Stoïk-Barometer „Cyberrisiko im Mittelstand“ Bewusstsein hoch, Schutz lückenhaft

Franziska Geier, Geschäftsführerin von Stoïk Deutschland © Stoïk

Der europäische Mittelstand nimmt Cyberrisiken ernst, doch wirkungsvoller Schutz hinkt hinterher. Das zeigt das jährliche Barometer von IFOP für Stoïk, Europas führenden Cyber-Versicherer für KMU.

Die Mehrheit der befragten mittelständischen Unternehmen bereitet sich auf Angriffe vor und erhöht die Budgets. Zugleich bleibt die Absicherung mit spezifischen Cyberpolicen und die operative Begleitung im Ernstfall ausbaufähig, gemäß der Datenerhebung Stoïk von in Partnerschaft mit EY. Damit bleibt die Lücke zwischen wahrgenommener Bedrohung und tatsächlicher Absicherung weiterhin bestehen. Viele Unternehmen sehen die Notwendigkeit eines besseren Schutzes, die erforderlichen Schritte bleiben jedoch aus.

Franziska Geier, Geschäftsführerin Stoïk GmbH: „Der Mittelstand in Deutschland und Österreich ist ein Rückgrat von Wertschöpfung und Beschäftigung. Genau deshalb geraten diese Firmen zunehmend ins Visier von Cyberangreifern. Der Wille zur Absicherung ist da. Was vielerorts fehlt, sind passgenaue Angebote, die Prävention, Deckung und Krisenunterstützung sinnvoll verzahnen.“

Zentrale Ergebnisse des Stoïk-Barometers

-> Bewusstsein & Vorbereitung: 81 % bereiten sich auf einen möglichen Angriff vor; 77 % nehmen ein höheres Risiko für ihr Unternehmen wahr; 73 % erhöhen ihr Cyber-Budget in den nächsten 12 Monaten.
-> Betroffenheit: 32 % der Unternehmen waren bereits Opfer mindestens eines Cyberangriffs – über 20 % davon im vergangenen Jahr. Mit der Größe steigt die Exposition: In der Klasse 2.000–4.999 Beschäftigte berichten 42 % über Vorfälle.
-> Absicherung: Trotz der Wachsamkeit haben nur 51 % eine spezifische Cyberversicherung abgeschlossen – ein deutlicher Gap zwischen wahrgenommener Vorbereitung und tatsächlich implementierten Maßnahmen.
-> Sorgen & Erwartungen: Hauptsorge ist der Betriebsstillstand (36 %), gefolgt von Abfluss sensibler Daten (29 %); zusätzlich belasten Ermittlungskosten, Systemwiederherstellung und Lösegeldzahlungen. Klare Erwartung an Versicherer: 64 % wünschen vollumfängliche Entschädigung, knapp die Hälfte erwartet Präventions-Tools, 43 % den Zugriff auf ein Cyber-Expertenteam im Krisenfall.

Wo der Mittelstand an Grenzen stößt

Mehr Budget führt nicht automatisch zu mehr Resilienz. Zwischen Risikoerkenntnis und wirksamer Umsetzung stehen oft heterogene Tool-Landschaften, Ressourcenkonflikte in der IT-Beschaffung und Policen, die primär kompensieren, aber wenig steuern.

Aus Sicht von Stoïk lässt sich diese Lücke durch einen geschlossenen Risikokreislauf adressieren: Deckung, Prävention und Incident-Response greifen vertraglich definiert ineinander, die Wirksamkeit wird technisch überprüfbar hinterlegt – auf Basis einer europäischen KI-Architektur.

Vor diesem Hintergrund hat Stoïk jüngst sein E-Mail-Security-Modul vorgestellt – für viele KMUs der entscheidende Hebel gegen Business-E-Mail-Kompromittierung und zahlungsbezogenen Betrug. Das Modul ist API-basiert (Microsoft 365/Google Workspace), SOC-gestützt und an klare Sicherheitsstandards gekoppelt; in der Police ermöglicht es verbesserte Entschädigungsgrenzen.