Verfügt Cyber Crucible über ein Patch-Management-Programm?

Kurze Antwort: Ja. Ein risikobasiertes Patch- und Schwachstellen-Management-Programm hält Software, Kernel-Treiber, Server und Endpunkte auf dem neuesten Stand, und Feststellungen werden bis zur Behebung nachverfolgt.

Funktionsweise

Kontinuierliche automatisierte Sicherheitstests laufen innerhalb der Entwicklungspipeline, risikobasierte manuelle Penetrationstests werden mit einer jährlichen Mindestfrequenz durchgeführt, und ereignisgesteuerte Tests laufen bei jeder wesentlichen Änderung, wobei sowohl interne als auch externe Netzwerke abgedeckt werden. Sicherheitspatches und Hotfixes werden gemäß Herstellerempfehlung eingespielt, und die verantwortlichen Gruppen (Owner Groups) sind dafür zuständig, bei den jeweils relevanten Patches auf dem Laufenden zu bleiben. Wechseldatenträger und tragbare Medien unterliegen demselben Schutz und derselben Prüfung wie fest installierte Medien.

Priorisierung und Bereitstellung

Feststellungen werden nach Schweregrad und Ausnutzbarkeit priorisiert, wobei aktiv ausgenutzte Schwachstellen über einen beschleunigten, außerplanmäßigen Weg bearbeitet werden. Patches durchlaufen den Change-Management-Prozess – sie werden vor der Überführung in die Produktivumgebung validiert –, und Kernel-Treiber-Updates werden vor der Veröffentlichung erneut über Microsoft WHCP validiert.

Ausrichtung an Rahmenwerken und die ehrliche Grenze

Das Programm orientiert sich an NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7 und ISO/IEC 27001:2022 A.8.8. Es wird keine Zertifizierung beansprucht. Konkrete Zielfristen für die Behebung sowie entsprechende Nachweise werden Prüfern unter NDA zur Verfügung gestellt.

Revision #1
Created 2026-07-24 23:30:16 UTC by Dennis Underwood
Updated 2026-07-24 23:30:16 UTC by Dennis Underwood