Wirtschaft

29. Jun. 2022 | 08:21 Uhr | von Siegfried Müller

Kolumne

Vom Wissen und Wollen ins Handeln kommen

Klar - Sybersecurity ist eine gute Sache. Das wissen wir. Und wir wollen sie auch, denn wer öffnet böswilligem Code schon gerne Tür und Tor. Entscheidend ist aber, endlich etwas zu tun, sagt unser Kolumnist Siegfried Müller.

Unternehmen wissen oft um die Gefahr einer Cyberattacke - aber oft handeln sie nicht entsprechend, wenn es um die Sicherheit geht. (Bild: blackboard - stock.adobe.com)

Eine ersprießliche Idee, wenn Sie mal nicht wissen, was Sie tun sollen ist, einfach den Begriff „ins Handeln kommen“ in Ihre favorisierte Suchmaschine einzugeben. Da finden Sie sehr viele Personen, die gute Tipps – in der Mehrzahl sind es jeweils fünf – offerieren, um den Suchenden zu motivieren, sich (natürlich im übertragenen Sinne) bezüglich seines Ziels endlich in Bewegung zu setzen. Obwohl in der ersten Empfehlung konträr dazu erst einmal geraten wird „Ruhe zu bewahren“. Grundsätzlich eine gute Idee, weil hektisch agieren ohne Ziel bringt ja genauso wenig wie Nichtstun. Wer hat das nicht schon selber erlebt?

Doch auch danach kann es de facto noch immer nicht richtig losgehen, weil im zweiten Schritt von den Ratgebern mehrheitlich auf die Notwendigkeit hingewiesen wird, vorab doch alle „Risiken abzuschätzen“ – also sich damit auseinanderzusetzen, was im schlimmsten Fall passieren könnte und ob überhaupt die Bereitschaft dazu besteht ein Wagnis einzugehen. Nur wenn diese Analyse entsprechend ausfällt, ist es dann endlich möglich mit dem Durchstarten zu beginnen: es folgen die Phasen der „Planung“ sowie „Umsetzung“. Wer bis dahin durchgehalten hat, erfährt zum Schluss dann, dass auch ein kritisches Hinterfragen, ob das anvisierte „Ziel erreicht“ wurde, nicht fehlen darf. Gut – das sollte eigentlich selbstverständlich sein, oder? Gefallen hat mir im Weiteren ein Tipp von einem, ansonsten eher esoterisch angehauchten, Verfasser – scheinbar gibt es doch mehr als nur den einen einzig wahren Weg vom Wollen ins Handeln zu kommen – der rät, erst einmal „in kleinen Schritten zu beginnen“.

Wahrscheinlich sind Denkanstöße, die dazu anregen, ins Handeln zu kommen prinzipiell gar nicht so verkehrt oder momentan vielleicht sogar vonnöten – denn abwarten in der Hoffnung, dass sich ein Problem von allein löst, macht weder Sinn noch ist die Eintrittswahrscheinlichkeit diesbezüglich sehr hoch. Zugegebenermaßen könnten einige Vorschläge, die ich gelesen habe, durchaus den Impuls dazu geben, sich endlich mit der Cyber-Sicherheit zu beschäftigen und vielleicht sogar zuträgliche Anhaltspunkte liefern. Denn auch wenn es hinsichtlich der Sicherheitsstrategie erprobte Vorgehensweisen – unter anderem im Hinblick auf die notwendigen Schritte – gibt, scheint es nichtsdestotrotz keinesfalls einfach zu sein, ins Handeln zu kommen.

Wo liegen die Knackpunkte?

Konkret bezogen auf die Absicherung von Produktion und Fertigung liegt dies meines Erachtens darin begründet, dass es oftmals unklar ist, in wessen Verantwortungsbereich die IT- und Cyber-Sicherheit fällt. Folglich sind häufig bei Unternehmen die Zuständigkeiten nicht eindeutig zugeordnet – weder intern noch, beispielsweise bei den Maschinen- und Anlagenbauern, im Verhältnis zum Kunden. In der Praxis führt dies zu den verschiedensten Ausprägungen – teilweise steht hier die IT-Abteilung sogar in der

alleinigen Verantwortung, das heißt die IT-Fachleute agieren, ohne mit den Verantwortlichen der OT-Netzwerke zu kommunizieren. Tatsächlich bin ich der Ansicht, dass die mangelnde Abstimmung zwischen IT und OT eine der Ursache ist, warum die Initialisierung und Durchführung von Prozessen zur Absicherung der Produktions-Netzwerke nicht reibungslos verläuft. Denn dies führt unter anderem dazu, dass über die Priorisierung von notwendigen Projekten unterschiedliche Ansichten bestehen. Zudem resultieren daraus divergente Konzepte, die keinesfalls umfassend genug sind, um das erforderliche Schutzniveau zu gewährleisten.

