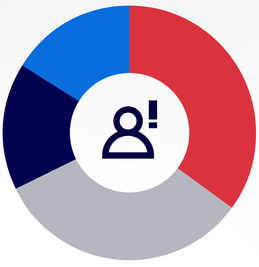
INSIDER-BEDROHUNGEN VERSTEHEN UND DATENVERLUST VERHINDERN

UMFRAGE 1: RISIKEN DURCH INSIDER-BEDROHUNGEN

WELCHE ART VON INSIDER-BEDROHUNGEN BEREITET IHNEN DIE GRÖSSTEN SORGEN?

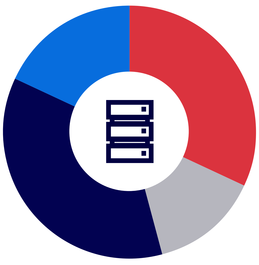


Wichtige Erkenntnis

Insider-Bedrohungen werden vor allem durch Technologien und menschliche Faktoren getrieben. GenAI-Tools (35%) und ausscheidende Mitarbeitende (33%) zeigen die größten Risiken, während Quellcode-Leaks und nicht genehmigte Anwendungen (je 16%) weitere Herausforderungen darstellen. Zusammen verdeutlichen diese Zahlen den Handlungsbedarf bei Technologieeinsatz und Mitarbeitermanagement.

UMFRAGE 2: AKTUELLE DLP-ANSÄTZE

WIE GEHT IHRE ORGANISATION DERZEIT MIT DATENVERLUST-PRÄVENTION (DLP) UM?

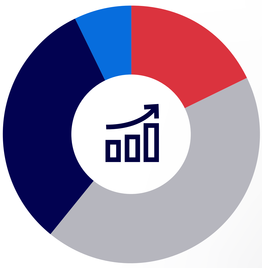


Wichtige Erkenntnis

36% der Organisationen setzen moderne Verhaltensanalysen ein, um Datenverluste proaktiv zu verhindern, während 32% noch stark auf manuelle Prozesse und Schulungen setzen. Diese Ansätze sensibilisieren Mitarbeitende und setzen Richtlinien über Awareness-Programme und manuelle Checks um, sind jedoch anfällig für Fehler und Inkonsistenzen. 18% der Organisationen verfügen über keine aktive DLP-Strategie und laufen damit Gefahr, Datenverluste zu erleiden.

UMFRAGE 3: VERBESSERUNGEN BEI DLP-PROGRAMMEN

WENN SIE EINEN ASPEKT IHRES DLP-PROGRAMMS VERBESSERN KÖNNTEN, WELCHER WÄRE DAS?



Wichtige Erkenntnis

Automatisierungs- und Erkennungstools stehen an oberster Stelle der Verbesserungsprioritäten: 43% der Befragten wünschen sich schnellere und intelligentere Reaktionen auf Datenverlustvorfälle. 32% setzen auf Mitarbeiterschulungen und Sensibilisierung, um das menschliche Verhalten zu stärken. 18% streben bessere Echtzeit-Übersicht über Datenflüsse an, um Anomalien frühzeitig zu erkennen, während nur 7% verknüpfte Sicherheitssysteme priorisieren.

FAZIT

Die Ergebnisse unterstreichen die zunehmende Bedeutung moderner Tools und Strategien, um Insider-Bedrohungen zu begegnen und DLP-Programme zu verbessern. Organisationen setzen verstärkt auf Automatisierung, Verhaltensanalysen und Mitarbeiterschulungen, um Risiken proaktiv zu begegnen.

JETZT HANDELN

Die Daten sind eindeutig: Insider-Bedrohungen entwickeln sich weiter – halten Ihre Abwehrmaßnahmen Schritt?

Incydr von Mimecast bietet Echtzeit-Übersicht, Verhaltensanalysen und schnelle Erkennung, um Ihre DLP-Lücken zu schließen.

MEHR ERFAHREN

Quelle: LinkedIn-Umfragen, durchgeführt zwischen Mai und Juli unter mehr als 100 Teilnehmern aus Europa und Südafrika.
Diese Daten dienen nur zu Informationszwecken und stellen keine professionelle Beratung oder rechtsverbindliche Aussage dar.