PRESSEINFORMATION

96 Prozent der deutschen Unternehmen sind von Spionage, Diebstahl oder Sabotage betroffen oder vermuten einen Angriff. Wie Unternehmen Informationssicherheit systematisch stärken können

Von der Risikoanalyse bis zur Notfallvorsorge: Warum strukturierte Managementprozesse entscheidend sind.

Wien, Oktober 2026 – Die Bedrohungslage für Unternehmen in Deutschland bleibt angespannt. Laut der Bitkom-Studie „Wirtschaftsschutz 2026" waren 67 Prozent der befragten Unternehmen in Deutschland innerhalb der vergangenen zwölf Monate von Diebstahl, Industriespionage oder Sabotage betroffen. Weitere 29 Prozent gehen davon aus, ebenfalls betroffen gewesen zu sein. Die Schäden bleiben im dreistelligen Milliardenbereich, für 2026 ergibt sich ein Schadenskorridor von 211 bis 270,8 Milliarden Euro. (Quelle: Bitkom, Wirtschaftsschutz 2026)

Zahlen verdeutlichen, wie wichtig es ist, Informationssicherheit nicht ausschließlich als technische Aufgabe zu betrachten, sondern als festen Bestandteil des unternehmerischen Risikomanagements.

Informationssicherheit ist eine Managementaufgabe

Ein wirksames Sicherheitskonzept beginnt damit, schützenswerte Informationen, Systeme und Geschäftsprozesse zu identifizieren. Unternehmen sollten Risiken bewerten, Verantwortlichkeiten festlegen und die Wirksamkeit ihrer Maßnahmen regelmäßig überprüfen. Auch die Notfallvorsorge spielt eine wichtige Rolle. Notfallpläne müssen bekannt sein und in der Praxis getestet werden.

Ein Informationssicherheitsmanagementsystem (ISMS) schafft dafür einen strukturierten Rahmen. Ein Datenschutzmanagementsystem (DSMS) unterstützt die Organisation datenschutzbezogener Pflichten und Prozesse. Business Continuity Management (BCM) ergänzt diese Ansätze um die Vorbereitung auf Störungen und die Aufrechterhaltung kritischer Geschäftsprozesse.

„Informationssicherheit darf nicht bei der Erfüllung regulatorischer Anforderungen und der Dokumentation von Maßnahmen enden. Entscheidend ist, dass Risiken, Verantwortlichkeiten und Sicherheitsmaßnahmen im Unternehmensalltag zusammenwirken. Ein ISMS muss deshalb gelebt und laufend weiterentwickelt werden", sagt Benigna Prochaska, Geschäftsführerin der Intervalid GmbH.

Softwaregestützte Lösungen können helfen, Anforderungen, Zuständigkeiten, Maßnahmen und Nachweise zentral zu dokumentieren und miteinander zu verknüpfen. Die Intervalid GmbH bietet dafür Intervalid ISMS und Intervalid DSMS sowie ein ergänzendes BCM-Modul an.

Intervalid GmbH
Am Heumarkt 11/1/2 | A-1030 Wien
www.intervalid.com

AT: +43 1 905 10 44 | info@intervalid.at
DE: +49 721 1608 1337 | info@intervalid.de

IBAN: AT61 1200 0100 2028 5218 | BIC: BKAUATWW | UID: ATU72303358 | Firmenbuch 470426d | Rechtsform: Gesellschaft m.b.H, Sitz Wien

Über Intervalid

Die Intervalid GmbH mit Sitz in Wien entwickelt Software für Informationssicherheits- und Datenschutzmanagement (Intervalid ISMS und DSMS) sowie Business Continuity Management (BCM).

2026 führte Intervalid eine neue Oberflächengeneration mit verbesserter Benutzerführung, Navigation und Barrierefreiheit ein. Die Lösungen sind mehrsprachig, mandantenfähig und als SaaS ohne lokale Installation nutzbar. Persönlicher Support und Schulungen ergänzen das Angebot.

Intervalid richtet sich an Unternehmen unterschiedlicher Größen sowie an externe Informationssicherheits- und Datenschutzberater.

Pressekontakt

Intervalid GmbH
Olivia Löwenpapst-Haspel
olivia.loewenpapst-haspel@intervalid.com
www.intervalid.com

Quelle: Bitkom, *Wirtschaftsschutz 2026*. Repräsentative Befragung von 1.003 Unternehmen in Deutschland. https://www.bitkom.org/sites/main/files/2026-09/bitkom-studienbericht-wirtschaftsschutz-2026.pdf