Engineer

Bevisade att intrångsspärren fungerar varje gång

Bevisade spärrkedjan mot intrång från början till slut vid varje härdningskörning genom att spärra en reserverad testadress, läsa den kärnregel som uppstod och häva spärren i ett städblock som alltid körs, så att en jail som slutar fungera fäller körningen i stället för att rapportera att allt är i ordning.

september 2026

spärrkedjan, bevisad vid varje härdningskörning

Situation. Tjänsten som spärrar intrångsförsök hade redan ertappats med att lägga spärrar på en port som SSH-daemonen inte lyssnade på. Att rätta porten stängde just det fallet. Det gjorde ingenting åt orsaken till att felet hade överlevt så länge, nämligen att ett spärrflöde saknar synligt felläge: tjänsten körs, jailen listas som aktiv, och ingenstans står det om en spärr någonsin når kärnan.

Uppgift. Spärrflödet måste provas skarpt vid varje konvergenskörning, mot den aktiva regeluppsättningen, i stället för att härledas ur att tjänsten är igång.

Handling. Konvergenskörningen spärrar nu en adress ur det block som standarderna reserverar för dokumentation, läser tillbaka den resulterande regeln i kärnans paketfilter och häver spärren i ett städblock som körs oavsett om kontrollen gick igenom eller misslyckades. Det reserverade intervallet är det bärande valet — testadressen tillhör ingen, så en kvarglömd spärr som överlever en misslyckad körning kan inte stänga ute ett verkligt nätverk. Återläsningen från kärnan är den andra halvan: tjänstens egen statusutdata skulle rapportera framgång för en spärr som inte gav upphov till någon regel, vilket är exakt det fel som testas. Vid sidan av detta är spärrbackenden fastlåst i stället för att lämnas åt tjänstens egen identifiering, och loggbackenden är inställd på automatisk identifiering eftersom operativsystemet inte levereras med någon traditionell autentiseringslogg och fel val misslyckas tyst genom att bevaka en fil som aldrig dyker upp.

Resultat. Ett spärrflöde som slutar fungera får nu en konvergenskörning att misslyckas i stället för att fortsätta rapportera felfri status, och det var den enda egenskap som spelade någon roll. Det kostar några sekunder vid varje körning, och varje gång skrivs och tas en brandväggsregel bort i produktion, vilket är ett verkligt ingrepp i ett system i drift och godtogs med motiveringen att alternativet redan hade visat sig vara sämre.

Använd erfarenheten i ert projekt

Använd ”Bevisade att intrångsspärren fungerar varje gång” som utgångspunkt för en liknande utmaning i er organisation. Tjänsterna bakom arbetet finns tillgängliga för ert projekt. Övervakning och larm som säger till medan ett fel fortfarande är litet, och siffrorna som visar hur ofta det förblir så.

Se våra tjänster Hör av er →

Se bakom resultatet

Läs om situationen, besluten och resultatet i exemplet. Vi kan diskutera vad som passar era förutsättningar och vad som kräver ett annat angreppssätt. Bevisade att intrångsspärren fungerar varje gång — spärrkedjan, bevisad vid varje härdningskörning

Se våra tjänster Hör av er →

Skulle du märka om en skyddsåtgärd slutade fungera?

Prata om ert projekt med ingenjören som ansvarar för leveransen. Vi avtalar omfattning, hur priset beräknas och överlämning skriftligt innan arbetet börjar.

Roll i uppdraget: Säkerhetsingenjör. Det bygger på Infrastruktur, Automatisering och CI/CD, Tillförlitlighet och säkerhetskopiering, Linux och servrar, Säkerhet och Test och kvalitetssäkring. Och nu när ni är här: vi är ganska bra på Tillförlitlig drift och övervakning, Systemadministration, Säkerhet och behörighetshantering och Säkerhet för AI-agenter.

Hör av er Se våra tjänster

En del av **en längre historik** — och den finns i sin helhet här.

Varje post är skriven på samma sätt: situationen, uppgiften, vad vi gjorde och vad som förändrades.

Se hela historiken

Definiera förbättringen ni behöver

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Skulle du märka om en skyddsåtgärd slutade fungera?

Fråga om besluten bakom ”Bevisade att intrångsspärren fungerar varje gång”. Ni talar med personer som kan förklara arbetet och bedöma ert eget projekt.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/portfolio/proved-the-intrusion-ban-works-every-run/