P R E S S E M I T T E I L U N G

Verkannter Wettbewerbsvorteil: 61 Prozent der Geschäftsführer unterschätzen die Bedeutung von Cybersecurity für den Unternehmenserfolg

Delinea-Studie zeigt: Fast ein Drittel der Sicherheitsentscheider stuft die eigene Kommunikation mit der Geschäftsführung als verbesserungswürdig ein

München, 11. Mai 2023 – **Die Mehrheit der Geschäftsführer und Vorstände verkennt nach wie vor, welche entscheidende Rolle eine funktionierende Cybersicherheit für den Geschäftserfolg ihres Unternehmens spielt. Dies führt dazu, dass Geschäfts- und Sicherheitsziele oft nicht aufeinander abgestimmt sind, wie eine aktuelle Umfrage* von Delinea, dem Spezialisten für Lösungen, die Privileged-Access-Management nahtlos erweitern, nun zeigt. Nur 39 Prozent der befragten IT-Sicherheitsentscheider sind demnach der Meinung, dass die Führungsetage ihres Unternehmens die Bedeutung von Cybersecurity als Business Enabler tatsächlich richtig einschätzt.**

Vielmehr wird das Thema Sicherheit oft nur im Hinblick auf die Compliance und die Einhaltung gesetzlicher Bestimmungen als wichtig erachtet, wie 35 Prozent angegeben haben. Laut 17 Prozent der Befragten wird der Cybersecurity von der Unternehmensleitung sogar keinerlei geschäftliche Priorität zugeschrieben. Dabei hat die globale wirtschaftliche Unsicherheit die Situation noch verschlimmert und macht es für rund die Hälfte der Befragten (48 %) noch schwieriger, die Cybersicherheit mit den allgemeinen Unternehmenszielen in Einklang zu bringen.

Mangelnde Ausrichtung schwächt die Sicherheitslage

Die fehlende Einschätzung des Sicherheitsaspekts von Seiten der Geschäftsführung hat für die Unternehmen weitreichende Auswirkungen, auch auf Investitionen und Budgetverteilungen. So berichten 35 Prozent der Befragten von Verzögerungen bei wichtigen Sicherheitsinvestitionen, fast ebenso viele (34 %) von aufgeschobenen strategischen Entscheidungen.

Dies blieb auch für die Sicherheitslage der Unternehmen nicht ohne Folgen: Die überwiegende Mehrheit der Befragten (89 %) konnte aufgrund der Diskrepanz zwischen Geschäfts- und Sicherheitszielen im vergangenen Jahr mindestens eine negative Auswirkung für ihr Unternehmen erkennen. Mehr als ein Viertel gab etwa an, dass dies zu einem Anstieg erfolgreicher Cyberangriffe geführt hatte, und zudem den Stress erhöht hat, dem die Security-Teams ausgesetzt sind, wie 31 Prozent der Befragten bestätigten.

Security-Teams haben Schwierigkeiten, ihre Erfolge sichtbar zu machen

Doch die Umfrage bringt auch positive Aspekte in der Zusammenarbeit von Security-Teams und Geschäftsleitung zutage: So gaben 62 Prozent der Befragten an, sich regelmäßig mit

Führungskräften zu treffen und auszutauschen und in 54 Prozent der Unternehmen sind Security-Verantwortliche sogar Teil der Führungsetage.

Indes besteht Verbesserungspotenzial beim Abstimmen der Sicherheitsstrategien sowie dem Sichtbarmachen von Erfolgen. So dokumentiert nur etwa die Hälfte der Unternehmen (48 %) Richtlinien und Verfahren, um Abstimmungen und Anpassungen von Maßnahmen zu erleichtern, und ein weiteres Drittel (33 %) gab an, dass Abstimmungen grundsätzlich nur ad hoc oder bei Bedarf erfolgen. Zudem macht die Studie deutlich, dass die Metriken, mit denen der Erfolg von Cybersicherheitsmaßnahmen sichtbar gemacht und bewertet wird, immer noch streng an technische oder tätigkeitsbasierte Kennzahlen geknüpft sind. Laut 31 Prozent der Befragten ist die Zahl der abgewehrten Angriffe das wichtigste Maß für den Erfolg, gefolgt von der Erfüllung der Compliance-Ziele (29 %) und der Reduzierung der Kosten für Sicherheitsvorfälle (29 %).

