KOPF IN DEN SAND IST KEINE LÖSUNG

Der Mensch ist ein seltsames Wesen. Einerseits strebt er nach maximaler Sicherheit, andererseits neigt er dazu, die Vorboten einer drohenden Gefahr solange zu ignorieren bis alles über ihn hereinbricht. Ein proaktives Risikomanagement ist in vielen Bereichen nach wie vor eher die Ausnahme und nicht die Regel. Leider, denn egal ob es darum geht, die unternehmenseigene Cyber Security, den Umgang mit einem neuartigen Virus oder irgendeine andere Krise zu managen – es ließe sich enorm viel abfangen und bewirken, wenn vermehrt vorausschauend agiert werden würde. **Ein Gastkommentar von T&G-Geschäftsführer Harald Taschek**

Von einem Tag auf den anderen war alles anders. Die Corona-Krise kam aus dem Nichts. Dieses Virus erwischte uns alle am falschen Fuß. Aussagen wie diese beherrschen seit Monaten die Schlagzeilen. Aber ist dem wirklich so? Gab es nicht in Wahrheit auch hier wie bei nahezu jeder Art von Bedrohung mehrere Hinweise auf eine herannahende Gefahr, die zumindest eine Zeitlang geflissentlich ignoriert wurden?

Meine Überlegungen in diese Richtung führen mich zu einer der größten Schwächen von uns Menschen: Wir neigen dazu, Probleme nicht wahrhaben zu wollen – selbst wenn diese nicht mehr „nur" an die Tür klopfen, sondern bereits am Hereinmarschieren sind. Wir sehen nicht hin, verharmlosen, verdrängen, stecken den Kopf in den Sand und sind alles in allem sehr erfinderisch bei unseren Ausweichstrategien. Dabei gibt es in solchen Situationen nur eine Herangehensweise, die auf lange Sicht zielführend ist. Man muss sich der Herausforderung stellen. Umso früher, desto besser. Schließlich geht es vor allem auch darum, sich einen gewissen Handlungsspielraum zu bewahren und nicht zu sehr in die Defensive zu geraten. Denn wer bei herausfordernden Rahmenbedingungen noch mit Bedacht agieren kann, befindet sich in einer erheblich günstigeren Ausgangsposition als jemand, der unter Druck reagieren muss.

Vorsorgen bringts

„Die Menschen werden selten durch fremden Schaden klug", stellte „Gesellenvater" und Kolpingwerk-Begründer Adolph Kolping bereits in den 1850er Jahren fest. Und es zeigt sich in der Tat immer wieder und zwar in den unterschiedlichsten Bereichen, dass wir oftmals nur aus eigener Erfahrung lernen. Ein typisches Beispiel dafür ist für mich die Cyber Security-Thematik. Es wird seit Jahren von verschiedensten Seiten darauf hingewiesen, dass sich Cyberangriffe auf die Industrie mehren, trotzdem hält sich das Risikobewusstsein der Unternehmen nach wie vor in sehr bescheidenen Grenzen. Und selbst wenn nicht, wird vielfach lieber in kleine, unkoordinierte Einzelmaßnahmen investiert als gesamtheitlich betrachtet und in ausreichendem Maße vorgesorgt. Warum? Weil Sicherheit, wie wir sowohl beim Umgang mit dem Corona-Virus als auch bei der Umsetzung anspruchsvoller Industrie 4.0-Projekte feststellen, nicht gerade einfach herzustellen ist. Besonders dann nicht, wenn man es mit einer komplexen Gesamtsituation zu tun hat, bei der zahlreiche Einflussfaktoren zu berücksichtigen sind. So gilt es bei einem strategischen „Ja" zu einer zunehmenden Vernetzung mit der Erstellung eines passenden Schutzkonzepts einiges im Auge zu behalten – angefangen vom Spagat zwischen Cyber-Sicherheit und Anlagenverfügbarkeit, über einen „securen" Brückenschlag zwischen OT und IT bis hin zur richtigen Balance zwischen dem, was technologisch möglich ist und jenem, was aus wirtschaftlichen Gründen auch tatsächlich Sinn macht.

