Engineer Rådgivning

Skrev en avgränsningsregel efter läckta uppgifter

Skrev in en avgränsningsregel i repot efter att en omstrukturering hade fört in ett annat företags värdförteckning, brandväggsundantag och text i det — och höll de karantänsatta resterna kvar under skanningen efter hemligheter i stället för att undanta dem.

september 2026

en avgränsningsregel, efter att ett annat företags IT-miljö hade dykt upp

Situation. Arbete som hade gjorts åt ett annat företag följde med genom en omstrukturering av repot och blev kvar. Det som följde med var inte abstrakt: en kladdlogg med aktiva inloggningsuppgifter i klartext, som låg kvar i trädet förbi varje skydd under större delen av repots historik; en inaktuell inventory som namngav det företagets värd; och en task-fil för brandväggen som öppnade portar mot sexton av dess kundnätverk. Inget av det kördes. Det är precis därför det överlevde — ingenting som inte körs någonstans granskas någonsin igen.

Uppgift. Gränsen måste bli en regel med ett test kopplat till sig, snarare än en avsikt, och resterna måste hanteras på ett sätt som inte bara gömde undan dem.

Handling. Regeln är nu det inledande avsnittet i repots instruktioner: det här repot hanterar ett enda företags infrastruktur och bara den, och en annan parts värd, inventory, brandväggsöppning, DNS-zon eller inloggningsuppgift hör inte hemma i det — inte ens avaktiverad, bortkommenterad eller parkerad i en fil som ingen playbook importerar. Det praktiska testet står bredvid: skulle det här företaget fortfarande vara ansvarigt för detta om relationen tog slut. Resterna sattes i karantän i en tydligt namngiven katalog i stället för att raderas, så att historiken förblir läsbar, och karantänen är medvetet partiell — de två strukturella lintverktygen hoppar över den, medan hemlighetsskannern, vault-skyddet och emojikontrollen medvetet fortfarande läser den, eftersom det är de tre som skulle fånga det som tog sig in. Läckan i sig gav upphov till en

lintregel: ett eget mönster som flaggar en inloggningsuppgift som skickas som en kommandoradsflagga, vilket var den form den läckta hade och som den vanliga regeluppsättningen inte matchade.

Resultat. Omfattningsgränsen är en nedskriven regel med ett angivet test, resterna är synliga i stället för begravda, och den specifika form av inloggningsuppgift som tog sig igenom får nu en commit att misslyckas. Lärdomen som har dokumenterats vid sidan av är den allmänna: den farliga artefakten är inte den som körs, utan den som inte gör det, eftersom det är den som ingen läser igen.

Använd erfarenheten i ert projekt

Använd ”Skrev en avgränsningsregel efter läckta uppgifter” som utgångspunkt för en liknande utmaning i er organisation. Tjänsterna bakom arbetet finns tillgängliga för ert projekt. Överlämningar, driftinstruktioner och manualer som låter din egen personal driva systemet utan att ringa den som byggde det.

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. Skrev en avgränsningsregel efter läckta uppgifter — en avgränsningsregel, efter att ett annat företags IT-miljö hade dykt upp

Se våra tjänster Hör av er →

Kan ett projekts hemligheter hamna i ett annats?

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 Datastyrning, Infrastruktur, Automatisering och CI/CD, Säkerhet och Dokumentation. Och nu när ni är här: vi är ganska bra på Datastyrning och datakvalitet, Säkerhet och behörighetshantering, Säkerhet för AI-agenter och Teknisk dokumentation.

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 beslutet, människorna som berörs och alternativen som övervägts. Vi kan tydliggöra avvägningarna och lämna en dokumenterad rekommendation.

Se vad det kostar Hör av er →

Kan ett projekts hemligheter hamna i ett annats?

Fråga om besluten bakom ”Skrev en avgränsningsregel efter läckta uppgifter”. 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://advisory.engineer.company/sv/portfolio/wrote-a-scope-rule-after-a-credential-leak/