„Cybersicherheit kann ein wichtiger Business Enabler sein, doch in den Köpfen von Geschäftsführung und Vorstand ist dies noch nicht ganz angekommen, wie unsere neue Studie zeigt“, so Joseph Carson, Chief Security Scientist und Advisory CISO bei Delinea. „Führungskräfte dürfen Cybersicherheit nicht nur unter dem Gesichtspunkt von Compliance oder der reinen Unternehmenssicherheit sehen, sondern müssen endlich auch ihre strategische Bedeutung für den Geschäftserfolg erkennen.“

Security-Verantwortlichen mangelt es oft an klassischen Business-Kompetenzen

Technische Skills und Fachwissen im Bereich der Cybersecurity werden von den Befragten als die wertvollsten Fähigkeiten angesehen, über die Sicherheitsentscheider verfügen sollten und werden daher deutlich höher bewertet als Kommunikationsgeschick, Geschäftssinn oder Mitarbeiterführung. Dabei sind es diese klassischen Business-Kompetenzen, die Sicherheitsverantwortlichen dabei helfen, sich besser mit der Geschäftsführung abzustimmen. Tatsächlich gibt fast ein Drittel der Befragten zu, dass das erfolgreiche Vermitteln von Geschäftsszenarien an den Vorstand und die Geschäftsleitung eine Lücke in den eigenen Fähigkeiten darstellt, und fast ebenso viele (30 %) stufen ihre Kommunikationsfähigkeiten als verbesserungswürdig ein.

Soll die Diskrepanz zwischen Business- und Sicherheitszielen überwunden werden, braucht es optimierte Berichtslinien sowie mehr Sichtbarkeit der Cybersicherheit auf Vorstandsebene: Die Umfrage deutet jedoch darauf hin, dass die Bereitschaft, aktuelle Berichtsstrukturen zu ändern, nur sehr gering ist. So sind nur 27 Prozent der befragten Sicherheitsentscheider der Meinung, dass die CISOs bzw. die ranghöchsten Cybersecurity-Führungskräfte dem CEO Bericht erstatten sollten, um die Cybersecurity optimal auf die Gesamtziele des Unternehmens abzustimmen.

„Die Abstimmung der Cybersicherheit mit den Geschäftszielen ist für den Erfolg eines Unternehmens entscheidend“, ergänzt Joseph Carson. „Welche negativen Folgen es haben kann, wenn das Sicherheitsteam und die Geschäftsführung nebeneinander agieren anstatt miteinander und Metriken nur die Sicherheitsaktivitäten nicht aber deren Auswirkungen auf das Business messen, hat diese Studie deutlich gezeigt. Der Schlüssel liegt dabei in einer besseren Kommunikation der Security-Teams – ungeachtet dessen, dass starke technische Fähigkeiten für den Erfolg ihrer Arbeit nach wie vor sehr wichtig sind. Sicherheitsverantwortliche müssen mehr denn je in der Lage sein, zu kommunizieren, Einfluss zu nehmen und den Wert, den ihre Arbeit für den allgemeinen Geschäftserfolg hat, sichtbar zu machen. Security-Teams, die diese Mischung von Fähigkeiten aufweisen und dabei die gleichen Ziele wie die Unternehmensführung verfolgen, können wirklich etwas bewegen.“

Die vollständigen Report-Ergebnisse stehen ab sofort kostenlos zum Download bereit: https://delinea.com/resources/aligning-cybersecurity-and-business-outcomes

***Methodik**:
Im Auftrag von Delinea befragte das unabhängigen Marktforschungsunternehmen Sapio Research im März 2023 insgesamt 2.007 IT-Sicherheitsentscheider aus 23 Ländern, darunter 100 aus Deutschland. Die Stichprobe ist branchenübergreifend und die Interviews wurden online in einem strengen mehrstufigen Screening-Verfahren durchgeführt.

Über Delinea
Delinea ist ein führender Anbieter von Privileged-Access-Management (PAM)-Lösungen für moderne, hybride Unternehmen. Die Delinea Platform erweitert PAM nahtlos, indem sie eine identitätsübergreifende Autorisierung bereitstellt und den Zugriff auf die kritischsten Hybrid-Cloud-Infrastrukturen sowie die sensibelsten Daten eines Unternehmens kontrolliert. Auf diese Weise werden Risiken reduziert, Compliance gewährleistet und die Sicherheit vereinfacht. Die Kundenbasis von Delinea umfasst Tausende Unternehmen weltweit und reicht von KMUs bis hin zu den weltweit größten Finanzinstituten und Unternehmen der kritischen Infrastruktur.
Weitere Infos unter: http://delinea.com/de

Erfahren Sie mehr über Delinea auf LinkedIn, Twitter und YouTube.

Pressekontakte:

Delinea DACH
Claudia Specht, Senior Marketing Manager DACH
claudia.specht@delinea.com

PR-Agentur: Weissenbach PR
Dorothea Keck
T: +49 89 54 55 82 02
delinea@weissenbach-pr.de
Web: www.weissenbach-pr.de