Engineer

Drei Türschlösser, keines davon abgeschlossen

Drei nie funktionierende SSH-Brute-Force-Schutzmechanismen gefunden und korrigiert: eine Sperr-Jail für Port 22 bei einem auf 1986 lauschenden Daemon, eine durch eine allgemeinere vorherige Regel verdeckte Ratenbegrenzung und eine Sperraktion, deren Programm nie gefunden wurde, sodass nie eine Sperre griff.

August 2026

drei Brute-Force-Abwehrmechanismen, die nie funktioniert hatten

Situation. Eine Härtungsprüfung des Produktivhosts im August 2026 stellte eine üblicherweise selbstbewusst beantwortete Frage: Funktionieren die Schutzmaßnahmen gegen SSH-Brute-Force-Angriffe? Alle drei waren konfiguriert, alle drei erschienen in jedem betrachteten Bericht, und alle drei waren seit dem Aufbau des Hosts wirkungslos gewesen.

Aufgabe. Die Kontrollen mussten gegen die tatsächliche Paketverarbeitung des Kernels geprüft werden statt gegen Konfigurationsdateien, die nur das beabsichtigte Verhalten beschreiben.

Massnahmen. Das Lesen der Konfiguration hätte dreimal die falsche Antwort bestätigt. Deshalb wurde das laufende System untersucht. Die Angriffssperr-Jail überwachte Port 22, während der Daemon bei der anfänglichen Härtung auf 1986 verlegt worden war. Jede Sperre nannte einen Port, auf dem nichts lauschte. Die Ratenbegrenzung der Firewall war subtiler fehlerhaft: Die Regel existierte, stand jedoch unter einer weiter gefassten, zuerst passenden Regel. Benutzerregeln werden von oben nach unten ausgewertet; der erste Treffer gilt. Eine allgemeine Freigabe oberhalb der Ratenbegrenzung macht diese zu unerreichbarem Code, der dennoch in jeder Statusliste erscheint. Der dritte Fehler war am stillsten: Die Sperraktion ruft ein Paketfilterprogramm auf, das die Paketverwaltung lediglich empfiehlt, statt es zwingend vorauszusetzen. Ohne dieses Programm startet die Jail, zählt und entscheidet,

scheitert aber genau beim Sperrversuch. Alle drei Korrekturen waren klein. Wesentlicher waren zwei daraus entstandene Repositoryregeln: Sicherheitskontrollen erhalten eine ausführbare Prüfung statt eines Kommentars; Firewalls werden nach Regelposition statt bloßer Regelexistenz verifiziert.

Ergebnis. Drei zuvor nie wirksame Schutzmaßnahmen funktionieren nun. Ihre Fehlerklasse — eine Kontrolle, die bei Ausfall weiterhin einen gesunden Zustand meldet — ist genau diejenige, auf deren Erkennung die Plattformprüfungen jetzt ausgerichtet sind. Alle drei waren seit der Erstinstallation wirkungslos. Alle drei meldeten überall, wo jemand hinsah, einen gesunden Zustand. Genau deshalb blieben sie so lange unentdeckt.

Diese Erfahrung für Ihr Projekt nutzen

Nutzen Sie „Drei Türschlösser, keines davon abgeschlossen“ als Ausgangspunkt für eine ähnliche Herausforderung in Ihrer Organisation. Die Leistungen hinter dieser Arbeit stehen auch für Ihr Projekt zur Verfügung. Monitoring und Alarme melden sich, solange ein Fehler noch klein ist; Kennzahlen zeigen, wie oft das gelingt.

Unsere Leistungen entdecken Kontakt aufnehmen →

Hinter das Ergebnis schauen

Lesen Sie die Situation, die Entscheidungen und das Ergebnis dieses Beispiels. Wir können besprechen, welche Teile sich auf Ihre Rahmenbedingungen übertragen lassen und welche einen anderen Ansatz erfordern. Drei Türschlösser, keines davon abgeschlossen — drei Brute-Force-Abwehrmechanismen, die nie funktioniert hatten

Unsere Leistungen entdecken Kontakt aufnehmen →

Schützt Ihr Angriffsschutz wirklich?

Besprechen Sie Ihr Projekt mit der Ingenieurin, die für die Umsetzung verantwortlich ist. Wir vereinbaren Umfang, Preisgrundlage und Übergabe schriftlich, bevor die Arbeit beginnt.

Rollenkontext: Sicherheitsingenieurin. Die Arbeit baut auf Infrastruktur, Monitoring und Observability, Netzwerke und VPN, Linux und Server, Sicherheit und Systemadministration. Und wenn Sie schon hier sind: Wir sind auch ziemlich gut in Site Reliability und Monitoring, Netzwerke und VPN-Einrichtung, Sicherheits- und Zugriffsverwaltung und Sicherheit von KI-Agenten.

Kontakt aufnehmen Unsere Leistungen entdecken

Ein Teil einer **längeren Arbeitsbilanz** — vollständig auf dieser Website zu finden.

Jeder Eintrag folgt demselben Aufbau: die Situation, die Aufgabe, unser Vorgehen und die Veränderungen.

Alle Arbeiten ansehen

Die benötigte Verbesserung definieren

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Schützt Ihr Angriffsschutz wirklich?

Fragen Sie nach den Entscheidungen hinter „Drei Türschlösser, keines davon abgeschlossen“. Sie sprechen mit den Menschen, die die Arbeit erklären und Ihr eigenes Projekt einschätzen können.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/portfolio/three-locks-on-the-door-none-of-them-locked/