CISCO
SECURE

5 praxiserprobte Schritte zur Stärkung der Cybersicherheit

Cybersicherheit bleibt auch weiterhin ein Thema von höchster Brisanz. Denn die Vernetzung schreitet immer rasanter voran, mit immer komplexeren Systemstrukturen. Komplexität, die für Sicherheitsteams vor allem eines bedeutet: mehr Herausforderungen.

Diese aber lassen sich anhand konkreter Maßnahmen angehen. Praxisrelevante Daten dazu haben wir im Rahmen der nunmehr zweiten Ausgabe der Security Outcomes-Studie erhoben, für die wir über 5.100 Verantwortliche aus Sicherheit und IT in 27 Ländern befragt haben. Die folgenden fünf Maßnahmen unserer Checkliste kristallisierten sich dabei als zentral für die Umsetzung starker Sicherheitsverfahren heraus.

Modernisierung von Technologie

Im Schnitt sind 39 % der von Unternehmen eingesetzten Sicherheitstechnologien veraltet.

Nehmen Sie Modernisierungen proaktiv in Angriff – bevor Ihnen ein Sicherheitsvorfall den Stand Ihres Tech-Stacks vor Augen führt.

> Dass knapp 40 % der Unternehmen in puncto Sicherheit technologisch überholt sind, zeugt von den nach wie vor erheblichen Defiziten. Erfreulicherweise verzeichnen wir aber auch proaktive Unternehmen, die über moderne, konsolidierte Cloud-Architekturen regelmäßig Modernisierungen ihrer Technologie vornehmen. Das Problem und die Lösung."
>
> Richard Archdeacon, Advisory CISO, Cisco

Transparenz durch Integration

77 % der Unternehmen würden integrierte Lösungen lieber kaufen als selbst entwickeln.

Cloud-basierte Lösungen und leistungsstarke Integrationen sind inzwischen erfreulicherweise weit verbreitet, denn sie liefern Sicherheitsteams umfassendere Transparenz für ihre Systeme.

> Moderne, gut integrierte IT trägt mehr zum Gesamterfolg des Programms bei als jede andere Sicherheitspraxis oder -kontrolle."
>
> Helen Patton, Advisory CISO, Cisco

Personalaufstockung im Team

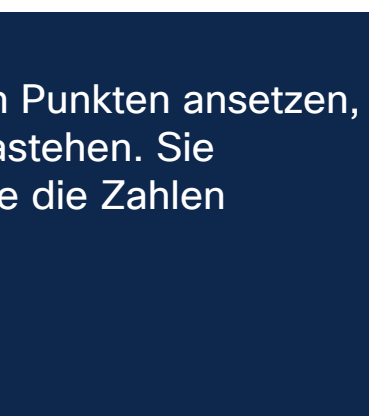
Bei Unternehmen mit den im Verhältnis zur Mitarbeiterzahl stärksten Sicherheitsteams ist eine starke Erkennung und Beseitigung von Bedrohungen um 20 % wahrscheinlicher.

Zusätzliches Personal einzustellen ist natürlich nicht immer eine Option. Bestehendes Personal weiterzubilden wäre eine Alternative – beziehungsweise ist dies tatsächlich immer eine sinnvolle Investition.

> Wählen Sie die am besten qualifizierten Mitarbeiter:innen für Ihre SecOps-Teams aus, denn das ist wichtiger als die reine Anzahl. Durch Automatisierung können Sie die Lücken Ihrer Nachwuchskräfte schließen und Ergebnisse erzielen, die genauso stark sind wie mit erfahreneren Mitarbeiter:innen."
>
> Wendy Nather, Head of Advisory CISOs, Cisco

Intelligente Erkennung mit Threat-Intelligence

Durch die Nutzung von Threat-Intelligence ist bei den entsprechenden Unternehmen eine starke Erkennung und Beseitigung doppelt so wahrscheinlich.



Threat-Intelligence sollten Sie sich in jedem Fall und in sämtlicher verfügbarer Form zunutze machen, um intelligenter zu arbeiten und bessere Ergebnisse zu erzielen.

> Wenn Unternehmen starke Mitarbeiter:innen, Prozesse und Technologien kombinieren, erhalten sie erweiterte Funktionen zur Bedrohungserkennung und -reaktion – vorausgesetzt, sie stützen sich dabei auf leistungsfähige Threat-Intelligence."
>
> Dave Lewis, Advisory CISO, Cisco

Testweises Herbeiführen von Störfällen

Bei Unternehmen, die Chaos Engineering anwenden, sind Verbesserungen rund um die Business Continuity doppelt so wahrscheinlich.

Im Chaos die Ordnung finden – so in etwa lässt sich die Strategie beschreiben, anhand derer in regelmäßigen Abständen beabsichtigt herbeigeführte IT-Störfälle Ihnen dabei helfen, sich für den Ernstfall vorzubereiten.

> Wer Notfallszenarien gezielt durchspielt, hält im Ernstfall eher den Betrieb stabil. Bei Unternehmen, die hierzu regelmäßig verschiedene Testverfahren zur Anwendung brachten, war dies um 2,5 mal wahrscheinlicher. Chaos Engineering bietet hier ein noch effektiveres Testverfahren."
>
> Wolfgang Goerlich, Advisory CISO, Cisco

Zahlen lügen nicht, wie man sagt. Wenn Sie also an diesen Punkten ansetzen, werden Sie in puncto Cybersicherheit signifikant stärker dastehen. Sie möchten mehr Details? Im vollständigen Bericht können Sie die Zahlen nachprüfen.

Bericht herunterladen

779292577 | 12/21

CISCO The bridge to possible