Der CISO-Mythos – Checkliste zur Vorbereitung

Die Patches kommen. Bevor sie eintreffen, werden Ihr Vorstand, Ihre Rechtsabteilung und die Regulierungsbehörden Fragen haben.

1 Exposure & Asset-Sichtbarkeit

„Wie groß ist unsere Gefährdung, und haben wir ein genaues Bestandsverzeichnis unserer Assets?"

- ☐ Aktualisieren Sie Ihr Asset-Verzeichnis, um Ihre aktuelle Produktionsumgebung abzubilden.
- ☐ Bestätigen Sie, dass kontinuierliches Scanning in allen Produktionsumgebungen aktiv ist.
- ☐ Bewerten Sie Schwachstellen neu mit risikobasierter Priorisierung statt reiner CVE-Zählung.
- ☐ Bereiten Sie eine einseitige Exposure-Zusammenfassung vor, die Sie jederzeit für die Geschäftsführung bereitstellen können.

2 Patch-Geschwindigkeit & Produktionssicherheit – Erkennung & Eindämmung

„Können wir schnell genug und in großem Maßstab patchen, ohne die Produktion zu beeinträchtigen?"

- ☐ Überprüfen Sie Ihren aktuellen Patch-Zyklus gegen das Fenster zwischen Offenlegung und Waffeneinsatz.
- ☐ Priorisieren Sie Assets nach Kritikalität, bevor die Welle kommt – nicht währenddessen.
- ☐ Dokumentieren Sie ein Change-Management-Protokoll mit benannten Verantwortlichen und Rollback-Pfaden.
- ☐ Führen Sie ein Tischübungsszenario für eine schnelle Patch-Bereitstellung durch, um Entscheidungspfade und Rollback-Bereitschaft zu testen.

3 Supply-Chain & Open-Source-Exposure

„Was verbirgt sich in unserer Open-Source- und Drittanbieter-Software?"

- ☐ Erstellen oder aktualisieren Sie Ihre Software Bill of Materials (SBOM).
- ☐ Erfassen Sie Drittanbieter-Integrationen, die durch Übernahmen geerbt wurden.
- ☐ Implementieren Sie kontinuierliches Scanning von Open-Source-Bibliotheks-Abhängigkeiten.
- ☐ Identifizieren Sie Patch-SLAs von Lieferanten und Kontaktpunkte, bevor die Offenlegung erfolgt.

4 Engineering-Kapazität

„Verfügen wir über die Engineering Kapazität, um unseren eigenen Rückstand zu beheben?"

- ☐ Schätzen Sie die Behebungsstunden gegen die aktuellen Verpflichtungen Ihres Teams.
- ☐ Triagieren Sie den Rückstand, um interne Teams nur auf die höchsten Risiken zu konzentrieren.
- ☐ Sichern Sie externe Engineering-Ressourcen, bevor Sie sie benötigen.
- ☐ Integrieren Sie sichere Standardpraktiken in die laufende Entwicklung jetzt schon.

5 Erkennung & Eindämmung

„Falls ein Patch verzögert wird – können wir den Exploit erkennen und eindämmen?"

- ☐ Bestätigen Sie, dass die 24/7-SOC-Überwachung in allen kritischen Umgebungen aktiv ist.
- ☐ Definieren Sie ein Ziel für die mittlere Zeit bis zur Triage und Isolierung (Minuten, nicht Stunden).
- ☐ Führen Sie proaktive Threat-Hunts durch, die auf Mythos-Exposure-Flächen abzielen.
- ☐ Validieren Sie Ihr „Assume-Breach"-Playbook durch eine aktuelle Übung oder Simulation.

Executive Readiness Check

Bevor Sie die Geschäftsführung informieren:

- ☐ Identifizieren Sie, welche dieser Antworten Sie heute verteidigen können und welche Unterstützung oder Rückendeckung der Geschäftsführung erfordern.

Falls Sie entscheiden, wie diese Lücken geschlossen werden:

Einige Organisationen bauen diese Fähigkeiten intern auf. Andere arbeiten mit Partnern zusammen, um die Abdeckung zu beschleunigen oder begrenzte Teams zu unterstützen. Insight Managed Exposure Defence ist ein integrierter Ansatz, der alle fünf Bereiche oben abdeckt – zunächst intern aufgebaut und betrieben, dann auf Kunden ausgeweitet, die vor denselben Fragen stehen.

Weitere Informationen: de.insight.com