Wirtschaft

10. Mär. 2022 | 13:30 Uhr | von Siegfried Müller

Kolumne

Cyberangriffe: Risikobewusstsein muss auch umgesetzt werden

Im Bereich Cybersecurity müssen Unternehmen jetzt zügig ins Handeln kommen und zeitnah Strukturen etablieren, schreibt unser Kolumnist

Viele Unternehmen wurden bereits Opfer von Cyberattacken. (Bild: pinkeyes - stock.adobe.com)

Schnallen Sie sich an? Denken Sie bei diesem Vorgang jedes Mal nach? Zum Beispiel darüber, warum Sie dies tun oder ob Sie vielleicht lieber losfahren würden, ohne sich anzugurten. Wahrscheinlich doch eher nicht, denn die Gurtpflicht besteht jetzt bereits seit über 44 Jahren und hat sich im Laufe der Zeit nicht nur de facto etabliert, sondern auch bestens bewährt. Also warum sollte es sinnvoll sein sich damit auseinanderzusetzen, physikalischen Gesetzen entgegenarbeiten zu wollen oder deren Wirksamkeit keinen Glauben schenken? Ja stimmt – von dieser Analogie Gebrauch zu machen, um damit etwas in Bezug auf die IT-Sicherheit verdeutlichen zu wollen, ist mittlerweile ziemlich abgenutzt. Aber sie passt eben so gut, weil sich mittels offenkundiger Parallelen signifikant etwas verdeutlichen lässt.

Denn, die Gurtpflicht wurde am 1. Februar 1976 aus dem Grund eingeführt, um bei Unfällen volkswirtschaftliche Schäden durch Körperverletzungen und weitere Schadensereignisse abzuwenden. Meines Erachtens ein guter Ansatz, verpflichtend im Sinne der Allgemeinheit etwas zu verfügen, um einen hohen Nutzen daraus für die Gemeinschaft zu erzielen – einfach überzeugend und von daher eigentlich auch gut übertragbar als plausibles Instrument in Bezug auf IT- und Cyber-Sicherheit. Die Notwendigkeit dafür ist offensichtlich, das haben die ersten Wochen im neuen Jahr in aller Deutlichkeit gezeigt.

Es muss mehr zum Schutz der Unternehmen aber auch der Gesellschaft getan werden, da die Angriffswellen der Cyber-Kriminellen definitiv nicht abebben. Doch nicht nur dieser Fakt als solcher sollte uns Kopfzerbrechen bereiten. Denn mittlerweile resultieren daraus keinesfalls nur weitreichende Konsequenzen für die betroffenen Unternehmen – etwa in der Form, dass sämtliche Systeme offline genommen werden müssen, da sie in den allermeisten Fällen durchgängig verschlüsselt sind oder dass zudem ein gezielter Cyberangriff auch in den meisten Fällen den Diebstahl von Daten umfasst, um diese für eine Erpressung zu nutzen.

Cyberangriffe: Der Kreis der Betroffenen erweitert sich graduell

Die Auswirkungen für das jeweilige Unternehmen sind mittlerweile nur eine Dimension der Bedrohungslage, inzwischen kommt noch eine zweite hinzu, der in diesem Kontext zukünftig mehr Bedeutung beigemessen werden muss: die Implikationen in Bezug auf die Gesellschaft. Dies hat der Angriff auf die Tanklager von Oiltanking eindringlich aufgezeigt – mit einem Mal waren direkt völlig Unbeteiligte involviert, weil großflächig Tankstellen in bestimmten Regionen Deutschlands nicht mehr beliefert werden konnten.

Mit anderen Worten, ein Cyberangriff betrifft inzwischen keinesfalls nur das jeweilige Unternehmen in dem Sinne, dass dieses – insbesondere im Produktionsbereich – nicht mehr in der Lage ist den Geschäftsbetrieb aufrechtzuerhalten, wodurch hohe Kosten durch Pönale entstehen können und im schlimmsten Fall zusätzlich ein Reputationsschaden. Sondern im Gegenteil, der Kreis der Betroffenen erweitert sich graduell und es muss zunehmend damit gerechnet werden, dass dies auch die Versorgungssicherheit von Grundbedürfnissen tangieren kann.

Cyberattacken haben auch Folgen innerhalb der Lieferkette

Bei dem Blick auf die Zahl potenziell Geschädigter aufgrund eines Angriffs ist noch eine weitere Thematik von hoher Relevanz: Die Folgen innerhalb einer Lieferkette. Denn mit der Digitalisierung geht eine zunehmende Verzahnung relevanter Prozesse zwischen Unternehmen und Kunden oder Lieferanten einher – die Verknüpfung von Warenwirtschaftssystemen ist heute bereits gang und gäbe. Die Krux dabei: Eine Optimierung wird hauptsächlich unter funktionalen Gesichtspunkten betrieben, ausgerichtet auf die Steigerung der Effizienz. Nicht das Sie mich jetzt falsch verstehen, ich stelle keinesfalls den Nutzen der Digitalisierung infrage.

