expertenReport

Quelle: Redaktion experten.de / KI-generiert

Cyberversicherung wird technischer: Was Vermittler jetzt verstehen müssen

Michael Fiedler

Schwachstellenscans, Darknet-Monitoring, Threat Intelligence: Cyberversicherungen entwickeln sich zunehmend zu technischen Präventionssystemen. Für Vermittler steigen damit die Anforderungen in der Beratung deutlich.

Schwachstellenscan ist nicht gleich Penetrationstest

In der Praxis werden technische Begriffe häufig vermischt. Dabei unterscheiden sich die Verfahren teilweise deutlich. Ein klassischer Schwachstellenscan untersucht automatisiert öffentlich erreichbare Systeme eines Unternehmens auf bekannte Sicherheitslücken. Dazu gehören etwa:

- veraltete Softwareversionen,
- offene Ports,
- fehlerhafte TLS-/SSL-Konfigurationen,
- bekannte Sicherheitslücken in Webanwendungen.

Der Vorteil: Die Verfahren lassen sich automatisiert, kostengünstig und regelmäßig durchführen. Ein Penetrationstest geht deutlich weiter. Dabei versuchen Sicherheitsexperten gezielt, Schwachstellen aktiv auszunutzen und reale Angriffsszenarien zu simulieren. PenTests sind aufwendiger, individueller – und erheblich teurer. Für Vermittler wird diese Unterscheidung relevant, weil Kunden häufig davon ausgehen, ein Schwachstellenscan entspreche bereits einer vollständigen Sicherheitsprüfung.

Darknet-Scans und Leak-Monitoring gewinnen an Bedeutung

Parallel dazu wächst die Bedeutung sogenannter Data-Leak- und Darknet-Scans. Diese Verfahren prüfen beispielsweise ob Zugangsdaten bereits kompromittiert wurden, ob Unternehmensdaten in Leaks auftauchen oder auch, ob Mailadressen oder Passwörter in bekannten Datenbanken kursieren. Gerade Cyberversicherer nutzen solche Informationen zunehmend zur laufenden Risikobewertung. Das verändert auch die Beratung: Cyberrisiken werden weniger abstrakt. Statt theoretischer Bedrohungen können konkrete Sicherheitsprobleme sichtbar gemacht werden.

Versicherer wollen kontinuierliche Transparenz

Der Trend geht dabei klar weg von punktuellen Prüfungen hin zu dauerhaftem Monitoring. Laut Whitepaper führen inzwischen neun der elf untersuchten Anbieter kontinuierliche oder regelmäßig automatisierte Scans durch. Dadurch verändert sich auch die Rolle der Versicherung: vom reinen Schadenträger hin zum aktiven Präventionspartner. Für Unternehmen bedeutet das: Die eigene IT-Sicherheitslage wird nicht mehr nur beim Vertragsabschluss relevant, sondern dauerhaft beobachtet.

Technische Scores werden zum Wettbewerbsfaktor

Cyberversicherer arbeiten zunehmend mit technischen Risikoscores. Diese sollen bewerten, wie angreifbar ein Unternehmen aktuell ist. Solche Scores können künftig Einfluss haben auf:

- Versicherbarkeit,
- Prämienhöhe,
- Selbstbehalte,
- Vertragsbedingungen,
- Präventionsauflagen.

Damit geraten Vermittler stärker in eine beratende Rolle zwischen IT-Sicherheit und Versicherungsschutz.

Die Grenzen automatisierter Verfahren

Gleichzeitig zeigt das Whitepaper auch die Schwächen automatisierter Analysen. Fast alle Anbieter setzen inzwischen auf vollautomatisierte Verfahren. Das bringt Probleme mit sich:

- Fehlalarme,
- fehlende Kontextbewertung,
- keine Erkennung unbekannter Zero-Day-Lücken,
- begrenzte Aussagekraft über reale Angriffswege.

Ein „grüner“ Sicherheitsstatus bedeutet daher nicht automatisch, dass ein Unternehmen tatsächlich sicher ist. Gerade deshalb gewinnen ergänzende Verfahren wie: Threat Intelligence, manuelle Penetrationstests, Sicherheitsberatung, Patchmanagement an Bedeutung.

Vermittlerrolle verändert sich

Für Vermittler entsteht daraus ein neues Spannungsfeld. Künftig reicht es immer seltener aus, lediglich Deckungssummen und Bedingungen zu vergleichen. Unternehmen erwarten zunehmend Orientierung bei:

- technischen Mindeststandards,
- Sicherheitsanforderungen,
- Präventionsmaßnahmen,
- Monitoring-Tools.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4949693/Cyberversicherung-wird-technischer-Was-Vermittler-jetzt-verstehen-muessen/