expertenReport

Quelle: Redaktion experten.de / KI-generiert

Cyberversicherer setzen auf Dauer-Überwachung

Michael Fiedler

Cyberversicherer verändern ihre Risikoprüfung grundlegend. Statt punktueller Sicherheitschecks rücken kontinuierliche Schwachstellenscans, Echtzeit-Monitoring und automatisierte Warnsysteme in den Mittelpunkt. Ein neues Whitepaper von CyberDirekt zeigt: Die Branche entwickelt sich vom reinen Risikoträger zunehmend zum aktiven Präventionspartner.

Vom Fragebogen zur technischen Dauerprüfung

Die Studie analysiert elf führende Anbieter von Schwachstellenscans – darunter Cyberversicherer ebenso wie spezialisierte Security-Rating-Dienste. Das Ergebnis: Kontinuierliche Überwachung wird zunehmend zum Marktstandard. Neun der elf untersuchten Anbieter führen Scans inzwischen in kurzen Intervallen durch – teils täglich, wöchentlich oder sogar in Echtzeit. Mehrere Cyberversicherer bieten darüber hinaus ein 24/7-Monitoring mit automatischen Warnmeldungen bei neu entdeckten Schwachstellen an. Einzel-Scans verlieren dagegen an Bedeutung. Damit verändert sich auch die Rolle der Cyberversicherung selbst. Versicherer beschränken sich immer seltener auf die reine Schadendeckung, sondern greifen stärker in die laufende Prävention ein. Unternehmen sollen Sicherheitslücken möglichst erkennen und schließen, bevor daraus ein Schadenfall entsteht.

Versicherer honorieren gute Sicherheitswerte

Für Unternehmen entsteht dadurch ein neuer Zusammenhang zwischen IT-Sicherheit und Versicherbarkeit. Laut Whitepaper honorieren einige Versicherer gute Scan-Ergebnisse inzwischen mit günstigeren Prämien oder verbesserten Versicherungsbedingungen. Gleichzeitig steigt damit der Druck auf Unternehmen, ihre externe Angriffsfläche permanent im Blick zu behalten. Zu den typischen Prüfbereichen moderner Schwachstellenscans gehören unter anderem:

- offene Ports und aktive Dienste,
- veraltete Softwarestände,
- fehlerhafte TLS-/SSL-Konfigurationen,
- kompromittierte Zugangsdaten im Darknet,
- Malware- und Botnet-Indikatoren,
- Datenlecks in Cloud-Umgebungen.

Besonders auffällig: Mehr als die Hälfte der Anbieter integriert inzwischen Darknet- oder Data-Leak-Scans in ihre Lösungen.

Unternehmen sollen dadurch frühzeitig erkennen können, wenn Zugangsdaten oder sensible Informationen bereits außerhalb der eigenen Systeme kursieren.

Die Branche automatisiert – aber nicht ohne Grenzen

Trotz des technologischen Fortschritts zeigt das Whitepaper auch die Grenzen automatisierter Verfahren auf. Fast alle Anbieter setzen inzwischen auf vollautomatisierte Scans ohne individuelle Prüfungen durch Security-Analysten. Manuelle Penetrationstests werden häufig nur noch als Zusatzleistung angeboten. Das spart Aufwand und Kosten, bringt aber neue Probleme mit sich. Automatisierte Scans können Fehlalarme erzeugen und erkennen in der Regel nur bekannte Schwachstellen. Zero-Day-Lücken bleiben häufig unsichtbar. CyberDirekt verweist deshalb darauf, dass der eigentliche Mehrwert künftig weniger in der reinen Identifikation von Schwachstellen liegen dürfte, sondern stärker in deren Bewertung, Priorisierung und Behebung. Schwachstellenscans müssten zunehmend mit Threat Intelligence, Penetrationstests und aktivem Patchmanagement kombiniert werden.

Neue Anforderungen auch für Makler

Die Entwicklung dürfte auch die Rolle von Vermittlern verändern. Denn Cyberversicherungen werden technischer. Wer Unternehmen künftig beraten will, muss Unterschiede zwischen Schwachstellenscans, Leak-Monitoring, Darknet-Scans oder Threat-Intelligence-Ansätzen erklären können. „Die am Markt verfügbaren Angebote für Schwachstellenscans unterscheiden sich teils erheblich“, sagt Ole Sieverding, Geschäftsführer von CyberDirekt. „Mit diesem Whitepaper möchten wir Transparenz schaffen und Unternehmen sowie Maklern konkrete Entscheidungshilfen an die Hand geben.“ Die Studie zeigt zugleich, dass sich die Anbieter zunehmend angleichen. Neun von elf untersuchten Diensten decken inzwischen ein vergleichbares technisches Fundament ab. Unterschiede bestehen vor allem bei Zusatzfunktionen wie Darknet-Überwachung, Threat-Intelligence oder Beratungsleistungen.

Cyberversicherung entwickelt sich zur Präventionsplattform

Der Trend geht damit klar in Richtung integrierter Sicherheitsökosysteme. Versicherer entwickeln sich zunehmend zu Plattformanbietern, die Risikoanalyse, Monitoring, Prävention und Versicherungsschutz miteinander kombinieren. Das dürfte auch regulatorisch an Bedeutung gewinnen. Angesichts wachsender Anforderungen an Cyber-Resilienz, Dokumentation und IT-Sicherheit wächst der Druck auf Unternehmen, ihre Sicherheitslage dauerhaft nachweisen zu können. Das Whitepaper von CyberDirekt deutet damit auf einen strukturellen Wandel hin: Die Cyberversicherung der Zukunft dürfte weniger über den Schadenfall definiert werden – sondern stärker über die Fähigkeit, Schäden möglichst früh zu verhindern.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4949687/Cyberversicherer-setzen-auf-Dauer-Ueberwachung/