RMA
Risk Management & Rating Association e.V.

Cybersicherheit heißt auch: Vor die Lage kommen

Andreas Eicher

„Die Menschheit digitalisiert sich. Immer mehr Daten, immer neue Vernetzungen und immer komplexere Systeme führen leider auch zu immer neuen Schwachstellen und Einfallstoren für kriminelle Machenschaften. Zum Schutz fehlt es vielerorts an Know-how, Personal und den nötigen Mitteln.“

Dass Chancen und Risiken oft eng beieinander liegen, verdeutlichen die Autoren des Magazins „Cybersicherheit in Zahlen“ wenn sie schreiben: „Die Menschheit digitalisiert sich. Immer mehr Daten, immer neue Vernetzungen und immer komplexere Systeme führen leider auch zu immer neuen Schwachstellen und Einfallstoren für kriminelle Machenschaften. Zum Schutz fehlt es vielerorts an Know-how, Personal und den nötigen Mitteln.“ Bei Letzteren wird oft am falsche Ende gespart, was die vielen Cybervorfälle der vergangenen Jahre verdeutlichen. Zu lange haben Unternehmen und deren Geschäftsleitungen die Augen vor den Risiken der Cybergefahren verschlossen oder nur halbherzig geöffnet. Damit müsste das Einstiegszitat ergänzt werden, um die Vokabeln Risikobewusstsein, Sensibilisierung und den Halbsatz – im Sinne einer umfassenden Cybersicherheit. Denn jeder erfolgreiche Cyberangriff ist einer zu viel. Um am Ende die Chancen der Digitalisierung zu wahren, gilt es für Organisationen die Risiken zu begrenzen. Eine Aufgabe, die mehr Risikobewusstsein von allen Beteiligten erfordert. Ein klarer Auftrag an die Führungsetagen in den Unternehmen.

Was haben der Batteriehersteller Varta, der Hörgerätehersteller Kind und das Dreifaltigkeits-Hospital in Lippstadt gemeinsam? Alle wurden kürzlich Opfer von Cyberattacken. Dabei zeigt sich: Angriffe auf Organisationen und deren IT-Infrastrukturen gehen quer durch alle Branchen. Zudem liegen die Straftaten im Bereich des Cybercrime nach Aussagen des Bundeskriminalamts (BKA) „weiter auf einem sehr hohen Niveau." In Zahlen ausgedrückt heißt das nach BKA-Informationen, dass „über 130.000 Fälle von Cybercrime in 2022" registriert wurden. Die Dunkelziffer dürfte weitaus höher liegen. Der geschätzte Gesamtschaden für die deutsche Wirtschaft beläuft sich laut Digitalverband Bitkom auf „206 Milliarden Euro (…) pro Jahr durch Datendiebstahl, Spionage und Sabotage".

206 Mrd. €

geschätzter Gesamtschaden für die deutsche Wirtschaft durch Datendiebstahl, Spionage und Sabotage

Vom reaktiven Lagezentrum und dem Rückspiegel

Die Zahlen beunruhigen die deutsche Wirtschaft, von der sich 52 Prozent der Betriebe durch Cyberangriffe in ihrer Existenz bedroht fühlen. Gleichfalls verkündet Bitkom-Präsident Dr. Ralf Wintergerst: „Die deutsche Wirtschaft ist ein hoch attraktives Angriffsziel für Kriminelle und uns feindlich gesonnene Staaten." Und was machen die Behörden vor dem Hintergrund der anhaltend hohen Bedrohungslage im Cyberumfeld? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) eröffnete Anfang Februar 2024 das neue „Nationale IT-Lagezentrum" in Bonn. Als „Herz der operativen Cyberabwehr für Deutschland" umschrieben, bewerben die handelnden Personen das IT-Lagezentrum unter anderem mit neuester Medientechnik und einem multifunktionalen Raumkonzept. Hinzu kommen Experten und Teams unterschiedlicher Bereiche, die im Rahmen oder außerhalb der Bürozeiten die Cybersicherheitslage überwachen sollen. „Lage erkannt – angemessen reagieren", heißt es auf den entsprechenden Seiten zum IT-Lagezentrum. Mit Blick auf die digitale Bedrohungslage hierzulande wirft das zumindest Frage auf, ob ein solches IT-Lagezentrum dem Cybersicherheitsumfeld mit seinen vielfältigen Risikoszenarien überhaupt gerecht werden kann. Eine klare Antwort darauf hat Marco Wolfrum, stv. Vorstand der RMA Risk Management & Rating Association e.V.: „Das viel zitierte ‚Vor die Lage kommen' lässt sich mit einem reaktiv ausgelegten Lagezentrum wohl weniger realisieren." Damit meint Wolfrum: „Cybersicherheit braucht ein aktives und vorausschauendes Auseinandersetzen mit den Risiken, aber auch den Chancen disruptiver Technologien im digitalen Zeitalter." Ansonsten bestehe seiner Meinung nach die Gefahr lediglich in den Rückspiegel der Ereignisse zu schauen und Risiken zu verwalten.

