CYBER RESILIENZ
WIRD UNTER DORA ZUNEHMEND ZUR MANAGEMENTAUFGABE

protiviti®
Global Business Consulting

Die Versicherungsbranche steht vor einer stillen, aber tiefgreifenden Verschiebung: Während die Digitalisierung weiter an Geschwindigkeit gewinnt, entwickeln sich auch Cyberangriffe mit einer Dynamik, die klassische Sicherheitsansätze zunehmend überfordert. Mit dem Digital Operational Resilience Act (DORA) reagiert die Europäische Union darauf und macht Cyber Resilienz zur klaren Managementaufgabe.

Im Kern geht es um eine neue Frage: Wie verwundbar ist eine Organisation tatsächlich – unter realen Bedingungen? Zwei Ansätze rücken deshalb in den Mittelpunkt, ein risikobasiertes Vulnerability Management und das Threat led Penetration Testing (TLPT). Gemeinsam verschieben sie den Fokus weg von abstrakten Schwachstellen hin zu realen Angriffsszenarien.

Besonders deutlich wird dieser Perspektivwechsel im Vulnerability Management. Was lange als technischer Nebenprozess galt, entwickelt sich zu einem zentralen Steuerungsinstrument. Entscheidend ist nicht mehr allein, wie kritisch eine Schwachstelle bewertet wird, sondern ob sie tatsächlich ausnutzbar ist und welche Auswirkungen dies auf zentrale Geschäftsprozesse hätte. Erst durch die Verknüpfung von technischer Bewertung, Bedrohungslage und Geschäftsrelevanz entsteht eine belastbare Grundlage für Priorisierung und Entscheidungen.

Gleichzeitig wächst die Bedeutung der Integration. Schwachstellenmanagement, Incident Response und Threat Intelligence greifen zunehmend ineinander und formen ein lernendes System, das sich dynamisch anpasst. Damit verändert sich auch die Perspektive auf Sicherheit – von isolierten Maßnahmen hin zu einer durchgängigen Betrachtung der eigenen Angriffsfläche.

An dieser Stelle setzt TLPT an. Während Vulnerability Management Transparenz schafft, konfrontiert TLPT die Organisation mit einem realitätsnahen Stresstest. Statt einzelner Systeme werden vollständige Angriffsverläufe simuliert, inklusive Motivation, Vorgehensweise und Zielbild potenzieller Angreifer. Sichtbar werden dadurch nicht nur technische Schwächen, sondern vor allem Brüche in Prozessen, Entscheidungswegen und der Zusammenarbeit.

Gerade für Versicherer ist das von besonderer Relevanz. Komplexe IT Landschaften, eng verflochtene Partnerstrukturen und sensible Daten führen dazu, dass Verwundbarkeiten selten isoliert auftreten. Sie entstehen im Zusammenspiel zwischen Systemen, Prozessen und beteiligten Einheiten. TLPT macht diese Zusammenhänge sichtbar und zeigt, wo Risiken im Ernstfall tatsächlich wirksam werden.

Die eigentliche Stärke entfaltet sich jedoch erst im Zusammenspiel beider Ansätze. Während das Vulnerability Management kontinuierlich Risiken sichtbar macht und strukturiert reduziert, zeigt TLPT, welche dieser Risiken im konkreten Angriffsszenario entscheidend sind. So entsteht erstmals ein belastbares Gesamtbild der eigenen Verwundbarkeit und eine fundierte Basis für Priorisierung und Steuerung.

In der praktischen Umsetzung zeigt sich hingegen, dass genau diese Verzahnung vielfach die größte Herausforderung darstellt. Einzelne Komponenten sind häufig vorhanden, entfalten aber nicht ihre volle Wirkung, weil sie nicht konsistent miteinander verbunden sind. Schwachstellen werden erkannt, aber nicht entlang realer Angriffsszenarien priorisiert. Testergebnisse liefern Erkenntnisse, werden jedoch nicht systematisch

in nachhaltige Verbesserungen überführt. Gerade TLPT erfordert zudem eine präzise Orchestrierung von der Definition realistischer Szenarien bis zur Abstimmung zwischen technischen und organisatorischen Einheiten.

Damit wird deutlich: Cyber Resilienz ist weniger eine Frage einzelner Maßnahmen als eine Integrationsaufgabe. Sie erfordert ein abgestimmtes Zusammenspiel von Methodik, Organisation und operativer Erfahrung. In vielen Fällen entsteht der größte Aufwand nicht durch fehlende Instrumente, sondern durch die Herausforderung, diese wirkungsvoll zu verbinden und dauerhaft steuerbar zu machen.

DORA gibt hierfür den Rahmen vor, lässt aber bewusst Spielraum in der Umsetzung. Versicherungsunternehmen stehen daher vor der Aufgabe, aus regulatorischen Anforderungen ein konsistentes und wirksames Resilienzmodell zu entwickeln. Gerade dort, wo interne Strukturen auf komplexe Anforderungen und hohe Umsetzungstiefe treffen, zeigt sich, dass zusätzliche methodische Erfahrung und externe Vergleichsperspektiven häufig den entscheidenden Unterschied ausmachen.

Cyber Resilienz ist damit kein Zielzustand, sondern ein fortlaufender Prozess. Unternehmen, die es schaffen, Vulnerability Management und TLPT integriert zu denken und nachhaltig zu steuern, gewinnen nicht nur Sicherheit im Umgang mit regulatorischen Anforderungen, sondern vor allem ein realistisches Verständnis ihrer eigenen Verwundbarkeit und die Fähigkeit, diese gezielt zu reduzieren.

Kontakt

DR. MICHAEL RIECKER
Director Cyber Security
Protiviti Deutschland
michael.riecker@protiviti.com