Wirtschaft

03. Mär. 2023 | 08:15 Uhr | von Siegfried Müller

Kolumne

Cybersecurity: Das müssen Sie für 2023 wissen

Derzeit zielen Cyberattacken verstärkt auf Industrieunternehmen ab. Unser Kolumnist Siegfried Müller erklärt, warum das so ist und was Firmen jetzt unternehmen müssen.

Unternehmen müssen sich verstärkt um ihre IT- und Cybersicherheit kümmern. (Bild: makstorm - stock.adobe.com)

Das neue Jahr hat gerade erst begonnen und schon gibt es einige Sensationsmeldungen. Eine war relativ vorhersehbar: es lässt sich bereits jetzt rechnerisch nachweisen, dass „Avatar – The Way of the Water“ – trotz einem mageren Startwochenende – der erfolgreichste Film aller Zeiten ist.

Mit dem (bislang) weltweit generierten Einspielergebnis von 2,9 Milliarden US-Dollar liegt dieser unangefochten an erster Stelle im entsprechenden Ranking der Kinofilme.

2,9 Milliarden – diese Zahl hört sich gigantisch an und jeder, der sie hört ist wahrscheinlich tief beeindruckt davon. Doch im Vergleich zu den Summen, die durchschnittlich durch Cyberangriffe eingenommen werden – allein in 2021 im Bereich Ransomware 20 Milliarden US-Dollar – ist dieser Betrag gar nicht mehr so respekteinflößend.

Doch es gibt auch gute Meldungen im Bereich Cybersicherheit – wie beispielsweise Ende Januar, dass die Ransomware-Gruppe Hive zerschlagen werden konnte. Oft währt dann die Freude nicht lange. Denn sofort kommt ein „Aber“. Verständlicherweise, denn die Angreifer – hier vor allem die Hintermänner und Entwickler – sind so gut organisiert und verfügen nicht nur über umfassende finanzielle Mittel, sondern auch über eine hervorragende Infrastruktur sowie die fortschrittlichsten Werkzeuge. Gute Voraussetzungen, die dem Netzwerk eine Restrukturierung wahrscheinlich leicht ermöglicht. Oder ein Teil davon formiert sich einfach neu.

Mit Cyberattacken kann großer Schaden angerichtet werden

Hinzu kommt, dass die guten Nachrichten zumeist sowieso von den schlechten übertrumpft werden. Denn fast zeitgleich wurde darüber berichtet, dass bislang etwa 24 Hochschulen sowie Universitäten von Cyberangriffen betroffen gewesen seien – unter anderem Freiburg, Leipzig und Wuppertal. Im Fokus steht dabei in erster Linie Forschungsdaten abzugreifen, und zwar in allen relevanten Bereichen – angefangen bei den Technikwissenschaften bis hin zu den Natur- und Sozialwissenschaften – aber natürlich werden hierbei auch jede Menge schützenswerte personenbezogene Daten entwendet.

Kurzum, mit diesen Attacken lässt sich ein großer Schaden anrichten, nicht zuletzt auch, weil oftmals aufgrund dessen eine Hochschule alle Verbindungen zum Internet kappen muss und sich dies negativ auf einen geregelten Lehrbetrieb auswirken kann.

Folglich werden in diesem Jahr die bekannten Gegebenheiten sowohl die Industrie als auch die Gesellschaft im Allgemeinen auf den Prüfstand stellen. Darauf müssen wir uns jetzt gut vorbereiten.

