Cyber-Security betrifft fast alle Unternehmensbereiche.

Was geht Cyber-Security die Unternehmensleitung an?

Cyber-Security ist mehr als nur ein IT-Thema und betrifft alle Stufen einer Unternehmung. Gerade deshalb muss sich zwingend auch die Unternehmensführung darum kümmern. Der Beitrag liefert Denkanstösse zum Reflektieren.

Almut Eger

Cyberangriff, das Wort ist in aller Munde. Kaum eine Unternehmenssicherheit, die sich in den letzten zwei Jahren nicht damit befasst hat. Auch in Trainings mit Notfall- und Krisenstäben hatte dieses Thema Hochkonjunktur. Das liegt unseres Erachtens daran, dass erstens noch ein grosses Unbehagen besteht im Verständnis, was ein Cyberangriff bedeutet. Zweitens haben einige reale Ereignisse aufgezeigt, welche Auswirkungen die digitale Vernetzung von Informationen, die für die eigene Firma einiges an Vorteilen mit sich bringt, erreichen kann.

Ein bekanntes Beispiel ist der «WannaCry»-Verschlüsselungstrojaner aus dem Jahr 2017. Innert Kürze breitete sich ein Zustand aus, der Teile des öffentlichen Lebens lahmlegte (z.B. Deutsche Bahn), Firmen der kritischen Infrastrukturen kurzzeitig vom Markt nahm (z.B. Logistik-Konzern Maersk), Ängste in der Grundversorgung auslöste (z.B. Stromverteilung in einem europäischen Land).

«WannaCry» hat wachgerüttelt. Der Computerwurm hat hervorgerufen, was viele Experten schon zuvor äusserten: Es geht nicht um die Frage, ob ein bestimmtes Unternehmen getroffen wird, sondern wann.

Und somit steht sofort die Anforderung im Raum: Es ist nicht die Frage, ob sich Unternehmen und Privatpersonen um Cyber-Security kümmern müssen, sondern wo und in welchem Ausmass.

Mit anderen Worten: Cyber-Security geht alle etwas an – sie beginnt im täglichen Leben, sowohl privat wie auch am Arbeitsplatz. Die Gesellschaft lebt in einer vernetzten Welt:

– Die Nutzung von Daten und Informationen ist nicht mehr auf definierte Räume (z.B. Arbeitsplatz) und Geräte (z.B. Firmenhandy) eingrenzbar, denn

das «flexible Arbeiten» entspricht der heutigen Vorstellung von Kreativität, Produktivität, Teamergebnissen und Work-Life-Balance mehr als fixe Arbeitseinheiten in Raum und Zeit. Ausserdem nähren wirtschaftliche Interessen die Bestrebungen, die Fixkosten pro Arbeitsplatz so tief wie möglich zu halten, und damit die Weiterentwicklung der flexiblen Arbeitsweisen.
- Damit brechen aber auch Sicherheitseinrichtungen auf, Einfallstore für Cyberangriffe werden unwissentlich geöffnet.
- Die Nutzung von Daten und Informationen ist nicht mehr in ihrer Bestimmung eingrenzbar, denn für die Kombination von Daten stehen so viele wertvolle Nutzerinteressen Schlange, dass es trotz der Gefahren kaum Mehrheiten gibt, diese digitalen Errungenschaften rückgängig zu machen (z.B. Anzeigen des Verkehrsaufkommens auf Googlekarten oder Anwenderentwicklungen mit Big-Data-Technologien für bedarfsgerechte Zugbereitstellung für Pendler).
- Die Digitalisierung schreitet fast im Gleichschritt voran mit der Individualisierung: Je individueller Käufer ihre Produkte gestalten können, umso mehr Einzelheiten müssen im Internet auffindbar, austauschbar und kombinierbar sein, womit Manipulationen respektive Cyberangriffe einfacher möglich sind.

Das Loch in der Mauer

Es ist eine einfache Rechnung: Je mehr ausgetauscht, geredet und gehandelt wird, umso mehr entstehen Fehler, Lecks und Löcher, die keiner wollte, keiner sah. Umso mehr entstehen Kombinationen, an die keiner gedacht hatte und für die noch keine «Security» vorhanden ist. Das Loch in der Firewall war gestern, die ungewollt zu grosse Sicherheitsmasche im Kettenhemd der Unternehmens-IT ist heute.

Cyber-Security trifft deshalb fast alle Unternehmensbereiche. Aus der Vielzahl von Themen greifen wir hier nur einzelne heraus, um die Reflektion über Auswirkungen im eigenen Unternehmen anzustossen:

1. Personal: Verhaltensregeln zu Informationssicherheit sind unumgänglich, aber gehören oft zu den am meisten gebrochenen Regeln im Unternehmen.

2. Gebäudesicherheit: Badges und Zutrittslösungen beinhalten Zugangscodes. Vernetzungen dieser Systeme mit anderen Einheiten wie z.B. Logistik- oder Personaldaten bieten ein ideales Einfallstor für unrechtmässige Schadsoftware.

