Cyberresilienz

Digitale Transformation? Sicher!

Die Möglichkeiten der digitalen Transformation sind gewaltig: leichterer Marktzugang, neue Geschäftsmodelle, schnelle Skalierbarkeit, neue Wertschöpfungsketten, einzigartige Kundenerlebnisse und nicht zuletzt riesige Datenmengen – das neue Gold. Umso mehr verwundert die Sorglosigkeit, die oft im Umgang mit den Risiken der Digitalisierung herrscht.

Zur Person

Brigitte Christ ist stellvertretende Direktorin der Eidgenössischen Finanzkontrolle (www.efk.admin.ch) und Mitglied des Netzwerkes Risikomanagement

> *www.netzwerk-risikomanagement.ch*

Brigitte Christ

Auch Angreifer – böswillige Personen, cyberkriminelle Organisationen oder Staaten – nutzen die neuen Möglichkeiten und sind grundsätzlich einen Schritt voraus. Was sind sinnvolle Ansatzpunkte für Führungskräfte im Kampf gegen Cyberangriffe?

Widerstandsfähig muss die Organisation sein

Massnahmen zur Erkennung und Abwehr von Cyberangriffen, also Cybersicherheit, sind essenziell und unverzichtbar. Starke Authentisierung, Virenscanner, Patches, sichere VPN-Verbindungen etc. bilden eine Verteidigungsmauer, die regelmässig gewartet und verstärkt werden muss. Nur reicht das nicht mehr.

Die Angreifer finden und nutzen immer komplexere Angriffswege und -muster. Die Schwachstellen nehmen zu, und die Frage lautet nicht mehr, ob ein Unternehmen erfolgreich attackiert wird, sondern wann – und ob das Unternehmen in der Lage sein wird, zuverlässig funktionstüchtig zu bleiben. Das bezeichnet man als Cyberresilienz. Dazu braucht es ein fundiertes Verständnis von Abläufen, Systemen und Daten im Unternehmen und schnelles Handeln bei Angriffen.

Das Ziel ist klar, der Weg ist steinig: In seiner Cyberresilienz-Studie 2020 kommt das Beratungsunternehmen AWK[1] zum Ergebnis, dass lediglich 20 Prozent der Befragten ihr Unternehmen als ausreichend resilient beurteilen. Es gibt also zu tun.

Cyberrisiken sind Chefsache

Geschäftsführung und Verwaltungsrat müssen Cyberbedrohungen als unternehmensweites Risikomanagementthema verstehen und adressieren – es ist kein IT-Problem. Die Leitungsebene muss die Bedrohung verstehen, sie trägt das Risiko, nicht der CISO, nicht der Sicherheitsbeauftragte, nicht die Informatikabteilung, nicht der IT-Architekt … Bei der Führung laufen die Fäden zusammen, sie ist verantwortlich für ein Gesamtbild aus Unternehmenssicht, und dazu

Resilient ist nur, wer darauf trainiert ist.

Bild: Depositphotos_Krakenimages

braucht es den engen Austausch mit den Experten. Die Führung legt fest, wie viel Risiko das Unternehmen tragen kann und will. Sie ist im Schadensfall rechenschaftspflichtig. Es ist mehr als eine Good Practice, es ist gesetzliche Pflicht und damit eine Verantwortlichkeitsfrage für Verwaltungsrat und Geschäftsleitung. Dank der digitalen Transformation ganzer Wertschöpfungsketten beginnen und enden Cyberrisiken übrigens nicht an den Unternehmensgrenzen: Lieferanten und Kunden müssen bei der Risikobetrachtung und Massnahmendefinition berücksichtigt werden. Cyberrisiken sind also keine IT-, sondern integrale Geschäftsrisiken, die bis zur Existenzbedrohung gehen können. Sie gehören auf die Chefetage.