Auch im Verhältnis der Maschinen- und Anlagenbauern mit ihren Kunden ist es unerlässlich, dass die Zuständigkeiten klar definiert sind. Allein um zu vermeiden, dass die Verantwortung beliebig hin- und hergeschoben werden kann. Theoretisch müsste es sogar im beiderseitigen Interesse sein, dafür Sorge zu tragen, dass die Funktionsfähigkeit der Maschinen optimal gewährleistet ist. Praktisch bedarf es hierfür entsprechend neben dedizierter IT-Lösungen auch eines ganzheitlichen Ansatzes, da die Vermeidung von Produktionsausfällen nicht ausschließlich auf der Abwehr von Cyberangriffen basiert – sondern ebenso auf der prozesssicheren Vernetzung,
bei der es gilt durch Abgrenzung von Funktionalitäten
Störeinflüsse von außen zu verhindern und so für eine ordnungsgemäße Weiterleitung der Netzwerkprotokolle zu sorgen.

Erste Schritte, um ins Handeln zu kommen

Ein essenzieller Punkt ist hierbei, Verantwortlichkeiten bezüglich IT-/Cyber-Sicherheit auf den Prüfstand zu stellen und eventuell neu festzulegen. Zum Beispiel unter dem Aspekt, dass in IT-Abteilungen weder entsprechendes Know-how bezüglich der Produkte, etwa zur Absicherung von Produktions-Netzwerken, vorhanden sein kann noch, ob deren jeweiliger Einsatz für den angefragten Anwendungszweck tatsächlich geeignet ist.

Des Weiteren sollte dem Umstand Rechnung getragen werden, dass eine Netzwerksegmentierung – die klassische Maßnahme mit unmittelbar großer Auswirkung auf die IT- und Cyber-Sicherheit – grundsätzlich auch von einem versierten OT-Spezialisten vorgenommen werden kann. Sinnvoll allein unter dem Aspekt, dass dieser gleich die Implementierung der Produkte, die dediziert zur Absicherung der Maschinen notwendig sind, initiieren kann.

In Bezug auf den Einsatz von IT-Sicherheitslösungen empfehle ich Folgendes zu beachten: Auch oder gerade, wenn es sich hierbei um moderne, sichere und problemlos zu implementierende Produkte handelt, so sollten die Mitarbeiter doch in deren Nutzung eingewiesen werden. Denn, egal wie sicher ein Produkt konzipiert ist, durch einen fahrlässigen Umgang wird das Schutzniveau definiert gesenkt – denken Sie nur an technische Regelungen für eine hohe Passwortsicherheit, die nichts nutzen, wenn ein Post-it mit dem Passwort am Computer klebt.

Mein Fazit

Wie eingangs erwähnt bin ich der Meinung, dem – zugegebenermaßen sehr allgemeingültigen – Rat „mit kleinen Schritten beginnen“ sollte, fraglos mehr Beachtung geschenkt werden. Denn genau diese Maxime ermöglicht es, ins Handeln zu kommen. Natürlich verhelfen kleine Schritte maximal dazu, eine solide Basis zu schaffen und nicht, ein abschließendes Ergebnis zu erzielen. Dies sollte auch keinesfalls die Intention dahinter sein. Aber allein aus dem Grund, dass die IT nicht statisch ist und durch den Einsatz innovativer Technologien immer wieder neue Anforderungen entstehen, müssen hier beständig Anpassungen vorgenommen werden.

Um diese Erfordernisse zu meistern, müssen IT und OT unbedingt an einem Strang ziehen, die Stärken der jeweils anderen Abteilung sowohl kennen als auch anerkennen und vor allem permanent im Austausch bleiben.

Der Autor

(Bild: MB Connect Line)

Siegfried Müller, VP Advanced Technologies bei der MB Connect Line GmbH Fernwartungssysteme.
In seinen ersten Berufsjahren als Steuerungstechniker für den Maschinenbau hat er den Nutzen von Fernwartung erkannt. Im Alter von 25 Jahren gründete er MB connect line. Unter seiner Leitung entwickelte sich das Unternehmen zum Technologieführer in den Bereichen Fernwartung, Datenerfassung und Industrial Security. Heute ist die MB connect line der europäische Standort der Red Lion Inc. in der Industrial Division der Spectris plc Gruppe.
Seit über 20 Jahren treibt Siegfried Müller mit viel Engagement und Leidenschaft die Entwicklung neuer Produkte und Lösungen für die sichere industrielle Kommunikation über Internet voran. Als Stratege und Experte zur Cybersicherheit im industriellen Umfeld bringt er sein Wissen auch in nationalen und internationalen Arbeitskreisen ein – beispielsweise beim Cluster Mechatronik & Automation Bayern e.V., beim TeleTrusT – Bundesverband IT-Sicherheit e.V. und in der European Cyber Security Organisation (ECSO). Die wichtigen wirtschaftlichen Themen adressiert er als Senator im internationalen Wirtschaftssenat (IWS).