Engineer

Trois verrous sur la porte, aucun fermé

Détecté et corrigé trois protections SSH contre la force brute qui n'avaient jamais fonctionné : une prison de bannissement surveillant le port 22 alors que le démon écoutait sur 1986, une limitation de débit masquée par une règle plus large placée avant elle et une action de bannissement dont le binaire était introuvable, empêchant tout bannissement.

août 2026

trois défenses contre la force brute qui n'avaient jamais fonctionné

Situation. Un examen du durcissement de l'hôte de production en août 2026 a posé une question qui reçoit habituellement une réponse assurée : les protections contre les attaques SSH par force brute fonctionnent-elles ? Les trois étaient configurées, les trois figuraient dans tous les rapports consultés, et les trois étaient inertes depuis le jour de la création de l'hôte.

Tâche. Les contrôles devaient être vérifiés face à ce que le noyau fait réellement d'un paquet, plutôt que face aux fichiers de configuration qui décrivent ce qui devrait lui arriver.

Action. Lire la configuration aurait confirmé trois fois la mauvaise réponse ; l'examen a donc lu le système en fonctionnement. La jail de bannissement des intrusions surveillait le port 22 alors que le démon avait été déplacé sur le port 1986 lors du durcissement initial — chaque bannissement qu'elle écrivait désignait un port sur lequel rien n'écoutait. La limitation de débit du pare-feu était pire d'une manière plus subtile : la règle existait, mais se trouvait sous une règle plus large qui correspondait en premier. Les règles utilisateur du pare-feu sont évaluées de haut en bas et la première correspondance l'emporte ; une autorisation large placée au-dessus d'une limitation transforme donc cette dernière en code mort qui continue de figurer dans tous les états. La troisième défaillance était la plus discrète : l'action de bannissement appelle un binaire de filtrage des paquets que le gestionnaire de paquets recommande seulement au lieu de l'exiger ; sur un hôte qui en est dépourvu, la jail démarre, compte et

décide, puis échoue au seul moment où elle tente de bannir. Les trois corrections étaient petites. Le principal apport n'était pas la correction, mais deux règles qui gouvernent désormais le dépôt : un contrôle de sécurité reçoit une assertion plutôt qu'un commentaire, et un pare-feu se vérifie par la position des règles plutôt que par leur présence.

Résultat. Trois protections qui ne s'étaient jamais déclenchées fonctionnent désormais, et leur catégorie de défaut — un contrôle dont le mode de défaillance consiste à continuer de se déclarer sain — est celle que les vérifications de la plateforme cherchent maintenant à détecter. Les trois étaient inertes depuis l'amorçage. Les trois affichaient un état sain partout où l'on regardait, ce qui explique précisément leur longévité.

Mettez cette expérience au service de votre projet

Prenez « Trois verrous sur la porte, aucun fermé » comme point de départ pour un défi similaire dans votre organisation. Les prestations mobilisées pour cette réalisation sont disponibles pour votre projet. Une supervision et des alertes qui signalent les incidents tant qu'ils restent mineurs, avec les chiffres qui montrent à quelle fréquence ils le restent.

Découvrir nos prestations Contactez-nous →

Examinez ce qui a conduit au résultat

Découvrez la situation, les décisions et le résultat de cet exemple. Nous pouvons discuter des éléments transposables à vos contraintes et de ceux qui nécessitent une autre démarche.
Trois verrous sur la porte, aucun fermé — trois défenses contre la force brute qui n'avaient jamais fonctionné

Découvrir nos prestations Contactez-nous →

Votre protection contre les intrusions protège-t-elle vraiment ?

Discutez de votre projet avec l'ingénieure responsable de sa réalisation. Nous convenons par écrit du périmètre, de la base tarifaire et de la transmission avant le début des travaux.

Rôle exercé dans ce contexte : Ingénieure sécurité. Cette réalisation fait appel à Infrastructure, Supervision et observabilité, Réseaux et VPN, Linux et serveurs, Sécurité et Administration système. Et puisque vous êtes ici, nous sommes aussi plutôt doués en Fiabilité des services et supervision, Réseaux et configuration de VPN, Sécurité et gestion des accès et Sécurité des agents d'IA.

Contactez-nous Découvrir nos prestations

Un élément **d'un parcours plus long** — entièrement présenté sur ce site.

Chaque entrée suit la même structure : la situation, la tâche, ce que nous avons fait et ce qui a changé.

Voir l'ensemble du parcours

Définissez l'amélioration nécessaire

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Votre protection contre les intrusions protège-t-elle vraiment ?

Interrogez-nous sur les décisions qui sous-tendent « Trois verrous sur la porte, aucun fermé ». Vous parlerez aux personnes capables d'expliquer le travail et d'évaluer votre propre projet.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

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

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/portfolio/three-locks-on-the-door-none-of-them-locked/