TG Alpha: Number One in Digitalization and OT-Cyber Security

Letzten Endes ist der Umgang mit jeglicher Gefahrensituation eine beinharte Kosten-Nutzen-Rechnung. Wie hoch ist unser Sicherheitsbedürfnis? Wieviel sind wir bereit, zu investieren bzw. zu riskieren? Wo liegen die jeweiligen Schmerzgrenzen? Allesamt Fragen, die nicht so leicht zu beantworten sind. Denn für nahezu jedes „Für" gibt es auch ein „Wider". Wir als T&G unterstützen gerne dabei, alle „Pros" und „Kontras" herauszufinden, abzuwägen und in ein kundenindividuelles Maßnahmenpaket umzuwandeln. Einerseits steht dazu unser gesamtes Partnernetzwerk als kompetent beratender Ansprechpartner zur Verfügung, andererseits eine neue Tochtergesellschaft namens TG Alpha, die zusammen mit der deutschen Firma ProtectEM – einem Spezialisten für OT-Cyber Security – gegründet wurde.

Wir haben unsere „Human- bzw. Brainpower" gebündelt und bieten uns jetzt als „One-Stop-Kompetenzzentrum" an, in dem alles rund um die Themen Digitalisierung und OT-Cyber Security für Industrie, Infrastruktur und Maschinenbau aus einer Hand zu haben ist: Anforderungsgerechte Lösungen, kundenindividuelle Trainings sowie umfassende Beratungsdienstleistungen, die von einer „Cyber-FMEA"

> Mit TG Alpha bieten wir einen One-Stop-Shop für sichere Digitalisierung. Ein Kompetenzzentrum, von dem alles rund um die Themen Digitalisierung und OT-Cyber Security für Industrie, Infrastruktur und Maschinenbau aus einer Hand zu haben ist: Anforderungsgerechte Lösungen, kundenindividuelle Trainings sowie umfassende Beratungsdienstleistungen.
>
> **Harald Taschek, Geschäftsführer der T&G Automation**

(Failure Mode and Effects Analysis) bis hin zu Product Security Audits reichen. Als „D1 – Number One in Digitalization" und nun auch „C1 – Number One in OT-Cyber Security" können wir bei der Planung von Industrienetzwerken genauso unterstützen wie bei der Umsetzung von Security-Maßnahmen, der Entwicklung „securer" Hard- und Software gemäß IEC 62443 sowie bei der Erstellung maßgeschneiderter Testsysteme und bei der Implementierung entsprechender Managementsysteme. Kurz gesagt: „Ein One-Stop-Shop für sichere Digitalisierung"!

Change by Design versus Change by Disaster

Eines ist klar: Nachdem die durchschnittlichen Kosten, die ein Cyberangriff verursacht, laut Hiscox Cyber Readiness Report im Jahresabstand um den Faktor 6 gestiegen sind, kommt es wahrscheinlich erheblich günstiger, wenn man proaktiv agiert, entsprechende Schutzvorkehrungen installiert und alle im Unternehmen zur Verfügung stehenden Abwehrkräfte mobilisiert, um sich vor solchen Attacken zu schützen. Gerade in herausfordernden Zeiten wie diesen haben wir alle nichts zu verschwenden bzw. nichts zu riskieren. Also „changen" wir doch lieber freiwillig die Ausgestaltung unserer Unternehmensinfrastruktur, Produkte und Prozesse – noch bevor wir von irgendeinem „Disaster" genötigt werden, dies zu tun.

In der Corona-Zeit entpuppte sich z. B. der vermehrte Homeoffice-Betrieb als sicherheitstechnische Schwachstelle, die einige Angreifer für sich zu nutzen wussten. Äußere Zwänge, sich intensiver mit dem Thema Cyber Security auseinanderzusetzen, gibt es aber auch für Maschinenbauer: Hier sind es vor allem Haftungsfragen, die zu einem raschen Handeln zwingen, zumal es – wenn es wegen eines Produktionsausfalls wirklich hart auf hart kommt – letztendlich vollkommen egal ist, ob eine Anlage wegen eines technischen Defekts oder wegen einer Cyberattacke gestanden ist.

www.tug.at

XXX