3. Kommunikationslösungen: Die Vernetzung mit Providern und Dienstleistern für Kernapplikationen öffnen das komplette Kommunikationsnetz des Unternehmens. Umso wichtiger sind deshalb gut abgestimmte Vorkehrungen seitens Dienstleister und Unternehmung, im Falle eines Cyberereignisses Schäden eindämmen zu können.

4. Dienstleister: Auch die Diskussion um die optimale Unternehmensgrösse des Dienstleisters sollte unter dem Aspekt der Cyber-Security geführt werden: In ein grösseres Unternehmen wird tendenziell mehr Vertrauen zur «richtigen Reaktion» im Ereignis geschenkt (Bsp. Anbieter von Telekommunikations- oder ERP-Lösungen); und das, obwohl erkannt ist, dass im Fall eines Ereignisses beim Dienstleister die negativen Auswirkungen für die eigene Unternehmung fast unermesslich und kaum mehr steuerbar sein werden. Im Gegensatz dazu erbringt ein kleiner Anbieter eine überschaubare Leistung, womit ein allfälliger Schaden bei einem Cyberereignis ebenfalls besser abschätzbar und eingrenzbar erscheint. Hingegen fehlt hier oft das Vertrauen, dass ein kleinerer Anbieter die nötige Schlagkraft aufbringen kann, ein Cyberereignis angemessen zu verdauen, um weiterhin als Anbieter zur Verfügung zu stehen.

> «Grundregeln der Informationssicherheit müssen konsequent durchgesetzt werden.»

5. Legal & Compliance: Jedes Cyberereignis deckt Löcher auf, Ungereimtheiten in Abläufen und Zuständigkeiten, ein auch noch so kleines Nichtbeachten von Vorgaben. Es geht meist um ganz alltägliche Dinge, «die eigentlich jeder und jede kennt», wie im Nachhinein häufig gesagt wird:
- Die ungewollte, aber eben unrechtmässige Weiterverbreitung von Personendaten über den so oft benutzten Messengerdienst Whatsapp, der mit «Bring your own device» und der DSGVO eine Vielzahl von juristischen Verletzungen bereithält.
- Die Vermischung von privatem und geschäftlichem Mailverkehr, womit Sicherheitslücken in der Informationssicherheit aufgebrochen werden.
- Die Weitergabe von Informationen, die einzeln zwar kaum nutzbar sein können, in der Kombination mit anderswo erhaltenen Informationen aber das fehlende Element für das Einfallstor eines Cyberangriffs sind.

Strategische Rahmenbedingungen

Cyber-Security begleitet also Unternehmensleitungen täglich und in fast jeder Entscheidung. Aus den unendlich vielen Fragestellungen seien hier nur ein paar wenige herausgegriffen: Fragestellungen, die direkt kritische Geschäftsprozesse und/oder kritische Ressourcen betreffen. Denn zu diesen Fragen ist es umso wichtiger, dass strategische Rahmenbedingungen vorliegen – die von der Unternehmensleitung definiert werden müssen!

Bezüglich Informations- und Kommunikationstechnologien (ICT):
- das Verabschieden einer umsichtigen ICT-Strategie
- die gute Besetzung der IT-Stellen mit vernetzt denkenden Persönlichkeiten, welche die Möglichkeiten, Chancen und Gefahren der ICT-Entwicklung im Einklang mit der Unternehmensentwicklung im Auge haben können (z.B. Nutzen von «Big Data»-Quellen zum Generieren von Kundennutzen)
- das konsequente Umsetzen von Grundregeln der Informationssicherheit (z.B. entlang der Vorgaben aus Normen wie ISO 27001 ff)

Bezüglich Personal: Grundregeln der Informationssicherheit müssen konsequent durchgesetzt werden. Effizient organisierte und gut/richtig gelebte Informationssicherheit geht 1:1 einher mit Cyber-Security. Deshalb ist die Schulung allen Personals im richtigen Verhalten in allen Situationen (privat und geschäftlich) eine ebenso wirksame Präventionsmassnahme wie IT-Sicherheitsvorkehrungen für Datenhaltung und -austausch. (Aber: Dies kostet auch annähernd gleich

PROZESSBEZOGENE AUSWIRKUNGEN EINES CYBERANGRIFFS

Mögliche nicht «IT-bezogene», sondern prozessbezogene Auswirkungen eines Cyberangriffs in einem Unternehmen:

- Kommunikation ist nicht mehr möglich oder stark eingeschränkt (Voice over IP, Mail-Verkehr).
- Zutrittssysteme funktionieren nicht wie gewohnt, sondern nur im Ausnahmezustand wie beispielsweise bei einem Brandfall (z.B. Türen und Hintereingänge stehen ungesichert offen).
- Gebäudetechnik reagiert fremdgesteuert (z.B. Temperaturanstieg, blockierte Rollläden).
- Technische Einrichtungen reagieren fremdgesteuert (z.B. Liftanlage).
- Unternehmensspezifisches Know-how fliesst ab (z.B. via Daten und Dokumente, aber auch via mitgelesene Mails).
- Strategische Entscheide werden Mitbewerbern ungewollt bekannt.
- Die Zusammenarbeit mit einem Schlüsseldienstleister muss komplett aufgegeben werden.
- Die Zahlung von Lösegeld in Millionenhöhe bringt nicht nur finanzielle Schwierigkeiten mit sich, sondern auch rechtliche (z.B. welcher Weg muss begangen werden, um innert drei Stunden 5000 Bitcoins aufzutreiben und zu überweisen, ohne rechtliche Vorgaben des Handels mit Kryptowährungen zu verletzen?).
- Mitarbeiter arbeiten auf Basis falscher Daten und generieren nicht nur Fehler, sondern auch viele unbrauchbare Ergebnisse.
- Eine Unmenge an Handarbeit ist notwendig, um Daten wieder herstellen zu können (z.B. Neuaufbau ERP-Inhalte). Während dieser ganzen Zeit kann produktive Arbeit nur sehr begrenzt stattfinden.
- Die Verunsicherung der Mitarbeitenden ist enorm. Nicht nur, weil der gewohnte Zugriff auf Daten nicht möglich ist, sondern auch weil den noch vorhandenen Daten nicht mehr getraut wird. Allein das kann einen Businessprozess lahmlegen.
- Für einen betroffenen Businessprozess existiert kein Schutznetz aus Workaround, Notfall- und Wiederanlaufplänen, weil niemand via Business Continuity Management System daran gedacht hat, dass ein Wegfall dieses Prozesses heikel oder gar kritisch sein könnte. Das Wegfallen dieses einen Prozesses ist denn auch jetzt kein Problem, die Folgewirkungen auf andere Prozesse hingegen schon.

Ein Cyberangriff kann auch prozessbezogene Auswirkungen haben, wie z.B. auf Zutrittssysteme.

viel – nur ist das häufig kaum bewusst, denn Mitarbeiterkosten werden meist anders berechnet.)

Bezüglich Lieferanten und Dienstleistern: Das Unternehmen muss erkennen, welche Sicherheitsvorkehrungen garantiert werden und wie diese mit den eigenen Anforderungen übereinstimmen.

Bezüglich Legal & Compliance:

- das Erkennen, ob und in welchem Mass Informationssicherheit gefährdet ist
- das Erkennen, welches unternehmensspezifische Wissen, Daten, Dokumente etc. das Haus verlassen haben oder noch verlassen könnten

Schlüsselfragen der Unternehmensleitung

Die Unternehmensleitung muss sich also vorab mit den Auswirkungen eines Cyberangriffs auseinandersetzen. Und das im täglichen Geschäft.

Das ist auch im Fall eines Cyberangriffs so. Schlussendlich sind seitens IT «nur» ein paar Schlüsselfragen massgebend, die von der Unternehmensleitung beantwortet werden müssen. Aber die haben es in sich. Beispiele dafür sind:

- Soll ein Basissystem komplett abgekoppelt werden: ja oder nein?
- Das heisst, es kann danach auf keine Services mehr zugegriffen werden, sei es auf ein ERP mit Kundendaten, sei es die Erreichbarkeit von Dienstleistern (die zur Aufarbeitung des Schadens nötig wären), sei es ein Check von Passwörtern etc. Eventuell geht sogar das E-Mailen nicht mehr.
- Soll die Verbindung des Unternehmens mit dem Internet gekappt werden: ja oder nein?

Das heisst, das Unternehmen ist dann via Internet nicht mehr erreichbar, für den Angreifer nicht, aber auch nicht für Kunden, Mitarbeiter, Dienstleister mit Service-Programmen zur Reparatur von Datenbanken.

Die Auswirkungen seitens IT können von Unternehmensleitungen selten in ihrer vollen Konsequenz beurteilt werden, die Auswirkungen auf die Businessprozesse hingegen schon. Und da ist die breite Sicht auf das Unternehmen gefordert, die Vernetzung von Kenntnissen aus allen Bereichen.

Das «Leben der Unternehmung» findet normalerweise im Verbund mit der Aussenwelt statt. Und das ist im Fall eines Cyberangriffs auf gewohntem Weg nicht mehr möglich. Das neu zu organisieren, ist Aufgabe der Unternehmensleitung. Schäden an Daten, Algorithmen, Informationskanälen etc. zu reparieren, ist Aufgabe der IT in Zusammenarbeit mit Businessvertretern und Dienstleistern.

Fazit

Obwohl Cyber-Security alle Stufen einer Unternehmung etwas angeht, wird es häufig nur als «IT-Thema» verstanden. In der technischen Umsetzung von Cyber-Security mag das etwas Wahres für sich haben. Im Umgang mit Auswirkungen von Cyber- und Informationssicherheit sind Themenfelder der Unternehmensführung, Mitarbeiterführung und Verständnis von unternehmenseigenem Know-how und vieles mehr relevant. Themen, um die sich letztlich die Unternehmensführung kümmern muss, im Alltag wie im Ereignis. ■

ALMUT EGER
Senior Consultant und Trainerin für Notfall-/Krisenmanagement, BCM und ISMS bei 4m2s – 4 Management 2 Security GmbH, Zürich und Frankfurt, Auditorin für TÜV Rheinland Cert