Kein neues Thema, trotz KI

Apropos Zeitalter. Dass das Thema der Cyberkriminalität kein Neues ist, verdeutlicht die lange Historie und „Erfolgsgeschichte" an Schadprogrammen. „Creeper" und „Reaper" hießen die ersten bekannten Computerwürmer in den 1970er-Jahren. Seither gab es zahllose neue Computerviren, Trojaner und Spyware, um Cyberangriffe auf Unternehmen, Behörden, die Politik und wissenschaftliche Einrichtungen durchzuführen. Und mit jeder neuen Entwicklungsstufe der Digitalisierung wachsen gleichzeitig die Bedrohungsmöglichkeiten mittels Malware, Phishing, DDoS-Angriffen & Co. In unseren Tagen gehört auch der vermehrte Einsatz der künstlichen Intelligenz (KI) zur Klaviatur von Cyberkriminellen – ob staatlich gelenkt oder von professionellen und arbeitsteiligen Hackergruppen genutzt. So sieht unter anderem die Bitkom den KI-Einsatz als neue Herausforderung für die Cybersicherheit. Das heißt: „57 Prozent der Unternehmen sehen Gefahren durch KI". Eine Erkenntnis, die sich im „Bundeslagebild 2022" des BKA wie folgt liest: „KI wurde bereits zur automatisierten Erstellung von Phishing-Nachrichten, für Desinformationskampagnen oder zur Entwicklung von Malware ausgenutzt." Zudem erwarten die BKA-Experten eine „weitergehende kriminelle Ausnutzung von KI-Methoden, beispielsweise zur (Weiter-) Entwicklung eingesetzter Werkzeuge und Angriffsvektoren". Vorausschauend erkannte die Allianz mögliche KI-Risiken für die Unternehmenssicherheit bereits im Jahr 2018: „Künstliche Intelligenz (KI) macht Unternehmen anfälliger für Großschäden durch Cyberangriffe und technisches Versagen."

Das fehlende Risikobewusstsein

Aus all diesen Informationen und Erfahrungen mit der Cybersicherheit der letzten Jahrzehnte und den neuen Herausforderungen vor Augen wäre eine steile Lernkurve im gesamten Risiko- und Sicherheitsdenken zu vermuten. Doch weit gefehlt. In vielen Unternehmen sind das notwendige Risikobewusstsein und die Sensibilität hinsichtlich der eigenen Cybersicherheit nicht oder zu wenig

Andreas Eicher

Autor, (Wissenschafts-) Journalist, Redakteur, Schwerpunktthemen: Digitalisierung, Geo-IT, Risikomanagement, Smart-City-Entwicklungen, Technologie- und Wissenschaftstransfer

Cybersicherheit im Kontext des Krisen- und Risikomanagements

Die RMA Risk Management & Rating Association bietet vielfältige Möglichkeiten, sich mit dem Thema Cybersicherheit im Kontext des Krisen- und Risikomanagements zu beschäftigen. Dank zahlreicher Arbeitskreise und deren Schnittstellen zum Cyberumfeld können Risikomanager neue Impulse und Ideen für die eigene Organisation mitnehmen. Hierzu zählen unter anderem die Arbeitskreise „Krisenmanagement", „Information Risk Management" und „Risikomanagement-Standards". Hinzu kommen die Weiterbildungsmöglichkeiten zum Enterprise Risk Manager (Univ.) und Fernstudienprogramme sowie ein umfassendes Seminar-, Webinar- und Konferenzangebot, wie beispielsweise der jährlich stattfindende Risk Management Congress.

Weitere Informationen:

vorhanden; trotz der eindeutigen Zahlen und Fakten. Das Wirtschaftsmagazin Brand eins umschreibt es in seiner Lektüre „Cybersicherheit in Zahlen" so: „Cybersicherheit ist (...) in der Vergangenheit nicht an zu wenig Informationen gescheitert. Was gemeinhin fehlt, ist das Gefühl für die Gefahren in der digitalen Welt – und die Bereitschaft, sich mit der Materie auseinanderzusetzen". Das unterstreicht eine Umfrage von Sharp vom September 2023. Die kommt zu der Erkenntnis, dass zwei Drittel (66 Prozent) der kleinen und mittleren Unternehmen (KMU) „kein Vertrauen in den Umgang ihres Unternehmens mit Cyberrisiken" haben. Doch genau dieses Vertrauen sollten Mitarbeiter haben und dafür muss das Unternehmen die notwendigen Schritte einleiten. Denn die bekannte Frage ist nicht, ob es einen Cyberangriff auf die eigene Organisation geben wird, sondern wann. In diesem Kontext kommt der Geschäftsleitung eine Führungsrolle zu. Für Marco Wolfrum ein klarer Handlungsauftrag an die Leitungsebene des jeweiligen Unternehmens. Konkret heißt das für ihn: „Die Geschäftsführung muss geeignete Maßnahmen ergreifen, um die Informationssicherheit in der eigenen Organisation sicherzustellen."

