Studie: Wenig Vertrauen in Fähigkeiten beim Datenschutz

So schnell wie sich die Digitalisierung weiterentwickelt, so dringend muss der Datenschutz zu einem entscheidenden Geschäftsprinzip werden. Jedoch haben laut der ISACA-Studie „State of Privacy 2025" nur 38 Prozent der europäischen Fachleute Vertrauen in die Fähigkeit ihres Unternehmens, sensible Daten zu schützen. Dabei ist der Austausch personenbezogener Daten ein wichtiger Bestandteil moderner Geschäftsabläufe, so dass schwache Schutzmechanismen die Glaubwürdigkeit von Unternehmen untergraben und Misstrauen in Kundenbeziehungen schaffen. Die Auswirkungen spiegeln sich in den Umsätzen.

© IMAGO / Panthermedia

Datendiebstahl: Sensible Daten zu schützen, ist für viele Unternehmen keine leichte Aufgabe.

© privat

Chris Dimitriadis ist Chief Global Strategy Officer, ISACA.

Es gibt mehrere Gründe für die Vertrauenskrise unter den Datenschutzbeauftragten: 45 Prozent halten das Datenschutzbudget ihres Unternehmens für unterfinanziert und mehr als die Hälfte (54 Prozent) der Befragten rechnet mit weiteren Budgetkürzungen innerhalb des nächsten Jahres. Die Unterfinanzierung zeigt sich in Personalmangel: 52 Prozent der technischen Datenschutzteams geben an, unterbesetzt zu sein, und mehr als ein Drittel (37 Prozent) hat Schwierigkeiten, qualifizierte Datenschutzbeauftragte zu finden. Verschärft wird die Situation durch die Komplexität und Entwicklung der aktuellen Bedrohungslandschaft. Kein Wunder, dass zwei Drittel (66 Prozent) der befragten Fachleute angeben, ihre Arbeit sei heute stressiger als noch vor fünf Jahren.

Wichtige Meilensteine der regulatorischen Landschaft wie die EU-Gesetzgebung zur künstlichen Intelligenz, der Corporate Governance Kodex und die Datenschutz-Grundverordnung wirken sich positiv auf den Datenschutz in Europa aus. Diese Verordnungen bieten Organisationen Orientierung, um ihren Umgang mit dem Datenschutz zu optimieren.

Um jedoch Compliance zu erreichen und strenge Datenschutzstandards aufrechtzuerhalten, müssen Unternehmen die strukturellen Herausforderungen angehen – angefangen bei verstärkten Investitionen in Datenschutzmitarbeitende, die Zugang zu umfassenden Schulungen und Ressourcen erhalten. Organisationen, die Privacy by Design immer praktizieren, erreichen bei der Schließung der Qualifikationslücke im Bereich des Datenschutzes bereits entscheidende Fortschritte – 56 Prozent bieten Schulungen für Mitarbeitende an, die nicht im Bereich des Datenschutzes tätig sind und in diesen Bereich wechseln wollen, verglichen mit 44 Prozent in Unternehmen, die Privacy by Design nicht praktizieren.

KI hat die Arbeitswelt in vielen Branchen verändert. Laut der ISACA-Studie „State of Privacy 2025" setzen 37 Prozent der Unternehmen bereits KI für datenschutzrelevante Aufgaben wie Datenklassifizierung, Risikoanalyse und Compliance-Überwachung ein oder planen deren Einsatz. Die Technologie kann Prozesse beschleunigen, Routineaufgaben automatisieren und menschliche Fehler reduzieren.

Doch da KI-Technologien am Arbeitsplatz immer zugänglicher werden, stehen sie auch Cyberkriminellen offen. Allerdings sind nur 35 Prozent der Cybersicherheitsteams in Unternehmen an der Entwicklung von KI-Richtlinien beteiligt und 45 Prozent überhaupt nicht in die KI-Governance eingebunden. Aus Sicht des Datenschutzes ist es entscheidend, dass Unternehmen geschult werden, um mit den Angreifern Schritt zu halten, deren Angriffe zu erkennen und abzuwehren und zu verhindern, dass wichtige Daten in Gefahr geraten.

Es gibt drei grundlegende Schritte, die Unternehmen umsetzen sollten, um ihre Datenschutzteams zu unterstützen und sicherzustellen, dass sie effektiv arbeiten können.

Erstens: die Schließung der Qualifikationslücke. Fast die Hälfte (47 Prozent) der europäischen Organisationen bildet bereits Mitarbeitende, die nicht im Bereich des Datenschutzes tätig sind, zu Datenschutzbeauftragten aus. Bemerkenswert ist, dass 89 Prozent der Befragten Zertifizierungen gegenüber Hochschulabschlüssen (54 Prozent) den Vorzug geben.

Zweitens: die Nutzung neuer Technologien wie künstlicher Intelligenz. Investitionen in die Schulung von Datenschutzexperten können dazu beitragen, wertvolle Ressourcen freizusetzen und eine sichere Nutzung zu gewährleisten.

Drittens: die Priorisierung des Datenschutzes. Angesichts neuer und anhaltender Bedrohungen müssen Geschäftsleitungen in Datenschutzteams investieren und den Datenschutz in ihre übergreifenden Unternehmensstrategien integrieren, um kostspielige, reputationsschädigende Auswirkungen in der Zukunft zu vermeiden.

Datenschutz ist eine geschäftliche Notwendigkeit. Unternehmen, die nicht in den Datenschutz investieren, riskieren Rufschädigung, behördliche Sanktionen und den Verlust des Kundenvertrauens. Führungskräfte müssen jetzt handeln und in Mitarbeitende, Prozesse und Technologien investieren, um eine robuste und zukunftsorientierte Datenschutzstrategie aufzubauen.

Chris Dimitriadis

Die Studie „State of Privacy 2025" untersucht unter anderem die Priorisierung des Datenschutzes durch Vorstände, die Einhaltung von Datenschutzvorgaben, den Einsatz von Künstlicher Intelligenz im Datenschutz, Schulungen zum Datenschutzbewusstsein, Datenschutzverletzungen und die Rolle von „Privacy by Design". Die Ergebnisse basieren auf der fünften jährlichen globalen Datenschutz-Umfrage von ISACA, die im September 2024 durchgeführt wurde. Mehr als 1.600 Personen aus dem Berufsfeld „Datenschutz" nahmen an der Umfrage teil. 38 Prozent waren in Managementpositionen tätig, 29 Prozent gehörten zur oberen Führungsebene, 20 Prozent waren Einzelmitarbeitende und 12 Prozent Teil der Geschäftsleitung.