Mitarbeitende als starke Abwehrwaffe

Gerade die so menschlichen Eigenschaften wie Hilfsbereitschaft, Angst, Respekt vor Autorität oder Vertrauen machen den Menschen zu einem besonders beliebten und erfolgreichen Angriffspunkt. Im Gegensatz zur IT kann man nach einem Vorfall bei Menschen nicht einfach einen Patch einspielen und somit eine Sicherheitslücke systematisch schliessen. Das Verhalten eines Menschen ist individuell und oft unvorhersehbar, das macht ihn zum schwächsten Glied in der Kette. Die Wirksamkeit der Massnahmen gegen die Cyberrisiken steht und fällt mit den beteiligten Menschen. Nur wenn das Bewusstsein für Sicherheitsbedürfnisse und Bedrohungen in den Köpfen verankert ist, können Risiken bewusst und qualifiziert in Kauf genommen werden. Investitionen in Schulungen, Sensibilisierung, Stärkung der Eigenverantwortung und Fähigkeiten bringen also eine hohe «Rendite».

Investitionen in die Digitalisierung auch bei der Überwachung

Sicherheit und Resilienz kosten. Ressourcen sind knapp. Also geht es um gezielte, risikobasierte Investitionen mit hohem Nutzen. Auch im Kampf gegen Cyberbedrohungen gilt: automatisieren, wo immer möglich. Logfiles von Hand auszuwerten oder Datenströme manuell auf Auffälligkeiten zu scannen mutet fast nostalgisch an – mit hohem Aufwand und geringem Nutzen. Unternehmen nutzen den technologischen Fortschritt für ihr Business, warum nicht auch bei der Absicherung? Die Angreifer rüsten auf, setzen lernende Systeme, künstliche Intelligenz ein, beispielsweise um Angriffe zu automatisieren und zu personalisieren. Tun Sie es auch!

Cyberresilienz

Cyberkriminelle finden und nutzen immer komplexere Angriffswege und -muster. Cyberresilient sind nur Unternehmen, die trotz erfolgreichem Angriff in der Lage sein werden, als Organisation funktionstüchtig zu bleiben.

Laut einer repräsentativen Ipsos-Umfrage im Auftrag des deutschen TÜV-Verbands[2] nutzt bereits jedes achte Unternehmen künstliche Intelligenz für seinen eigenen Schutz. Unter den grossen Unternehmen ab 250 Mitarbeitern sind es sogar 38 Prozent.

Vorbereitet sein

Wenn ein Angriff Erfolg hat, ist keine Zeit zum Probieren. Jeder muss seinen Platz kennen und wissen, was zu tun ist. In vielen Schubladen sind Pläne, wie der Betrieb wiederhergestellt werden kann. Geübt wird die Wiederherstellung hingegen nur selten. Das Business Continuity Management steht somit auf wackeligen Beinen, was wiederum ein kritisches Risiko an sich darstellt. Zu einer guten Vorbereitung gehören auch Grundsatzfragen: Wie reagiert man auf Erpressung? Bleibt man hart und zeigt den Vorfall an oder zahlt man lieber, weil das wirtschaftlich gesehen vorteilhafter sein kann? Auch der Risikotransfer an Versicherer kann eine Option darstellen: Laut dem Versicherungsbroker Kessler[3] wird immerhin jede vierte Police auch in Anspruch genommen. Ausserdem ist ein Trend zu kleineren Tranchen pro Schadensfall zu beobachten: mehrere «kleinere» Schäden statt wenigen sehr grossen Vorfällen.

Ohne schlagkräftiges Risikomanagement ist keine erfolgreiche digitale Transformation möglich.

Ohne ein schlagkräftiges Risikomanagement ist keine erfolgreiche digitale Transformation möglich. Starke Abwehr- und Widerstandsfähigkeit gegen Cyberattacken sind kein notwendiges Übel, sondern ein Wettbewerbs- und Differenzierungsmerkmal. Unternehmerinnen und Unternehmer müssen diese Chance nutzen! ■

Dieser Fachartikel erscheint in einer Beitragsserie, die von Expertinnen und Experten des Netzwerkes Risikomanagement beigesteuert wird.

Hinweise:

1 AWK-Cyber-Resilienz-Studie-20201.pdf
2 Cyberrisiken: AI als Lösung und Problem – RiskNET – The Risk Management Network
3 PowerPoint-Präsentation (netzwerk-risikomanagement.ch)