Wirtschaft

04. Nov. 2022 | 08:57 Uhr | von Siegfried Müller

Thema OT-/Cyber-Sicherheit

Abwehrmöglichkeit gegen die verschärfte Cyber-Sicherheitslage

Die Fertigungsindustrie ist ein beliebtes Ziel für Cyberangriffe. Die Abwehrmöglichkeiten sind dieser Bedrohungslage allerdings meist nicht angemessen, sagt unser Kolumnist Siegfried Müller. Er hat ein paar Empfehlungen.

Unternehmen befürchten bei einer Cyber-Attacke massive Schäden. Ausreichend gewappnet sind sie aber oft nicht. (Bild: Maksim Shmeljov - stock.adobe.com)

Eigentlich wollte ich dieses Mal darüber philosophieren, ob möglicherweise zwischen den immer noch mangelnden OT-/Cyber-Sicherheitsvorkehrungen und Langeweile ein Zusammenhang besteht – unter anderem motiviert durch den Comic „IT-Sicherheit mal nicht langweilig“. Dieser Titel wirft doch Fragen auf, oder? Denn gemäß der Definition von Dr. John Eastwood (York University) ist Langeweile grundsätzlich „das unangenehme Gefühl, eine zufriedenstellende Aktivität ausführen zu wollen, aber nicht zu können”. Lässt sich hieraus – zumindest theoretisch – ein Erklärungsansatz für die, eingangs erwähnte, mögliche Wechselbeziehung ableiten?

Rein faktisch gesehen wohl doch eher nicht. Meines Erachtens aus zweierlei Gründen. Zum einen, weil inzwischen technische Lösungen zur Verfügung stehen, um die OT-/Cyber-Sicherheit zu erhöhen und somit zielgerichtete Initiative in diesem Bereich durchaus zufriedenstellend sein kann. Zum anderen, da mittlerweile – durch die Möglichkeit wieder auf Veranstaltungen und Messen gehen zu können – genügend Unterstützungsangebote bereitgestellt werden, mit denen es möglich ist ins Handeln zu kommen. Allein in den vergangenen vier Wochen – die fast unter dem Motto stehen könnten „nach der Veranstaltung ist nach der Messe ist vor der Messe“ – bestanden mit dem Maschinenbau-Gipfel und der it-sa sowie jetzt noch aktuell auf der SPS ausreichend Möglichkeiten, sich über das Thema OT-/Cyber-Sicherheit zu informieren. Selbstverständlich gibt es im Moment mehrere essenzielle Themen, die für die Industrie von Bedeutung sind, aber OT-/Cyber-Sicherheit sollte oder muss sogar definitiv dazu gehören.

Wer diesbezüglich (noch) nicht hundertprozentig überzeugt ist, der findet in der aktuellen Studie „State of Ransomware 2022“ von Sophos gute Argumente für ein Umdenken. Aber im Prinzip liegen die Tatsachen ja so auf der Hand: Insbesondere die Fertigungsindustrie ist bei Cyberkriminellen ein beliebtes Ziel – allein aus zwei prägnanten Gründen. Erstens, weil hier gravierende Schäden, sprich lange Produktionsausfälle, verursacht werden können die sehr oft mit immensen Kosten einhergehen. Zweitens, weil Unternehmen oftmals Teil einer Lieferkette sind und somit Störungen in der Produktion einen hohen Wirkungsgrad haben, da dies Auswirkungen auf die Prozessabläufe weiterer Betriebe hat.

Natürlich wird es den Angreifern teilweise auch sehr leicht gemacht, da sie hier auf veraltete Infrastrukturen treffen, die nur unzureichend oder gar nicht abgesichert sind. Aber es könnte ebenso daran liegen, dass die Fertigungsunternehmen dazu bereit sind viel Geld für die Entschlüsselung ihrer Daten in die Hand zu nehmen – denn deren durchschnittliche Lösegeldzahlung liegt bei 2.036.189 Dollar.

Doch auch wenn – wie im Lagebericht zur Cybersicherheit in Deutschland des „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) nachzulesen ist – Ransomware momentan die verschärfte Cybersicherheitslage maßgeblich mitbestimmt, sollte die Abwehr gegen kriminelle Angreifer nicht punktuell betrachtet werden, sondern ganzheitlich. Das bedeutet, dass Unternehmen nicht nur eine Neu-Bewertung ihrer Sicherheitsstrategie durchführen, sondern auch höhere Investitionen in die Cyber-Sicherheit tätigen müssen.

OT-/Cyber-Sicherheitsstrategie auf den Prüfstand stellen

Um gegen die zunehmenden Angriffe in der Produktionsumgebung besser gewappnet zu sein, ist es in erster Linie erforderlich die OT-/Cyber-Sicherheitsstrategie auf den Prüfstand zu stellen. Aktuell möchte ich Ihnen empfehlen, in diesem Kontext Ihre Abwehrstrategien einmal genauer zu begutachten und sie dahingehend zu bewerten, ob die eingesetzten IT-Sicherheitslösungen gemäß der Cyber-Sicherheitslage ausreichend sind. Wenn diese nur bereits bekannte Angriffe detektieren können, sind sie oftmals unzureichend, um ein notwendiges Schutzniveau zu etablieren.

Um dieses weiter zu optimieren, ist es erforderlich eine vollständige digitale Transparenz in den Netzen anzustreben – also eine Analyse der bestehenden Netzwerk-Infrastruktur und -Kommunikation durch die maschinelle Erfassung aller Systeme, Geräte und Datenflüsse der Produktionsanlagen. Diese komplette Netzübersicht ist notwendig, um im Weiteren Anomalien – von fehlerhaften Datenpaketen über Anlagenfehler bis hin zu einem Malware-Angriff – zu ermitteln: Das Ziel dabei ist, jegliche Veränderungen der erlaubten und bekannten Standardkommunikation in den Produktionsnetzen zu erkennen, um aufgrund des Monitorings dieser Abweichungen umgehend entsprechende Maßnahmen zur Schadensbegrenzung einleiten zu können.

Fazit

Unternehmen sollten es den Angreifern nicht so leicht machen, sondern stattdessen eher ein Stück weit deren Taktik adaptieren und immer die besten Methoden einsetzen, die aktuell auf dem Markt verfügbar sind. Darüber hinaus ist es meines Erachtens sinnvoll die vielfältigen Möglichkeiten zum Austausch zu nutzen – das könnte möglicherweise auch dem Aufkommen von Langeweile entgegenwirken.

Wir tun unser Möglichstes dagegen auf der SPS und freuen uns darauf, Sie mit unserer Erfahrung zu unterstützen. Sie finden uns in Halle 5, Stand 244.

Das ist unser Kolumnist Siegfried Müller

(Bild: MB Connect Line)

Siegfried Müller ist Vice-President 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.