versuchen, den Betrieb einer Maschine zu optimieren, die andernfalls zu viel Energie verbrauchen würde: Einerseits mit vorausschauender Wartung, um die Lebensdauer der Maschine zu beeinflussen, und andererseits mit künstlicher Intelligenz, um den Verbrauch zu optimieren*." In ihrem Bericht „*Industry 5.0 – Towards a sustainable, human centric and resilient European industry*" hebt die Europäische Kommission diese ergänzende Rolle hervor. **Es geht auch darum, auf die Schwächen der Industrie 4.0 zu reagieren, die sich bislang zu weit von den gesellschaftlichen Herausforderungen entfernt entwickelt hat.** Das Ziel ist es, Industrien aufzubauen, die nicht nur produktiv und effizient ist, sondern auch Vertrauen schaffen können – mit Werten, die denen dem Zeitgeist und den Anforderungen entsprechen, die von den neuen Generationen gestellt werden.

Wie kann die Industrie von morgen mit dieser strategischen Ausrichtung **vorbereitet werden?** Denn zwischen der Steuerung von Daten dank Big Data, präzisen Messungen dank IoT, der Vernetzung von Industriestandorten dank 5G oder auch dem Einsatz einer höheren Rechenkapazität dank Edge Computing ist die moderne Fabrik 4.0 weitgehend digitalisiert… Sie muss jedoch einen besonders komplexen makroökonomischen und geopolitischen Kontext berücksichtigen, der von steigenden Energiepreisen und der Dringlichkeit der Umweltfrage geprägt ist. **Eine industrielle Antwort auf diese zivilisatorischen Herausforderungen zu finden, erfordert deshalb, die richtigen Investitionen an den richtigen Stellen zu tätigen, aber auch die Prozesse in allen**

Phasen der Produktionskette zu überarbeiten. Für Vincent Nicaise erfordert diese Modernisierung der Industrieanlagen sowohl „*neue Kenntnisse im Zusammenhang mit technisch innovativen Protokollen und Prozessen als auch neue Kompetenzen für die Mitarbeiter, die Schlüsselakteure in der Produktionskette*“. Da die Industrie 5.0 eine neue Informationsebene einführt, weckt diese Ergänzung neue Bedürfnisse, was sich direkt auf die Frage der Personalausbildung auswirkt. „*Man kann sich dafür entscheiden, neue Stellen zu schaffen, z. B. lokale Referenten, welche die neuen Sicherheitsprotokolle an den Maschinen in den weltweit verstreuten Fabriken umsetzen, oder man kann sich dafür entscheiden, die Fähigkeiten der Bediener zu verbessern*“, so Nicaise.

Ist dies die Gelegenheit, Cybersicherheit endlich in das Herz der Industrie zu integrieren?

WELCHEN STELLENWERT HAT DIE CYBERSICHERHEIT FÜR DIE INDUSTRIE 5.0?

Im Rahmen des FIC 2022 war die Frage nach der Cybersicherheit in industriellen Umgebungen in aller Munde. **Denn eine vernetzte Fabrik bietet eine vielfach größere Angriffsfläche und birgt damit auch mehr Sicherheitsprobleme**. Schließlich bedeutet die Kombination aus einer wachsenden Zahl von Robotern, einer zunehmenden Vernetzung, der Integration von IoT, einer Dosis Augmented Reality und neuen Mensch-Maschine-Schnittstellen, dass die Zahl potenzieller Sicherheitslücken in den Systemen zunimmt.

Einem Bericht von Claroty zufolge wurden allein im Jahr 2021 82 Industrieunternehmen angegriffen. Im selben Jahr verzeichneten entdeckte Schwachstellen einen Nettozuwachs von 637 auf 787. All dies sind kritische Einstiegspunkte… Als Beispiel wird häufig ein veraltetes Betriebssystem angeführt, das auf Anlagen in Fabriken ausgeführt wird – dies ist einer der häufigsten Schwachstellenfaktoren im Bereich der industriellen Cybersicherheit. Das berühmte Windows XP ist nach wie vor ein unverzichtbares System für bestimmte industrielle Umgebungen und erfordert besondere Cybersicherheitstools, um das Risiko zu verringern. Denn die Folgen eines Cyberangriffs auf ein betriebliches Umfeld haben mannigfaltige Auswirkungen, vom vollständigen Stillstand der Produktionsketten über die Gefährdung von Arbeitnehmern bis hin zu erheblichen Auswirkungen auf den Ruf des betroffenen Unternehmens. Ganz zu schweigen vom Umweltrisiko, für das die Industrie 5.0 besonders anfällig ist.

Es stellt sich folglich die Frage: **Welche Cybersicherheitslösungen müssen eingesetzt werden, um die Industrieumgebungen der Zukunft zu schützen?** Um der Herausforderung der Sicherheit in der Industrie 5.0 zu begegnen, werden zwei Szenarien untersucht. Das erste ist ein „Revamping“-Szenario, bei dem die Produktionskette modernisiert wird, indem die Funktionen der Cybersicherheit in die Ausrüstung integriert werden. In diesem ersten Szenario ist die Installation von „*Komponenten des Typs Firewall ein gutes Mittel, um eine Segmentierung der Datenströme und Protokollanalysen vorzunehmen*“, erläutert Vincent Nicaise, ebenso wie „*die Verschärfung des Schutzes von Workstations mit großer Verstärkung durch die Verwaltung der USB-Ports, der WLAN-Netzwerke oder auch der Zugänge*“. Die Wahl von souveränen Cybersicherheitslösungen ist in diesem Zusammenhang eine Garantie

