Wirtschaft

06. Okt. 2022 | 09:45 Uhr | von Siegfried Müller

Kolumne

IT-Sicherheit: Die Situation ist paradox und herausfordernd

Es herrscht ein Digitalisierungs- und Sicherheits-Paradoxon, schreibt unser Kolumnist Siegfried Müller. Was er damit meint und wogegen sich Firmen wappnen müssen, lesen Sie hier.

Die größte Herausforderung besteht insgesamt darin, den Cyber-Kriminellen entgegenzuwirken. (Bild: Blue Planet Studio - stock.adobe.com)

Wer hat sich nicht schon einmal gewundert über den Effekt, den die beliebten Social Media-Kanäle auf Menschen ausüben – vor allem im Hinblick auf verschiedene Paradoxe das menschliche Verhalten betreffend, die in diesem Kontext ganz offensichtlich zu Tage treten.

Bekanntermaßen gibt es davon ja einige: Einerseits wünschen sich die Menschen mehr Nähe – also soll, so die Theorie, durch die Möglichkeit der Vernetzung mit Freunden und Bekannten weltweit der zwischenmenschliche Kontakt und Austausch forciert werden. Das führt aber, in der Praxis, andererseits oftmals zu einer Entfremdung mit den engsten Vertrauten.

Wer hat nicht schon einmal die Paare im Restaurant gesehen, die größtenteils stumm vis-a-vis sitzen, weil beide auf ihr Mobiltelefon blicken und ihren Gegenüber höchstens mal kurz ansprechen, etwa um ein Bild von gemeinsamen Bekannten auf Instagram zu zeigen. Oder wer wundert sich nicht, dass die breite Öffentlichkeit ein hohes Maß an Datenschutz fordert – vor allem, wenn es um Daten geht, die eine öffentliche Institution erheben möchte oder muss – aber auf Facebook Menschen alles gerne und ausführlich teilen.

Dies ist – nebenbei bemerkt – eine wahre Fundgrube für Cyberkriminelle, die momentan sehr intensiv genutzt wird für Smishing-Angriffe, also Phishing per SMS. Offenbar werden bei der Nutzung von Social Media-Kanälen alle Bedenken über Bord geworfen und der Schutz der Privatsphäre genauso zur Nebensächlichkeit erklärt wie die (IT-)Sicherheit.

Aber vielleicht sind wir mittlerweile daran gewöhnt, dass unser Verhalten und manch eine Einstellung im Rahmen der Digitalisierung zunehmend widersprüchlich geworden ist. Im Prinzip also wenig erstaunlich, dass es auch ein Digitalisierungs- und Sicherheits-Paradoxon gibt. Denn mit der zunehmenden Digitalisierung einhergehen müsste eigentlich kontinuierlich das Sicherheitsniveau entsprechend zu erhöhen. Dies ist jedoch keineswegs der Fall – viele Unternehmen handeln hier nicht angemessen –, wie sich leicht anhand der zunehmenden Zahl an erfolgreichen Angriffen nachweisen lässt.

Für das paradoxe Verhalten im Bereich Social Media gibt es bereits einige Erklärungsansätze – zum Beispiel, dass der Einzelne den persönlichen Nutzen, den er aus Facebook, Instagram oder TikTok ziehen kann höher gewichtet als die negativen Folgen, die daraus für ihn resultieren. Das ist nachvollziehbar. Aber eine analoge Erklärung für den Bereich IT-/OT-Sicherheit lässt sich für mich daraus nicht ableiten.

Allein unter dem Aspekt, dass es heutzutage möglich ist, immer mehr wertvolle Daten zu generieren – beispielsweise Maschinendaten, die mittels Sensoren beständig

erhoben werden und unter anderem als Basis für die Automatisierung im Rahmen der Smart Factory dienen – wäre die hierzu entsprechende Herleitung unlogisch. Denn die negativen Folgen eines erfolgreichen Angriffs – der aufgrund mangelnder Schutzmaßnahmen durchgeführt werden konnte – sind so immens, dass hier nur schwerlich mit irgendeinem unternehmerischen Nutzen argumentiert werden kann.

Daher halte ich es für essenziell, dass Unternehmen anfangen, das Paradoxon aufzulösen, denn sowohl die aktuelle als auch die zukünftige Sicherheitslage machen ein konzertiertes Vorgehen dringend erforderlich.

Wogegen sich Unternehmen heute wappnen müssen

Die aktuelle Bedrohungslage hat sich im Laufe des Jahres – nach Einschätzung des ‚Bundesamt für Sicherheit in der Informationstechnik' (BSI) – noch verschärft. Dabei ist die momentan meistgenutzte und, aus Sicht der Cyberkriminellen, erfolgreichste Angriffsmethode Ransomware. Denn, dies wird in der Studie „The State of Ransomware 2022" offengelegt, das durchschnittlich bezahlte Lösegeld lässt sich mit 253.160 Euro beziffern. Insgesamt betragen die durch Ransomware verursachten Kosten über 22 Milliarden Euro, allein in Deutschland.

