Der Fachkräftemangel im Bereich Cybersicherheit ist vorbei. Die Strategiekrise hat begonnen.

Unter Zeitdruck?

Hier ist die Zusammenfassung unserer aktuellen Studie zur Cybersicherheit. Die vollständige, tiefgehende Analyse zeigt die strategischen Veränderungen auf, die für den Aufbau echter operativer Resilienz erforderlich sind.

1 Die eigentliche Herausforderung ist nicht nur die Personalbeschaffung. Es ist die Strategie.

Unsere Studie, durchgeführt mit über 600 hochrangigen Technologie-Entscheidungsträgern, zeigt eine kritische Diskrepanz auf. Während die Suche nach Talenten weitergeht, liegt die eigentliche Gefahr darin, die Cybersicherheitsstrategie nicht an eine neue, komplexe digitale Landschaft anzupassen.

76% der Unternehmen melden einen Mangel an Cybersicherheitskompetenzen.

46% haben Schwächen auf Führungsebene, bei entscheidenden strategischen Fähigkeiten, einschließlich Governance und Risikobewertung.

85% verzeichnen bereits erhebliche operative Auswirkungen aufgrund dieser Defizite.

2 Die Kosten der Untätigkeit: Geschäftliche Stagnation

Ein strategisches Defizit ist kein Zukunftsproblem; es beeinträchtigt das Unternehmenswachstum schon heute.

der Unternehmen waren gezwungen, wichtige Cybersicherheitsinitiativen zu verschieben oder zurückzustellen.

Dies führt direkt zu Verzögerungen bei der breiteren Unternehmensinnovation, was das Wachstum bremst und die Tür für raffinierte Bedrohungen offen lässt.

3 Die Lösung: Ein strategisches Dreiergespann aus Menschen, Partnern und Plattformen

Führende Unternehmen gehen über interne, isolierte Ansätze hinaus. Sie bauen Resilienz auf, indem sie externes Fachwissen und intelligente Plattformen integrieren.

Die Macht der Partnerschaft 75% der Unternehmen nutzen mittlerweile Managed Security Service Provider (MSSPs), um ihre Teams zu verstärken.

Diejenigen, die mit MSSPs zusammenarbeiten, berichten von greifbaren Vorteilen:

79% haben ihre organisatorische Resilienz gestärkt.

72% haben ihre Compliance-Ergebnisse verbessert.

77% haben klare Sichtbarkeit und Kontrolle über die durchgeführten Arbeiten.

KI als Verbündeter KI ist ein Kraftmultiplikator, aber die Einführung befindet sich noch im Anfangsstadium.

Nur **1 von 5** Unternehmen hat KI vollständig in seine Sicherheitsabläufe integriert. **Das größte Hindernis? Vertrauen.**

52% befürchten ungenaue Ergebnisse von autonomer KI.

Die Nutzung von KI erfordert eine von Menschen geführte Strategie und eine robuste Governance – ein zentraler Schwerpunkt des vollständigen Reports.

4 Ihre Strategie bestimmt Ihre Resilienz.

Der Fachkräftemangel hat die Diskussion in Gang gesetzt, aber die Strategiekrise wird das Ergebnis bestimmen. Ist Ihr Unternehmen bereit?

Bleiben Sie am Laufenden.

Laden Sie den Report herunter, um eine vollständige Analyse der Risiken, Herausforderungen und strategischen Empfehlungen zur Zukunftssicherung Ihres Unternehmens zu erhalten.

Vollständigen Report herunterladen