Rocket software

フェイクITワーカーを見つけ出す

見逃してはいけない5つの兆候

メインフレームは世界のクレジットカード取引の90%を処理しており、現代のサイバー犯罪者にとって魅力的な標的となっています。しかし、最大の脅威の一部はすでに内部に潜んでいます。内部関係者による侵害の被害額は、平均499万米ドルにも上るのです。あなたは平然と紛れ込んでいるリスクを見抜けますか。

フェイクITワーカーを見抜く5つの方法

01 つじつまの合わないログイン

脆弱なパスワード、ログインの共有、時代遅れのセキュリティ対策が、フェイクワーカーの潜入を許しています。多要素認証（MFA）には対応しなければなりません。

専門家のアドバイス
ログインパターンを監視してください。予期せぬ場所や不自然な時間にログインがあった場合は、重大なリスクを示しています。

02 不審な給与支払いの動き

フェイクワーカーが給与計算業務に絡んでいて、不正な口座へ資金が流れている可能性があります。人事記録に幽霊社員や異常な変更がないか警戒してください。

顕著なケース
マサチューセッツ州で最近、偽の給与支払いサイトを使って州職員を騙し、個人情報を提供させるインシデントが発生しました[1]。

03 AIを利用した詐欺

AIツールを使い、検出がほぼ不可能なフィッシングメールや偽のプロフィールが作成されるようになっています。信頼できるものに見えますが、それらは人々を騙して機密情報を開示させるために作られているものです。

警戒すべき兆候
プリテキスティング詐欺：偽りの身分や状況(プリテキスト)を作りだし、従業員をだまして個人情報を開示させる状況を作り出す攻撃手法

04 内部脅威

不満を抱えた従業員や契約社員にデータを侵害される可能性があります。攻撃には意図的なものと偶発的なものがありますが、どちらにしても多大な損失がもたらされます。

顕著なケース
米国以外の某国家の利益のために、米国企業に300人のフェイクITワーカーを潜入させ、重要データにアクセスさせるというインシデントが発生しました[2]。

05 コンプライアンス問題

EU一般データ保護規則（GDPR）やデジタルオペレーショナルレジリエンス法（DORA）といった新しい規制の下、データに完璧な保護が必要になっています。1つでも問題があれば、罰金を科されるだけでなく、組織の評判に傷がつくことも避けられません。

今すぐできる対策
グリーンスクリーンへのログイン認証を、既存のID・アクセス管理（IAM）システムに統合してください。

1. “State employees fooled by fake payroll website farming their data” Boston.com, October 10, 2024.
2. “Charges and Seizures Brought in Fraud Scheme, Aimed at Denying Revenue for Workers Associated with North Korea” Justice.gov, May 16, 2024.

メインフレームの保護方法

グリーンスクリーンへのアクセスを保護する

他のオープン系システムと同様に、端末エミュレータ経由のメインフレームへのログインも保護する必要があります。TLS 1.3暗号化を使用し、すべてのログイン試行にMFAを強制してください。

ID・アクセス管理(IAM)システムを利用する

一元的なIAMシステムでアクセスを制御してください。これにより、許可されたユーザーのみが組織の機密システムにアクセスできることを保証できます。

すべてを監視する

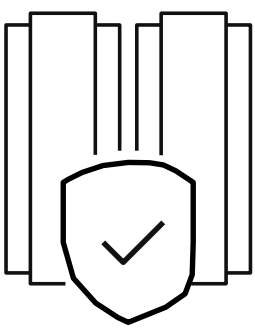
ログイン、システム活動、アプリの使用状況を追跡してください。リアルタイム監視によって不審な行動を早期に見つけ出し、侵害を防止しましょう。

活動を監査する

常に詳細なシステム操作ログを残してください。これによって脆弱性を特定できるだけでなく、侵害発生時にはログを証拠として使えるようになります。

専門家と協力する

常に脅威の先を歩き、GDPRやDORAといった規制への準拠を保証してくれるセキュリティ専門のベンダーと協力してください。



Rocket® Secure Host Access：フェイクITワーカーを防御する

重要なホストアプリケーションへの安全で、フィッシング対策が施された、パスワード不要のアクセスを提供します。既存のエンタープライズIAMを活用し、最小限の労力で、メインフレームアプリケーションへのアクセスを上位のITセキュリティ戦略に統合することができます。

Rocket Secure Host Accessの機能：

- SSO、SSH、MFAといったセキュリティのベストプラクティスの適用範囲を拡大させる
- 組織内のエンドユーザーロールに基づいて機密データを削除する
- サイバー攻撃の脅威と罰金のリスクを低減させる

侵害を防ぐ

システムのセキュリティ対策を遅らせるほど、脆弱性は増大します。ロケットソフトウェアでメインフレームの保護に取り組んでください。

詳細はこちらをご覧ください

Rocket software

MAR-12282_SecureHostAccess_Infographic_V1-2

RSIGSHA01-202603-KA