DXC.technology

So wird Cybersicherheit bei Vorständen und CFOs zur obersten Priorität

Von Mark Hughes, DXC Technology

> Um wirklich effektiv zu sein, müssen Vorstände und CFOs sich der Risiken voll bewusst sein und Cybersicherheit als grundlegend für fast alles betrachten, was das Unternehmen macht – beginnend an der Spitze.

Als Führungskraft, die für die Bereitstellung von Sicherheitslösungen für unsere globalen Kunden verantwortlich ist, sehe ich, dass das Thema Cybersicherheit auf der Agenda von Vorständen weiter nach oben rückt. Während die meisten Budgets aktuell schrumpfen, werden die weltweiten Ausgaben für Sicherheit **nach Prognosen von IDC** jährlich um 8,1 % steigen und bis 2024 174,7 Milliarden US-Dollar erreichen.

Und dafür gibt es einen guten Grund. Umfassende Datenschutzverstöße und lähmende Ransomware-Angriffe können in ihrer Wirkung Naturkatastrophen ähneln – oft bringen sie das Geschäft zum Erliegen und schädigen Marke, Kundenbindung, Partnerbeziehungen und mehr. Es mag erstaunlich sein, doch die prognostizierten Kosten der Cyberkriminalität – geschätzte 6 Billionen US-Dollar im Jahr 2021 – stellen laut Cybersecurity Ventures „den größten Transfer von wirtschaftlichem Wohlstand in der Geschichte“ dar.

Wenn Vorstände und CFOs 2020 etwas gelernt haben, dann, mit dem Unerwarteten zu rechnen. Aber um wirklich effektiv zu sein, müssen sie sich der Risiken voll bewusst sein und Cybersicherheit als grundlegend für fast alles betrachten, was das Unternehmen macht – beginnend an der Spitze.

Kein reines IT-Problem

Es gilt zu beachten, dass es bei Sicherheit nicht mehr nur um das Patchen und den Schutz von IT-Systemen geht. Wie wir wissen, ist das Thema vielmehr im gesamten betrieblichen Umfeld relevant.

Als im letzten Juni Ransomware die internen Netzwerke eines globalen Fertigungsunternehmens lahmlegte, war das Unternehmen gezwungen, die Produktionsanlagen, den Kundendienst und den Finanzbereich vorübergehend stillzulegen.

Ich sehe noch einen weiteren Trend, und das ist die zunehmende Bandbreite an Risiken, denen große Unternehmen ausgesetzt sind. Die Bedrohungslandschaft wird von einer Vielzahl soziotechnischer Faktoren wie dem regulatorischen Umfeld, sozialen und politischen Veränderungen und der Kultur beeinflusst.

Das Management von Sicherheitsprogrammen und die Abwehr von Angreifern wird immer ein Abwägen zwischen Kosten und Risiken erfordern, aber angesichts dessen, was auf dem Spiel steht, müssen Sicherheitsentscheidungen auf informierte, strategische und gemeinschaftliche Weise getroffen werden.

Die unzureichende Kommunikation von Richtlinien durch das Management kann zu Gefahren durch Insider und zur Weitergabe sensibler Daten führen. Die Einführung einer neuen Vorstandsdirektive, M&A-Aktivitäten oder die Zusammenarbeit mit einem Zulieferer können unbeabsichtigt dazu beitragen, dass eine Hacktivistengruppe die Unternehmenswebsite verunstaltet, Social-Media-Konten kapert oder Dienste durch einen verteilten Denial-of-Service-Angriff lahmlegt. Zu lasche Datenschutzprogramme können in einigen Regionen zu hohen Strafen führen, während sie in anderen wiederum nur angemahnt werden.

Während die meisten Vorstände um die Auswirkungen der Sicherheit auf die Marke und das Kundenvertrauen wissen – und CFOs mit den Kosten nur allzu vertraut sind –, stehen Chief Information Security Officers (CISOs) immer noch vor der schwierigen Aufgabe, ein sich ständig veränderndes Risikoszenario kommunizieren zu müssen.

Sicherheit als oberste Priorität

Unser Team konzentriert sich darauf, diesen Führungskräften zu helfen, Risiken in ihrem Sinne zu verstehen. Es gibt einige Best Practices, die Ihrem Unternehmen dabei helfen können, Sicherheit zur obersten Priorität zu machen.

Sprechen Sie über Risiken und ROI, nicht über Bedrohungen und Sicherheitslücken. Sicherheitsüberwachungs-Tools und Bedrohungsdaten vermitteln bereits einen guten Eindruck, wie stark die Anzahl der Cyberangriffe zugenommen hat, können aber keine Antwort geben auf die grundlegende Frage „Wie sicher sind wir?“.

Der Vorstand braucht Daten, um Kosten, Zuverlässigkeit und Risiken zu verstehen, doch darüber hinaus müssen CISOs auch eine ganzheitliche Sicht der Gefährdungslage bieten.

