Scharf beobachtend, genau hinterfragend und kritisch – T&G-Geschäftsführer Ing. Harald Taschek zeigt sich in diesem Gastkommentar von seiner „provokanten“ Seite.

www.tug.at

Vorbeugen hilft

Die Angst vor Cyber-Kriminalität wächst in Österreichs Unternehmen. Als größte Gefahr werden zwar laut Allianz Risk Barometer 2017 Betriebs- und Lieferunterbrechungen eingeschätzt (37 %), aber Cyber- und IT-Risiken schafften es mittlerweile schon auf Platz 2 (32 %) der Top 10-Risiken. So das Ergebnis einer jährlich durchgeführten Untersuchung, bei der Experten und Unternehmer aus 55 Ländern ihre Einschätzung abgeben. Nun, meine Einschätzung ist: Wir sollten uns von solchen Zahlen nicht in Panik versetzen lassen und schon gar nicht in eine Art Schockstarre verfallen. Mittlerweile gibt es durchaus bewährte Mittel und Wege, um potenziellen Angreifern das Eindringen in die eigenen Unternehmensnetze zu verwehren. Allerdings werden diese bis dato noch viel zu selten genutzt. Laut einer Bitkom-Umfrage zeigten sich im Vorjahr nicht einmal die großen Industriebetriebe ausreichend gewappnet für eine Zeit, in der die Angriffslust von Saboteuren und Wirtschaftsspionen permanent steigt wie es aussieht. Denn die Experten von Kaspersky Lab gehen davon aus, dass es 2017 vermehrt zu DDoS-Attacken über IoT-Botnetze kommen wird.

Aber zum Glück gibt es ja nicht nur „böse Hacker“, sondern auch gute. Diese sind zwar auch danach bestrebt, etwaige Sicherheitslücken aufzuspüren, allerdings nicht um diese für unlautere Zwecke auszunutzen, sondern ganz im Gegenteil um diese letztendlich zu schließen. Die Security-Experten von Wurldtech sind solche „White-Hat-Hacker“. Sie entwickelten eine Geschäftsidee daraus, industrielle Geräte zu knacken, um deren Anbieter auf etwaige Schwachstellen aufmerksam machen. Mit großem Erfolg: Das Zertifizierungsprogramm „Achilles" von Wurldtech gilt mittlerweile international als Standard für industrielle Cyber Security-Lösungen. Ebenfalls aus dem Hause Wurldtech stammt OpShield, ein wie der Produktname schon verrät ausgeklügeltes Schutzschild für die operative Technik, das auf eine intelligente Segmentierung von Anlagen- und Maschinennetzen setzt, um unbefugte Zugriffe auf Befehlsebene zu verhindern.

„Freund“ hört mit

Der 5. November 2016 schaffte es dank Kaspersky Lab in die Negativschlagzeilen. Alleine an diesem einen Tag wurden nämlich weltweit 1.915 DDoS-Attacken registriert. Aber trotz dieser alarmierenden Zahlen wird in vielen Unternehmen noch immer „Tee getrunken“ und abgewartet statt proaktiv geschützt und getan. Einen umfassenden Sicherheitsansatz, der mehrere Fronten und Verteidigungslinien aufbaut kennen viele Unternehmen nach wie vor nur vom Hörensagen – obwohl bei diversen Umfragen immer wieder angegeben wird, dass Security die Basis für eine funktionierende Digitalwirtschaft bildet. Woran scheitert es also beim konkreten Tun? Daran, dass die Zuständigkeiten zwischen IT- und Automatisierungsabteilung noch immer nicht geklärt sind? Daran dass vielfach noch immer nebeneinander statt miteinander getan wird auf IT- und OT-Ebene? Daran dass die Eintrittswahrscheinlichkeit eines Cyberangriffs als zu gering eingestuft wird, obwohl es immer heißt früher oder später treffe es jeden?

Müssen wir Menschen wirklich immer erst „Lehrgeld“ zahlen bevor wir umsichtiger agieren? Vielleicht. Vielleicht aber auch nicht. Bei Safety-Belangen ist es mittlerweile zur Selbstverständlichkeit geworden, ein umfassendes Risikomanagement zu betreiben, um gewissen Eventualitäten vorzubeugen. Im Security-Bereich herrscht diesbezüglich noch Aufholbedarf. Das ist mit ein Grund, warum wir von T&G dieses Thema vermehrt in den Fokus rücken wollen. Schließlich ist es uns seit jeher ein Anliegen, die produktiven Einrichtungen unserer Kunden möglichst reibungslos und effizient am Laufen zu halten. Mit OpShield können wir diesen Anspruch noch besser erfüllen. Denn diese selbst in bestehende Produktionslandschaften einfach zu implementierende Lösung schützt vor böswilligen Attacken und Fehlkonfigurationen. OpShield gibt vor, wer mit wem über welchen Port bzw. über welches Protokoll welche Inhalte „besprechen“ darf und schlägt sofort Alarm sollten die erlaubten Kommunikationswege verlassen werden. Still und heimlich irgendeine Schadsoftware in eine SPS einschleusen spielt es demnach nicht, weil genau definiert wird, welche Informationen eine bestimmte Steuerung von anderen Netzwerkteilnehmern erhalten darf. Man könnte also sagen: Freund hört mit! Dadurch dass nur „white gelistete“ Datenflüsse zugelassen werden, laufen nämlich auch etwaige Cyberangriffe ins Leere.

■ **www.tug.at**

www.tug.at www.tugsolutions.com