Doch meines Erachtens ist es wichtig zu sehen, dass damit ein hohes Risiko einhergeht, aber die notwendige Risikobetrachtung eher minimal ausfällt. Dafür mag es Gründe geben. Zum Beispiel, dass das gesamte Ausmaß der Bedrohung nie offensichtlich wird, da immer nur punktuell etwas publiziert wird. Wenn ein Unternehmen erfolgreich angegriffen wurde, dann ist dieser Vorfall zwei Tage sehr präsent, verschwindet dann aber wieder aus den Schlagzeilen und gerät folglich sofort in Vergessenheit. Ein Umdenken setzt oftmals erst ein, wenn ein Angriff auf das eigene Unternehmen stattgefunden hat. Da die Professionalität der Cyberkriminellen konstant steigt, muss mehr getan werden, um vorher ein Risikobewusstsein zu schaffen, dass Unternehmen dazu verleitet die notwendigen Schritte zum Schutz ihrer Systeme und Daten beständig durchzuführen.

Risikobewusstsein in die Umsetzung gebracht

Obwohl die Forderung nach IT- und Cyber-Sicherheit inklusive entsprechend adäquater Umsetzung im Prinzip normativ gesetzt ist, erscheint es fast so als ob Unternehmen daraus keine direkte Bringschuld schlussfolgern. Vielleicht lässt sich dieses Phänomen zum Teil darüber erklären, dass es allgemein schwierig ist, mangelhafte IT-Sicherheitsbedingungen im Unternehmen zu sanktionieren. Denn – im Gegensatz zu einer Verletzung der Gurtpflicht, die ja offensichtlich ist – sind Verstöße im Bereich IT-Sicherheit nicht unmittelbar evident und von daher die Gestaltung und Durchführung effektiver Sanktionsverfahren wesentlich komplexer. Das darf jedoch kein Hinderungsgrund sein.

Zudem faktisch bereits Grundlagen vorhanden sind, aus denen sich entsprechende Normen herleiten ließen, wie zum Beispiel der „Stand der Technik“, anhand derer eine Sanktionierung erfolgen könnte. Wünschenswert wäre natürlich, dass mittelfristig – genau wie bei der Gurtpflicht – daraus resultiert, dass der angemessene Einsatz von IT-Schutzmaßnahmen genauso automatisch erfolgt wie das Anschnallen im Auto.

Aber dies kann natürlich nicht der einzige Weg sein, um die IT- und Cyber-Sicherheit in den Unternehmen zu erhöhen. Ebenso wichtig ist es, hierbei alle Mitarbeiter einzubeziehen, also mittels bedarfsorientierter Schulungen deren Kenntnisse über mögliche Risiken kontinuierlich zu erweitern. Um dies zu realisieren sind verschiedene Ansätze denkbar. Meiner Erfahrung nach erweisen sich dafür teilweise auch Angebote

von einigen Cyberversicherungen als gut geeignet. Denn aufgrund der hier zusammengetragenen Kenntnisse und daraus resultierend aufgebauten Expertise ist es möglich, den Versicherungsnehmern angemessene Instrumente sowie relevante Informationen zur Verfügung zu stellen.

Fazit: Zügig ins Handeln kommen

Meines Erachtens müssen wir jetzt zügig ins Handeln kommen. Das bedeutet für Unternehmen zum einen zeitnah Strukturen zu etablieren, um im Angriffsfall so weit als möglich handlungsfähig zu bleiben. Dies lässt sich unter anderem auch über eine Cyberversicherung gewährleisten. Nebenbei bemerkt – abgesehen von den finanziellen Aspekten lässt sich diese aufgrund der zugesicherten Schadensabdeckung überdies gut als Wettbewerbsvorteil verargumentieren. Ebenfalls wichtig ist, das Unternehmen angemessen zu wappnen und beispielsweise über Notfallpläne eine schnelle Wiederherstellung von essenziellen Funktionalitäten garantieren zu können.

Nichtsdestotrotz sollte jedoch das Hauptaugenmerk darauf ausgerichtet sein, potenzielle Angriffsflächen so weit als möglich zu verringern, um es den Cyberkriminellen tunlichst zu erschweren einen großen Schaden anrichten zu können.

Über den Kolumnisten

(Bild: Siegfried Müller)

Siegfried Müller ist geschäftsführender Gesellschafter der MB connect line GmbH. 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.

Seit über 20 Jahren treibt Siegfried Müller mit viel Engagement und Leidenschaft die Entwicklung neuer Produkte und Lösungen für die sichere industrielle Kommunikation über Internet voran. Als Stratege und Experte zur Cybersicherheit im industriellen Umfeld bringt er sein Wissen auch in nationalen und internationalen Arbeitskreisen ein – beispielsweise beim Cluster Mechatronik & Automation Bayern e.V., beim TeleTrusT – Bundesverband IT-Sicherheit e.V. und in der European Cyber Security Organisation (ECSO). Die wichtigen wirtschaftlichen Themen adressiert er als Senator im internationalen Wirtschaftssenat (IWS).