Cyber Awareness fängt ganz oben an. Mit der Zunahme immer raffinierterer Spearphishing-Angriffe ist das Führungsteam verletzbarer denn je. CFOs denken in Kategorien, in denen sie die Kosten für die Risikominderung und die potenzielle Gefährdung abwägen, deshalb müssen CISOs die Investitionsrendite klar kommunizieren: Was sind die möglichen Auswirkungen auf Aktienkurs und Shareholder Value? Wie hoch sind die potenziellen Kosten einer Sicherheitslücke im Vergleich zu den Kosten für ihre Behebung?

Der Versuch, sich gegen alle möglichen Bedrohungen abzusichern, könnte sich als zu kostspielig erweisen und sogar die Innovation und das Wachstum des Unternehmens beeinträchtigen. Entscheidungen müssen in Zusammenarbeit getroffen werden, um das richtige Gleichgewicht zwischen Risikoprioritäten und effektiven Sicherheitskontrollen zu finden.

Suchen Sie sich jemanden, der sich mit Sicherheit auskennt. In den letzten Jahren haben sich Führungskräfte verstärkt darum bemüht, ihre Vorstände zu diversifizieren. Neben unterschiedlichen Hintergründen und Perspektiven können Vorstände auch von wichtigen Kompetenzen in den Bereichen Investitionsmanagement, Informationstechnologie, Personalwesen oder Risikomanagement profitieren.

Eine weitere Möglichkeit besteht darin, einen Experten für Cyberrisiken in den Vorstand zu berufen, insbesondere in Branchen, die stark von Cyberrisiken betroffen sind, wie Banken, Einzelhandel, Gesundheitswesen und Versorgungsunternehmen. Mit einem Sicherheitsexperten im Vorstand bleibt das Thema Sicherheit im Vordergrund. Ein Vorstandsmitglied mit Erfahrung in Sachen Sicherheit oder im Umgang mit größeren Sicherheitsverstößen kann weniger technisch versierten Vorstandsmitgliedern helfen, die sich schnell ändernden Risiken zu verstehen.

Setzen Sie nicht allein auf Cyber-Versicherungen. Cyber-Versicherungen sind ein relativ neues Instrument zur Risikominderung, das in der Regel Verpflichtungen im Zusammenhang mit Datenschutzverstößen abdeckt. Dazu gehören Schadenersatz, Anwaltskosten,

Benachrichtigungen an Kunden, die Wiederherstellung von Daten und die Reparatur von Computersystemen. Allerdings decken diese Policen nicht unbedingt den Wertverlust durch den Diebstahl von geistigem Eigentum oder die Kosten für die Aufrüstung von Software und Geräten zur Verhinderung von Angriffen ab.

CFOs und Chief Risk Officers sollten die Vorteile einer Cyber-Versicherung im Vergleich zu Selbstversicherungsoptionen sorgfältig abwägen. Im Jahr 2018 gab die Stadt Atlanta **2,7 Millionen US-Dollar aus, um sich von einem Cyberangriff zu erholen**, anstatt die Lösegeldforderung von 50.000 US-Dollar zu bezahlen. Das meiste Geld floss in die Aufrüstung veralteter Systeme. Eine Cyber-Versicherung macht dem CFO die Entscheidung leichter, auf die Zahlung des Lösegelds zu verzichten, aber sie kann den Schaden für die Reputation nicht mindern. Vorbeugung, eine schnelle Reaktion und Ausfallsicherheit sind immer noch die besten Verteidigungsmaßnahmen.

Nutzen Sie agile Managementprozesse. Es tauchen ständig neue Schwachstellen auf, Angreifer ändern kontinuierlich ihre Taktik, und Sicherheitsprogramme brauchen als Antwort darauf agile Managementprozesse.

Unternehmen müssen Sicherheit nach Best Practices und mit Ausfallsicherheitsplänen verwalten, genauso wie Kernsysteme Disaster Recovery-Pläne und Backups benötigen. Unternehmen arbeiten auf eine kontinuierliche Verbesserung der Betriebsabläufe, des Kundendienstes und anderer Schlüsseldisziplinen hin, und dies sollten Vorstand und CFO auch für die Sicherheit erwarten.

Das Management von Sicherheitsprogrammen und die Abwehr von Angreifern wird immer ein Abwägen zwischen Kosten und Risiken erfordern, aber angesichts dessen, was auf dem Spiel steht, müssen Sicherheitsentscheidungen auf informierte, strategische und gemeinschaftliche Weise getroffen werden. Vorstände und CFOs sind ein wesentlicher Bestandteil dieser Diskussion.

Informieren Sie sich über die neuesten Unternehmensrisiken. Abonnieren Sie den **DXC Bericht zu Sicherheitsbedrohungen**.

Über den Autor

Mark Hughes ist Senior Vice President, Offerings and Strategic Partners bei DXC Technology. Er ist weltweit für die Organisation und Angebote im Bereich Sicherheit verantwortlich. Dazu gehören die Abwehr von Cyber-Angriffen, geschützte Infrastrukturen, die digitale Identität und der Datenschutz. Zuvor war er in leitender Position bei BT Security tätig.