Cybercrime-Trend Resilience Matrix

Wie gut ist Ihre Organisation gegen die aktuellen Cybercrime-Trends aufgestellt?

Die folgende Cybercrime-Trend Resilience Matrix bietet Ihnen klare **Richtwerte zur Einschätzung der Cyberresilienz Ihrer Organisation** mit Blick auf die aktuellen Angriffstrends. Sie zeigt **wichtige Schritte** auf, die Sie von einem reaktiven Sicherheitsansatz zu maximaler Cyberresilienz bringen.

	Stufe 1 - Elementar	Stufe 2 - Proaktiv	Stufe 3 - Resilient
KI als Angriffsfläche	› Nutzung und Kontrolle von KI-Tools unzureichend reguliert › Mangelnde Sicherheitskontrollen interner KI-Tools › KI-getriebene Angriffsmethoden (Deepfakes, Phishing) nicht überwacht	› KI-Governance-Ausschuss vorhanden; eigene Risiken durch KI sind bekannt oder dokumentiert › Eingeschränkter Zugriff auf KI-Daten; bestimmte Prompt-Prüfungen vorhanden, um schädliche Absichten aufzudecken › KI-getriebene Angriffsmethoden werden sporadisch überwacht	› Sicherheit ist entscheidender Aspekt bei Entwicklung und Wartung von KI-Tools › Strenge Datenzugriffskontrollen; stetige Überwachung KI-getriebener Angriffsmethoden › KI-bezogenes Mitarbeitertraining und Risiko-Assessment
Multi-Channel-Angriffe	› Schutzmaßnahmen auf E-Mail fokussiert › Angriffe per SMS, Anruf oder Social Media nur in Richtlinien und Schulungen ein Thema › Kein Reaktionsplan für Multi-Channel-Angriffe vorhanden	› Teilweise Überwachung von SMS, Kollaborationstools und Social Media › Threat Detection vorhanden, doch die Response variiert je nach Kanal › Nur geringes Training zu Multi-Channel-Phishing	› Eine einheitliche Verteidigungsstrategie für alle Angriffskanäle › Proaktive Überwachung von E-Mail, SMS und sozialen Medien › Regelmäßige personalisierte Multi-Channel-Simulationen für Mitarbeitende
Lieferketten- und Drittparteienrisiko	› Mangelnder Überblick über die Abdeckung des Drittanbieterrisikos › Drittanbieter-Sicherheit auf Compliance-Anforderungen begrenzt › Viertparteienrisiken werden nicht erfasst › Kein fester Reaktionsplan für Datenschutzverstöße bei Zulieferern	› Assessment von Zulieferern, doch Drittparteienrisiko dennoch unklar › Sicherheitsanforderungen an Zulieferer, jedoch mangelnde Umsetzung und Nachverfolgung › Incident Response umfasst Datenschutzverstöße bei Dritten, es fehlen jedoch die formellen Prozesse	› Regelmäßige Drittparteienrisiko-Assessments mit auf Risiko/Abhängigkeit abgestimmten Prüfungen und Audits › Sicherheitsanforderungen in Lieferantenverträgen verankert, ggf. mit verpflichtender Übertragung auf Viertparteien › Viertparteienrisiken werden bedacht, beurteilt und verwaltet › Klar definierter Notfallplan für Supply-Chain-Attacken › Zulieferer in Business-Continuity-Simulationen miteinbezogen