Geschäftsführer als oberste Risikomanager

Neben der Sorgfalts- und Legalitätspflicht sieht Risikomanagementexperte Wolfrum vor allem die Pflicht zur Einrichtung von Überwachungssystemen als einen zentralen Punkt an. So heißt es in § 91 Abs. 2 Aktiengesetz: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." Weiterführend sind die gesetzlichen Pflichten für Vorstände börsennotierter Gesellschaften in Abs. 3 benannt. Darin wird die Einrichtung eines angemessenen und wirksamen internen Kontroll- und Risikomanagementsystems gefordert. Hinzu kommt das am 1. Januar 2021 in Kraft getretene Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG). In diesem heißt es hinsichtlich der Krisenfrüherkennung und des Krisenmanagements bei haftungsbeschränkten Unternehmensträgern: „Die Mitglieder des zur Geschäftsführung berufenen Organs einer juristischen Person (Geschäftsleiter) wachen fortlaufend über Entwicklungen, welche den Fortbestand der juristischen Person gefährden können. Erkennen sie solche Entwicklungen, ergreifen sie geeignete Gegenmaßnahmen und erstatten den zur Überwachung der Geschäftsleitung berufenen Organen (Überwachungsorganen) unverzüglich Bericht." Damit sieht der Gesetzgeber die klare Handlungs- und Überwachungspflicht bei der jeweiligen Geschäftsleitung und fordert geeignete Maßnahmen bei bestandsgefährdenden Entwicklungen. Und zu denen gehören Cybergefahren – von Datendiebstählen über Sabotagen bis zu Erpressungen – mit all ihren unabsehbaren Folgen in puncto Kosten und Reputationsverlusten für Unternehmen. Daraus folgert Marco Wolfrum: „Im Grunde ist der Geschäftsführer damit der oberste Risikomanager eines Unternehmens und muss eine aktive Rolle im gesamten Krisenfrüherkennungs- und Risikomanagementprozess einnehmen." Ein Prozess, der nach Wolfrums Dafürhalten bis zur Überwachung der Wirksamkeit und möglichen Neujustierung der jeweiligen Maßnahmen im Cybersicherheitsumfeld reiche.

Mensch und Wissensmanagement

Bei allen technischen Entwicklungen, mit deren Hilfe die Cybersicherheit in Organisationen verbessert werden soll, kommt den Menschen vor Ort die entscheidende Rolle zu. Das heißt: Wir reden hier nicht vom „Faktor" Mensch, sondern dem Mitarbeiter. Ohne ihn wird es keine umfassende Cybersicherheit geben. Leider haben das längst nicht alle handelnden Personen in den Führungsetagen deutscher Unternehmen verstanden. Und so herrscht nicht selten der Glaube vor, dass Organisationen die wichtigen IT-Security- und Risikomanagement-Funktionen und Unwägbarkeiten rein Software-getrieben lösen könnten. Das Ganze ähnelt einer Art modernem Ablasshandel und endet meist in einer Sackgasse. Denn in vielen Fällen werden damit Einzelrisiken betrachtet, ohne sich über die Gesamtrisikosituation im Unternehmen bewusst zu sein. Im Umkehrschluss heißt das für die Cybersicherheit einer Organisation: „Je mehr Wissen, desto mehr Risikobewusstsein", wie es das Magazin „Cybersicherheit in Zahlen" formuliert. Darin schwingt die Aufforderung mit, das Wissensmanagement in der eigenen Organisation zu forcieren. Das heißt, Mitarbeiter qualitativ besser im Umgang mit Cyberrisiken zu schulen und vor den Gefahren zu sensibilisieren. Für Marco Wolfrum muss die Geschäftsleitung solche Schulungs- und Awareness-Strukturen initiieren. Mehr noch: „Das Topmanagement tut gut daran, eine frühzeitige, klare und transparente Krisenkommunikation in der gesamten Organisation zu fördern", erklärt Wolfrum. Und er resümiert: „Nur so lassen sich alle Mitarbeiter in den Prozess der Schulungs- und Awareness-Programme einbinden." Das hilft, die Cybersicherheit sowie die organisationsweite Resilienz zu stärken und letztendlich eine gemeinsame Risikomanagementkultur im Unternehmen aufzubauen. Wichtige Bausteine jeder Organisation. Denn die bekannte Frage ist nicht, ob es einen Cyberangriff auf die eigene Organisation geben wird, sondern wann.