für Transparenz und verhindert, dass Daten zu böswilligen Zwecken missbraucht werden können. Solche Lösungen verfügen über einen kontrollierten, souveränen Code, der die Risiken einer Kompromittierung sowie von Angriffen aus dem Ausland abschwächt. Nur so kann eine tiefgreifende Verteidigung ohne schwache Glieder in der Kette erzielt werden. Das zweite Szenario der Industrie 5.0 betrifft neuere Geräte, die Cybersicherheit nativ integrieren. Aber dafür werden der menschliche Aspekt und der kollaborative Charakter Schlüssel sein. Über eine einfache Sensibilisierung hinaus muss bei allen neuen Projekten zwischen den Teams eine echte Zusammenarbeit aufgebaut werden. Auf der einen Seite stehen die Sicherheitsbedürfnisse der Cyber-Teams und auf der anderen Seite die betrieblichen Einschränkungen der OT-Teams. Ein notwendiger Schulterschluss, um Standpunkte auf den Prüfstand zu stellen und zu Kompromissen zu gelangen, die den Cyber- und OT-Anforderungen gerecht werden.

Vorausgesetzt, die Industrie ist auf diese cybergeschützte Industrie 5.0 vorbereitet.

INDUSTRIE DER ZUKUNFT UND CYBER-REIFE: IST DIE INDUSTRIE BEREIT?

Laut einer Studie der Firma Wavestone aus April 2023 ist die Cyber-Reife großer Organisationen in Frankreich nach wie vor gering: Nur 49 % der Befragten bezeichnen sich als reif. Ein ähnliches Ergebnis zeigt sich **allein auf der Ebene des Industriesektors, wo 49,4 % der Befragten angeben, dass sie beim Thema Cybersicherheit ausgereift sind**. Obgleich der Industriesektor im Vergleich zum Vorjahr um 4,6 Prozentpunkte gestiegen ist, gehört der Schutz von Industriesystemen zu den überfälligen Themen, mit denen sich große Unternehmen schwertun (ebenso wie die Verwaltung von externen Auftragnehmern und die Sicherheit in der Cloud).

Mit dem Ziel, diese Unternehmen zur Einführung von Cybersicherheitsstandards zu bewegen, werden demnächst europaweite Gesetze und Vorschriften eingeführt, wie beispielsweise die NIS2-Richtlinie für den Umgang mit Auftragnehmern in sensiblen Umgebungen oder der Cyber Resilience Act für die Härtung vernetzter digitaler Produkte. Aus der Sicht von Vincent Nicaise werden diese Gesetzestexte den Fachleuten dabei helfen, eine Reihe von konkreten Sicherheitsmaßnahmen zu ergreifen: „*Sobald der Cyber Resilience Act auf europäischer Ebene eingeführt wird, werden die Hersteller zum Beispiel verpflichtet sein, Sicherheitsvorrichtungen in ihre Geräte zu integrieren*." Parallel dazu können auch Referenzsysteme wie MITRE ATT&CK oder NIST dazu beitragen, dass die Industrie sich in Bezug auf das Thema Cybersicherheit weiterentwickelt. Unabhängig vom verwendeten Medium muss eine umfassende und seriöse technische Diagnose die Industrie dazu auffordern, ihre Widerstandsfähigkeit gegen Angriffe im Hinblick auf die Industrie 5.0 schnell auszubauen.

„Eine sensibilisierte Person ist besser als zwei. Und das ist meiner Meinung nach ein Punkt, der sich mit den Prinzipien der Industrie 5.0 deckt, welche die Zusammenarbeit zwischen Mensch und Maschine kennzeichnet."

Stéphane Potier, Leiter des Angebots Cybersecurity OT & IoT bei Advens

Operativ kann sich diese Fähigkeit in der Segmentierung von Netzwerken und Produktionsumgebungen, der Verwendung von Verschlüsselung für den Austausch sensibler Daten, der Einrichtung starker Authentifizierungssysteme oder auch der kontinuierlichen Überwachung sensibler Infrastrukturen niederschlagen. Deshalb wird es **absolut entscheidend sein, Mitarbeiter bezüglich der Erkennung von Cyberangriffen zu sensibilisieren und zu schulen**. *„Die Bediener kennen ihre Maschinen und sind sich der normalen Reaktionen ihrer Tools natürlich bewusst*“, betont Stéphane Potier. *„Sie für das Thema Cybersicherheit zu sensibilisieren, indem man ihnen die verschiedenen Arten von Angriffen und die möglichen Auswirkungen auf ihr Arbeitsumfeld erklärt, trägt dazu bei, sie wachsamer zu machen. Bediener werden so in die Lage versetzt, eine anormale Situation sehr schnell zu erkennen und sie an ihren CISO weiterzuleiten.“* Er stellt jedoch fest, dass die Sensibilisierung im OT-Umfeld nicht so systematisch verläuft wie im IT-Umfeld. *„Im Gegensatz zu dem beliebten Sprichwort in der Cybersicherheit, dass die größte Schwachstelle zwischen Stuhl und Tastatur zu finden ist, denke ich im Gegenteil, dass die Lösung zwischen Stuhl und Tastatur liegt*“, bemerkt er. Und weiter: *„Eine sensibilisierte Person ist besser als zwei. Und das ist meiner Meinung nach ein Punkt, der sich mit den Prinzipien der Industrie 5.0 deckt, welche die Zusammenarbeit zwischen Mensch und Maschine kennzeichnet.“*

Um effektiv zu sein, muss die Industrie 5.0 ihre Grundprinzipien – Menschen, Nachhaltigkeit und Resilienz – mit einem erhöhten Bewusstsein für Cybersicherheit und der Integration von robusten Geräten in ihre Systeme kombinieren. Mit anderen Worten: Die Cybersicherheit muss ein integraler Bestandteil dieses neuen industriellen Paradigmas für alle Unternehmen werden, die sich in diese Richtung entwickeln möchten.