Engineer Plattform

Tre lås på dörren, inget av dem låst

Hittade och åtgärdade tre skydd mot brute force-attacker över SSH som aldrig hade fungerat: en jail som bevakade port 22 medan daemonen lyssnade på 1986, en hastighetsbegränsning som skuggades av en bredare regel ovanför den och en spärråtgärd vars binärfil aldrig gick att hitta, så att ingen spärr någonsin hade tillämpats.

augusti 2026

tre skydd mot brute force-attacker som aldrig hade fungerat

Situation. En härdningsgranskning av produktionsservern i augusti 2026 ställde en fråga som brukar få ett självsäkert svar: fungerar skydden mot brute force-attacker via SSH. Alla tre var konfigurerade, alla tre syntes i varje rapport som någon tittade på, och alla tre hade varit verkningslösa sedan den dag servern byggdes.

Uppgift. Skydden måste kontrolleras mot vad kärnan faktiskt gör med ett paket, i stället för mot de konfigurationsfiler som beskriver vad som borde hända med det.

Handling. Att läsa konfigurationen hade bekräftat fel svar tre gånger, så granskningen läste det körande systemet i stället. Jailen för spärrning av intrångsförsök bevakade port 22, medan daemonen hade flyttats till 1986 under den första härdningen — varje spärr den skrev angav en port som ingenting lyssnade på. Brandväggens hastighetsbegränsning var värre på ett subtilare sätt: regeln fanns, och den låg under en bredare regel som matchade först. Brandväggens användarregler utvärderas uppifrån och ned och den första matchningen vinner, så en bred tillåtande regel ovanför en hastighetsbegränsning gör begränsningen till död kod som ändå syns i varje statuslistning. Det tredje skyddet var det tystaste av dem: spärråtgärden anropar via skalet en binär för paketfiltrering som paketsystemet bara rekommenderar i stället för att kräva, så på en server som saknar den startar jailen, räknar och fattar beslut, och fallerar sedan i just det ögonblick den försöker spärra. Alla tre åtgärderna var små. Det som kom ut av det var inte åtgärderna utan två regler

som nu styr repot: ett säkerhetsskydd får en kontroll i stället för en kommentar, och en brandvägg verifieras utifrån reglernas position snarare än utifrån att reglerna finns.

Resultat. Tre skydd som aldrig en enda gång hade slagit till gör det nu, och den klass av defekter som de tillhör — ett skydd vars sätt att fallera är att det fortsätter att rapportera att allt är i sin ordning — är den klass som plattformens kontroller nu är byggda för att fånga. Alla tre hade varit verkningslösa ända sedan servern sattes upp. Alla tre visade att allt var i sin ordning överallt där någon tittade, vilket är hela anledningen till att de fick bestå.

Använd erfarenheten i ert projekt

Använd ”Tre lås på dörren, inget av dem låst” 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. Tre lås på dörren, inget av dem låst — tre skydd mot brute force-attacker som aldrig hade fungerat

Se våra tjänster Hör av er →

Är du säker på att ditt intrångsskydd verkligen skyddar?

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, Övervakning och observerbarhet, Nätverk och VPN, Linux och servrar, Säkerhet och Systemadministration. Och nu när ni är här: vi är ganska bra på Tillförlitlig drift och övervakning, Nätverk och VPN-uppsättning, 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 →

Är du säker på att ditt intrångsskydd verkligen skyddar?

Fråga om besluten bakom ”Tre lås på dörren, inget av dem låst”. 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://platform.engineer.company/sv/portfolio/three-locks-on-the-door-none-of-them-locked/