Nach Meinung der meisten Experten wird diese Summe jedoch noch weiter ansteigen – obwohl die Risiken, die mit dem Angriffsvektor einhergehen bekannt sind: denn laut dem Cyber Risk Index (CRI) von Trend Micro bereiten insbesondere die sehr zielgerichteten und komplexen Angriffsmethoden den Verantwortlichen die größte Sorge. Diese Befürchtungen sind definitiv berechtigt, denn die Erkenntnisse verschiedener Sicherheitsexperten machen deutlich, dass die Methoden des Advanced Persistent Threat (APT) weiterentwickelt wurden; mit anderen Worten, ein APT-Angriff ist so intelligent konzipiert, dass er dem Angreifer ermöglicht, relativ lange unbemerkt im Unternehmen zu verbleiben.

So kann dieser unter anderem eingesetzt werden, um Wirtschaftsspionage zu betreiben, also mit der Intention in den Besitz sensitiver Informationen zu gelangen – etwa zur Unternehmensstrategie, zu Finanzdaten oder auch, um wertvolles Fertigungs-Know-how abzugreifen. Daneben darf jedoch die Möglichkeit eines Angriffs, der nicht dediziert auf ein Unternehmen ausgerichtet ist, keinesfalls unbeachtet bleiben – insbesondere von mittelständischen Unternehmen. Denn aus der Perspektive der Angreifer ist dies von daher effektiv, da sie hier gezielt ungepatchte Schwachstellen ins Visier nehmen und deren Zahl ist, laut Trend Micro, im Vergleich zum Vorjahr um 23 Prozent gestiegen.

Ausblick – die Herausforderungen von morgen

Die Komplexität in der IT nimmt kontinuierlich zu, es werden zunehmend neue Anwendungen und Werkzeuge im Unternehmen implementiert, ohne dass die neuen Technologien entsprechend unter dem Aspekt der IT-Sicherheit verifiziert und vorab organisatorisch in die IT-Sicherheitsstrategie integriert worden sind.

In Bezug auf Lieferketten gehen Experten davon aus, dass hier sowohl die Qualität als auch Quantität der Angriffe zunimmt, da dieser Angriffsvektor höchsteffizient ist – denn mit der Ausnutzung einer einzigen Schwachstelle bei einem Dienstleister können gleich hunderte von Unternehmen attackiert werden. Bereits heute nennen 53 Prozent der Teilnehmer des ‚2022 OT Cybersecurity Survey Report' Supply Chain-Angriffe „als eine ihrer drei größten Sorgen". Zu Recht: denn jedes Unternehmen ist darauf angewiesen, dass alle Beteiligten in der Lieferkette sich adäquat absichern – das eigene Schutzniveau ist somit nur so stark wie das des schwächsten Gliedes in der Lieferkette.

Die größte Herausforderung besteht insgesamt darin, den Cyber-Kriminellen entgegenzuwirken. Denn diese sind mittlerweile größtenteils in Ökosystemen organisiert, um die Effizienz und Erfolgsaussichten der Angriffe zu erhöhen. Auf diesem Wege lässt sich sehr viel Geld verdienen, was intelligent in die Entwicklung neuer Angriffsmethoden ‚re-investiert' wird. Das heißt, parallel zu der gestiegenen Komplexität der IT wird die Herangehensweise der Angreifer ebenfalls zunehmend komplexer und anspruchsvoller. Erschwerend kommt hier die Tatsache hinzu, dass sich durch die flächendeckende Digitalisierung gleichzeitig die potenzielle Angriffsfläche beständig vergrößert, nicht zuletzt, weil zusätzlich immer mehr digitale Werte geschaffen werden.

Mein Fazit

Wir müssen Wege finden, mit der Sicherheitslage umzugehen und nicht nur gegen die aktuellen Bedrohungen adäquat aufgestellt, sondern auch für zukünftige Bedrohungen besser gewappnet sein. Denn bereits heute ist jeder zehnte Sicherheitsvorfall gravierend, da die Angriffe zunehmend ausgereift sind, wodurch sich der Prozess bis zum Wiederanlauf aufwendiger gestaltet, und somit weitaus höhere Schäden verursacht werden – etwa durch die längeren Stillstände der Produktionsanlage.

Es gibt Optionen, wie Unternehmen das Digitalisierungs- und Sicherheits-Paradox auflösen – diese werde ich in meinen beiden nächsten Kolumnen näher beleuchten.

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.