Engineer

Tre låse på døren, ingen af dem låst

Har fundet og rettet tre SSH-beskyttelser mod brute force, der aldrig havde virket: en jail, der holdt øje med port 22, mens dæmonen lyttede på 1986, en ratebegrænsning, som en bredere regel over den overskyggede, og en blokeringshandling, hvis binærfil aldrig blev fundet, så ingen blokering nogensinde var trådt i kraft.

august 2026

tre brute force-forsvar, der aldrig havde virket

Situation. En hærdningsgennemgang af produktionsværten i august 2026 stillede et spørgsmål, der normalt får et selvsikkert svar: virker SSH-beskyttelserne mod brute force. Alle tre var konfigureret, alle tre optrådte i hver eneste rapport, nogen kiggede i, og alle tre havde været uvirksomme siden den dag, værten blev bygget.

Opgave. Kontrollerne skulle efterprøves mod det, kernen rent faktisk gør ved en pakke, og ikke mod de konfigurationsfiler, der beskriver, hvad der burde ske med den.

Handling. At læse konfigurationen ville have bekræftet det forkerte svar tre gange, så gennemgangen læste det kørende system i stedet. Jailen, der skulle blokere indtrængningsforsøg, holdt øje med port 22, mens dæmonen var flyttet til 1986 under den indledende hærdning — hver blokering, den skrev, gjaldt en port, som intet lyttede på. Firewallens hastighedsbegrænsning var værre på en mere subtil måde: reglen fandtes, og den lå under en bredere regel, der matchede først. Firewallens brugerregler evalueres oppefra og ned, og det første match vinder, så en bred tilladelse over en hastighedsbegrænsning gør begrænsningen til død kode, der stadig står i hver statusoversigt. Den tredje var den mest tavse af dem: blokeringshandlingen kalder et eksternt pakkefilterprogram, som pakkesystemet kun anbefaler og ikke kræver, så på en vært uden programmet starter jailen, tæller og beslutter og fejler så i netop det øjeblik, hvor den forsøger at blokere. Alle tre rettelser var små. Det, der kom ud

af det, var ikke rettelsen, men to regler, der nu gælder for repositoryet: en sikkerhedskontrol får en assertion og ikke en kommentar, og en firewall verificeres på reglernes placering og ikke på, om de findes.

Resultat. Tre beskyttelser, der aldrig én eneste gang havde grebet ind, gør det nu, og den fejlklasse, de tilhører — en kontrol, hvis fejltilstand er, at den bliver ved med at melde, at alt er i orden — er den klasse, som platformens tjek nu er bygget til at fange. Alle tre havde været uvirksomme lige fra bootstrap. Alle tre så sunde ud alle de steder, nogen kiggede, hvilket er hele grunden til, at de overlevede så længe.

Brug erfaringen i jeres projekt

Brug »Tre låse på døren, ingen af dem låst« som udgangspunkt for en lignende udfordring i jeres organisation. Ydelserne bag arbejdet kan også bruges i jeres projekt. Overvågning og alarmer, der siger til, mens fejlen stadig er lille, og tallene, der viser, hvor tit den bliver ved med at være det.

Se vores ydelser Kontakt os →

Se bag resultatet

Læs om situationen, beslutningerne og resultatet i eksemplet. Vi kan drøfte, hvad der passer til jeres vilkår, og hvad der kræver en anden tilgang. Tre låse på døren, ingen af dem låst — tre brute force-forsvar, der aldrig havde virket

Se vores ydelser Kontakt os →

Er du sikker på, at din beskyttelse mod indtrængen faktisk virker?

Tal om jeres projekt med den ingeniør, der har ansvaret for leverancen. Vi aftaler omfang, prisgrundlag og overdragelse skriftligt, før arbejdet begynder.

Rolle i opgaven: Sikkerhedsingeniør. Det trækker på Infrastruktur, Overvågning & observerbarhed, Netværk & VPN, Linux & servere, Sikkerhed og Systemadministration. Og når I alligevel er her, er vi ret dygtige til Site reliability & overvågning, Netværk & VPN-opsætning, Sikkerhed & adgangsstyring og Sikkerhed for AI-agenter.

Kontakt os Se vores ydelser

Ét stykke af **en længere fortegnelse** — og det hele ligger her på sitet.

Hver post er skrevet på samme måde: situationen, opgaven, hvad vi gjorde, og hvad der ændrede sig.

Se hele fortegnelsen

Definér den ønskede forbedring

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Er du sikker på, at din beskyttelse mod indtrængen faktisk virker?

Spørg til beslutningerne bag »Tre låse på døren, ingen af dem låst«. I taler med mennesker, der kan forklare arbejdet og vurdere jeres eget projekt.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/portfolio/three-locks-on-the-door-none-of-them-locked/