MEINUNGEN

INDUSTRIEUNTERNEHMEN: DIE DIGITALE SOUVERÄNITÄT IST DAS RÜCKGRAT IHRER OT-CYBERSICHERHEITSSTRATEGIE

Vincent Nicaise
Industrial Partnership and Ecosystem Manager, Stormshield

Cyberkriminelle visieren zunehmend den Industriesektor an – und ihre Angriffe haben weitreichende Folgen. Dies betrifft nicht nur Betreiber von lebensnotwendigen Diensten und Infrastrukturen entscheidender Bedeutung für das Land, denn die gesamte Sparte ist betroffen. Abgesehen von Vorschriften, die darauf abzielen, eine Entscheidung für europäische (souveräne) Lösungen zu forcieren, obliegt es der Verantwortung aller Industrieunternehmen, dieselben Regeln umzusetzen und Maßnahmen bezüglich aller Aspekte der gesamten Sicherheitskette zu ergreifen. Warum ist das Konzept der digitalen Souveränität so wichtig? Ein Artikel von Vincent Nicaise, Leiter Industriepartnerschaften bei Stormshield, und Yoann Delomier, Leiter des OT-Teams bei Wallix.

Die dank Digitaltechnik in der Industrie eingeführten neuen Praktiken haben in den letzten Jahren erheblich zur Entwicklung und Modernisierung dieses Sektors beigetragen. Dies gilt nicht nur für die Leistungs- und Wettbewerbsfähigkeit in einer Zeit starker Globalisierung, sondern auch für die Nachhaltigkeit und die Rückverfolgbarkeit im Sinne der Verbraucher und der europäischen Vorschriften.

Im Umkehrschluss bewirkten diese neuen Arbeitspraktiken im Industrieumfeld eine Zunahme der Cyberrisiken. Die Betreiber kritischer Infrastrukturen (Verkehr, Energie, Wasserversorgung usw.) nutzen Prozesse, bei denen Daten (mitunter ständig) in Echtzeit zirkulieren, um einen reibungslosen Betrieb zu gewährleisten. Letztlich sollen die Produktivität und die Erbringung von Diensten für die Allgemeinheit damit garantiert werden. Diese Daten sind nun Angriffen aus verschiedenen Richtungen ausgesetzt: Mögliche Zugangspunkte werden von immer professionelleren Hackern ausgenutzt, deren Ziele etwa Industriespionage und Produktionsstopps sind, um Lösegeld zu fordern. Teils stecken aber auch politische Zwecke dahinter. Angesichts der finanziellen, menschlichen und ökologischen Risiken, die hinter diesen Attacken stehen, hat der Industriesektor einen starken Anreiz, die geforderten Summen zu zahlen. Für Hacker bedeutet das einen regelrechten Geldregen.

Im März 2022 gab die französische Sicherheitsagentur ANSSI bekannt, ihr lägen für 2021 Informationen über 1.082 kritische Attacken vor, die das reibungslose Funktionieren des Landes unterminiert hätten. Das entspricht einem Anstieg von 37 % gegenüber dem Vorjahr. Diese Zahlen gelten bis zu einem gewissen Grad auch für Industrieunternehmen, die für die Sicherheit von Gütern und Personen sorgen und daher – unabhängig von deren Rolle oder Bedeutung im Produktionsprozess – dazu verpflichtet sind, sichere und vertrauenswürdige Cybersicherheitslösungen zu implementieren.

Nichtsdestoweniger ist festzuhalten, dass die Akteure in der Industrie bei der Ausarbeitung ihrer Modernisierungspläne den Aspekten der Cybersicherheit nicht immer Vorrang einräumen. Dabei ist dies ein ausschlaggebender Faktor zur Gewährleistung einer optimalen Prozesssicherheit bei der Konzeption von IT/OT-Projekten und wird ebenfalls bei allen Akquisitionsprojekten und an allen Standorten, im Inland wie im Ausland, berücksichtigt. Die Souveränität von Cybersicherheitslösungen (Made in Europe) spielt bei diesen Überlegungen eine wichtige Rolle.

