Quelle: HDI

Fünf Strategien für mehr Cyber-Resilienz im Mittelstand

Cyberangriffe treffen längst nicht mehr nur Konzerne – auch kleine und mittlere Unternehmen geraten zunehmend ins Visier. Welche Hebel wirklich wirken, erklärt David Bartolini, Head of Cyber Risk Engineering Tech bei HDI Global. Seine fünf praxisnahen Empfehlungen zeigen, wie Firmen ihre digitale Widerstandskraft erhöhen können.

Kontinuierliche Sensibilisierung und Schulung der Mitarbeitenden Menschliches Fehlverhalten bleibt ein wesentlicher Risikofaktor: Rund 60 Prozent aller Cybervorfälle sind laut ENISA-Report darauf zurückzuführen. Die HDI Cyberstudie zeigt, dass Angreifer vor allem über E-Mail und Social Engineering erfolgreich sind. 71 Prozent der befragten Unternehmen setzen inzwischen auf regelmäßige Awareness-Trainings und simulierte Phishing-Angriffe. Als Gegenmaßnahme besonders effektiv sind praxisnahe Angriffssimulationen und Readiness Workshops, wie sie im Rahmen von manchen Cyberversicherungen angeboten werden. Die Studie belegt jedoch, dass die Sensibilisierung nach einem Vorfall oft nur kurzfristig ansteigt. Nachhaltige, kontinuierliche Schulungsmaßnahmen sind daher unerlässlich. Aktualisierung von Software und Schließen von SicherheitslückenCyberkriminelle nutzen bevorzugt bekannte Schwachstellen in veralteter Software.
Ein konsequentes Patch-Management reduziert die Eintrittswahrscheinlichkeit eines Schadens um 23 Prozent. Ungepatchte Systeme gelten als Einfallstor für Angreifer. Gezieltes Risk Engineering und die kontinuierliche Überprüfung kritischer Infrastruktur sind daher nicht nur effektiv, sondern unabdinglich. Netzwerksegmentierung und technische Absicherung Mit der zunehmenden Vernetzung und der Ausweitung von Home-Office-Strukturen wächst die Angriffsfläche von Unternehmen. Wir sehen einen deutlichen Anstieg technischer Angriffe, etwa durch DDoS-Attacken. Professionelle IT-Maßnahmen wie Netzwerksegmentierung, Endpoint Detection and Response, Security Information and Event Management sowie der Betrieb eines Security Operations Center ermöglichen frühzeitiges Erkennen und Isolieren kompromittierter Systeme. Das Prinzip minimaler Zugriffsrechte begrenzt potenzielle Schäden. Management von Drittanbieter- und Lieferkettenrisiken Cyberrisiken entstehen auch durch externe Partner. Viele Unternehmen investieren nach einem Angriff in neue Hard- und Software und überprüfen verstärkt ihre Lieferantenbeziehungen. Dem ENISA-Report zufolge machen Supply-Chain-Angriffe mittlerweile über zehn Prozent der dokumentierten Bedrohungen aus. Besonders kritisch sind kompromittierte Software-Repositories und Schwachstellen bei Drittanbietern, die europaweit zu weitreichenden Sicherheitsvorfällen führen. Essenziell sind daher Cybersecurity-Klauseln in Verträgen, Nachweise über Sicherheitsstandards und gemeinsame

Infrastrukturtests. Vorbereitung auf den Ernstfall: Back-ups und Notfallübungen Eine hundertprozentige Prävention ist nicht möglich. Die durchschnittliche Betriebsunterbrechung nach einem Cyberangriff beträgt 4,2 Tage, bei kleinen Unternehmen sogar 5,5 Tage. Regelmäßige Back-ups und getestete Wiederherstellungspläne sind entscheidend, um Ausfallzeiten und Datenverluste zu minimieren.

Ganzheitliche Risikoanalyse erhöht Cyber-Resilienz Prävention und ganzheitliche Absicherung zahlen sich aus: Unternehmen mit einem hohen Umsetzungsgrad von Sicherheitsmaßnahmen sind rund 36 Stunden schneller wieder einsatzbereit und verzeichnen zehn Prozent geringere Kosten pro Schadenfall. Exzellente Versicherer agieren als Partner in Transformation für Industrie und Mittelstand, indem sie Kunden aktiv zur Seite stehen und praxisnahe Schutzkonzepte entwickeln, die Resilienz und Versicherbarkeit stärken. Durch individuelle Beratungsleistungen, und ein umfassendes Produktportfolio erhalten Unternehmen so gezielte Unterstützung bei ihrer digitalen Transformation.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4946729/Fuenf-Strategien-fuer-mehr-Cyber-Resilienz-im-Mittelstand/