Diese Länder stehen bei Cyberattacken im Zentrum

Es mutet so an, dass bestimmte Gegebenheiten – etwa die weltweit vorherrschende Unsicherheit aufgrund der geopolitischen Lage – zu entsprechenden Reaktionen führen. Wie sich augenblicklich herauszukristallisieren scheint, werden aufgrund dessen Deutschland, Frankreich sowie die USA mehr und mehr im Zentrum der Angriffe stehen. Hinzu kommt, dass auf den einzelnen Unternehmen zumeist ein enormer Druck lastet, da sie mit den vorhandenen (auch finanziellen) Ressourcen und zusätzlich gegebenen Engpässen immer noch optimale Ergebnisse erzielen wollen. Aus dieser wirtschaftlichen Betrachtung könnte ein gravierendes Ungleichgewicht resultieren: weniger oder gleichhohe Investitionen in Cyber-Sicherheitsmaßnahmen stehen immer zahlreicheren und massiveren Cyberangriffen gegenüber.

Allerdings bin ich in diesem Kontext nicht davon überzeugt, dass der Großteil der Anschläge gezielt auf bestimmte Unternehmen oder eben ausgewählte Hochschulen erfolgt, sondern der jeweilige erfolgreiche Angriff eher ein Zufallsprodukt ist. Bildlich gesprochen werfen die Hackergruppen mit ihren Angeln – sprich die bereits erwähnten fortschrittlichsten Werkzeuge – einen Köder aus und warten ab, wer diesen als erster frisst. Ist dann auf dieser Grundlage eine Sicherheitslücke gefunden worden, kann nachfolgend in aller Ruhe präzise ein gezielter Angriff geplant und umgesetzt werden.

Was für produzierende Unternehmen besonders relevant ist

Dass solche opportunistischen Angriffe – unter anderem mit massenhaft versendeten Phishing-E-Mails – momentan verstärkt auf Industrieunternehmen abzielen ist unmittelbar einleuchtend. Zum einen sind diese rein finanziell gesehen ein lohnendes Ziel und zum anderen sind die Mitarbeitenden in den OT-Abteilungen, was das anbelangt, noch nicht so versiert.

Aus diesem Grund sollte in diesem Jahr hier verstärkt das Augenmerk drauf gerichtet werden. Denn die Folgen für produzierende Unternehmen können zum Teil viel drastischer ausfallen als in anderen Sektoren – allein aus dem Grund, dass ein Angriff potenziell zu einem Stillstand in der Produktion führt und dieser oftmals mit hohen Kosten verbunden ist. Von daher sollte die IT-Infrastruktur eines jeden Unternehmens auf mögliche Einfallstore überprüft und für die detektierten Schwachstellen entsprechende Schutzmaßnahmen umgesetzt werden. Hierfür gilt es ein ganzheitliches Sicherheitskonzept zu erstellen, in dem für das vorhandene Risikopotential die notwendigen IT-Sicherheitslösungen festgelegt sind.

Im Rahmen der entsprechenden Strategie muss meines Erachtens bedacht werden, dass Awareness-Schulungen allein nicht genügen, um dem Bedrohungspotential angemessen begegnen zu können. Denn da diese Angriffe rein willkürlich erfolgen ist es – insbesondere im Produktionsumfeld – eher schwierig, die Mitarbeiter richtig vorzubereiten und deren Aufmerksamkeit gleichbleibend hochzuhalten.

Fazit: Unternehmen dürfen nicht mehr zögern

Eigentlich sollten die Wünsche für ein neues Jahr nicht mit mahnenden Worten versehen werden. Doch die Sicherheitslage ist meines Erachtens so, dass dies unvermeidbar ist. Unternehmen dürfen jetzt wirklich nicht mehr zögern und müssen sich um ihre IT- und Cybersicherheit kümmern. Dafür benötigen sie auch Aufklärung und Hilfestellung.

Von daher freue ich mich, dass wir eine neue BSI-Präsidentin haben. Denn sowohl dieses Amt als auch das Organ im Zeichen einer Zukunftsbehörde sind essenziell für das Ansehen von Deutschland im Ausland. Wir müssen zeigen, dass wir der IT- und Cybersicherheit einen hohen Stellenwert einräumen und zukünftig alles tun werden, um feindlichen Angriffen entgegenzuwirken.

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.