Engineer

3つあったが、どれも機能していなかった防御

一度も機能していなかったSSH総当たり攻撃対策を3件発見・修正。デーモンが1986番で待ち受けるのに22番を監視する遮断jail、上位の広いルールに隠されたレート制限、バイナリを解決できず遮断を一度も実行できなかったアクションを直した。

8月 2026

一度も機能していなかった3つの総当たり攻撃対策

状況. 2026年8月の本番堅牢化レビューで、通常は自信を持って答える「SSH総当たり攻撃対策は動くか」を問うた。3つとも設定され、見られていた全レポートに現れたが、構築当初からすべて無効だった。

課題. パケットに起こるはずのことを記す設定ではなく、カーネルが実際に行うことに対して安全策を検証する必要があった。

行動. 設定を読むだけなら3回誤答するため、実行中のシステムを読んだ。遮断jailは、初期堅牢化で1986へ移したSSHに対し22番を監視し、誰も待ち受けないポートを遮断していた。ファイアウォールの制限はさらに微妙で、上に先に一致する広い許可があった。先頭から最初の一致で決まるため、一覧には出ても制限は到達不能だった。3つ目は、必須でなく推奨依存のパケットフィルターバイナリを呼ぶアクションで、未導入ホストではjailが起動・集計・判断しても、遮断するときだけ失敗した。修正はいずれも小さかったが、重要なのは2つの規則だった。安全策にはコメントでなく検証を設け、ファイアウォールは存在でなく位置で確かめる。

結果. 一度も働いていなかった3対策が動くようになり、故障しても正常報告を続ける類の不具合を、基盤の検査が捉えるようになった。3つとも起動初日から無効なのに、見ていた場所ではすべて正常だった。それこそが長く残った理由だった。

この経験をお客様のプロジェクトに

「3つあったが、どれも機能していなかった防御」を、お客様の組織の似た課題を考える出発点にしてください。この実績を支えたサービスを、お客様のプロジェクトにも提供できます。 障害が小さいうちに知らせる監視とアラートを整え、安定した状態をどれだけ維持できているかを数値で示します。

サービスを見る お問い合わせ →

結果の背景を確かめる

この事例の状況、判断、結果をご覧ください。どの部分がお客様の制約の下でも生かせるか、どこに別の方法が必要かをご相談いただけます。 3つあったが、どれも機能していなかった防御 — 一度も機能していなかった3つの総当たり攻撃対策

サービスを見る お問い合わせ →

侵入対策は本当に機能していると確信できますか？

納品を担当するエンジニアに、プロジェクトについてご相談ください。着手前に、業務範囲、価格の算定方法、引き継ぎ内容を書面で合意します。

担当した役割：セキュリティエンジニア。 関連する分野： インフラ, 監視・オブザーバビリティ, ネットワーク・VPN, Linux・サーバー, セキュリティ および システム管理. こちらのサービスも得意としています サイト信頼性・監視, ネットワーク・VPN構築, セキュリティ・アクセス管理 および AIエージェントのセキュリティ.

お問い合わせ サービスを見る

より多くの実績の **一つです** — そのすべてをこのサイトで公開しています。

どの項目も、状況、課題、実施内容、変化という同じ構成で記載しています。

すべての実績を見る

必要な改善を定める

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

侵入対策は本当に機能していると確信できますか？

「3つあったが、どれも機能していなかった防御」の判断の背景についてお尋ねください。仕事内容を説明し、お客様のプロジェクトを検討できる担当者が対応します。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

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

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/portfolio/three-locks-on-the-door-none-of-them-locked/