VERTRAUEN: DAS ERSTE KRITERIUM BEI DER AUSWAHL IHRER CYBERSICHERHEITSLÖSUNGEN

Sich für souveräne Cybersicherheitslösungen zu entscheiden, bedeutet vor allem, Transparenz zu gewährleisten und jedes Risiko zu vermeiden, dass Daten zu böswilligen Zwecken missbraucht werden könnten. Hierbei geht es darum, Zugang zu gut überwachten, hoheitlichen Informationen zu haben und so die Risiken einer Kompromittierung oder von Angriffen durch ausländische Akteure zu verringern. Nur so kann eine umfassende Verteidigung ohne Schwachstellen gewährleistet werden.

Ein solcher Ansatz ist von entscheidender Bedeutung, um jegliches Risiko der Einmischung oder Wirtschaftsspionage zu vermeiden. Beispielhaft ist hierfür der Fall der chinesischen Hackergruppe Winnti gesehen, gegen die kürzlich aufgrund der Anschuldigung ermittelt wurde, im Auftrag des chinesischen Staates eine groß angelegte Spionageoperation in den USA, Europa und Asien durchgeführt zu haben.

Die Beibehaltung der digitalen Unabhängigkeit Europas ist auch der einzige Weg, um eine lokale, selbstständige Reaktion auf Produktionsprobleme und kritische Aktivitäten bei der Behebung von Cybervorfällen zu ermöglichen – zum Beispiel, um Produktionsabbrüche zu minimieren. Europäische Lösungen sind in der Lage, diese lokale Reaktion in Form von schnellem technischem Support, der Unterstützung lokaler Teams, eines Incident-Response-Verfahrens usw. zu liefern.

Und schließlich gewährleistet die Wahl souveräner Lösungen auch die Einhaltung der geltenden europäischen Regelungen und Normen, die den sicheren Zugang zu Informations- und operativen Systemen (Authentifizierung, Segmentierung, Rückverfolgbarkeit von Daten, Verschlüsselung usw.) gesetzlich vorschreiben.

Kurz gesagt: Es besteht Bedarf an vertrauenswürdigeren europäischen Lösungen, zumal Grenzen angesichts der Verbreitung von Produktionsstandorten in der ganzen Welt keine Rolle mehr spielen, wenn ein europäisches Industrieunternehmen angegriffen wird.

IN EUROPÄISCHE MARKTFÜHRER DER INDUSTRIELLEN CYBERSICHERHEIT INVESTIEREN: EIN VERANTWORTUNGSBEWUSSTER UND SOZIALVERTRÄGLICHER ANSATZ

Um die Industrie dabei zu unterstützen, die richtigen Entscheidungen zu treffen, können führende europäische Hersteller von Cybersicherheitslösungen auf mehrere Mittel zum Aufbau eines zuverlässigen, widerstandsfähigen Umfelds zurückgreifen. Die erste Möglichkeit besteht darin, das lokal verfügbare Angebot an Sicherheitslösungen zu erweitern, um sicherzustellen, dass Endkunden mindestens eine souveräne Lösung beziehen können. Dies geht Hand in Hand mit der Sensibilisierung industrieller Hersteller für die Implementierung europäischer Sicherheitskomponenten in das Design ihrer Produkte.

Im Allgemeinen ist es wichtig, Start-ups und die Cyberbranche über nationale Organisationen zu unterstützen, Investitionen in die lokale Cyberwirtschaft über spezielle Fonds zu garantieren und die Ausbildung zu fördern. Dies sind nicht nur die Voraussetzungen dafür, dass sich Unternehmen in Europa ansiedeln und dort bleiben, sondern auch für den Erhalt und die Weiterentwicklung des europäischen Know-hows.

Durch die Einbeziehung des gesamten Ökosystems und eine wirksame Zusammenarbeit zwischen den europäischen Akteuren wird es möglich sein, die digitale Unabhängigkeit bei der Absicherung der Industriebranche zu verstärken und gleichzeitig einen optimalen Schutz unserer Wirtschaft, unserer Bürger und unserer Umwelt zu gewährleisten.