ssh
Securing the path to your information assets

導入事例

トップ 5 に数えられるグローバル銀行

Universal SSH Key Manager でコンプライアンスを回復し、リスクを削減。

2兆5千億ドル以上の資産を持つ世界でも最大規模の銀行が、外部監査の際にセキュリティ及びコンプライアンスの問題で警告を受けました。当行では毎日、数千のミッション・クリティカルなトランザクションを行うために OpenSSH を使用していましたが、Secure Shell 環境のセキュリティを確保するためにアプリケーション間及び特権ユーザーの ID 及びアクセス・コントロールを管理する必要がありました。

背景

Secure Shell (SSH)は、インフラレベルのセキュリティ プロトコルであり、企業で広範に利用されていますが、充分に理解されていません。SSHは、企業活動の継続に不可欠な IT機能として使用されています。これら機能には、自動ファイル転送、バックアップ、ディザスターリカバリー、システム管理も含まれています。SSHは、RADIUS、AD 及びその他中央集約されたAAAサーバーでは完全には制御統合できない公開鍵ベースの認証方式を使用しています。

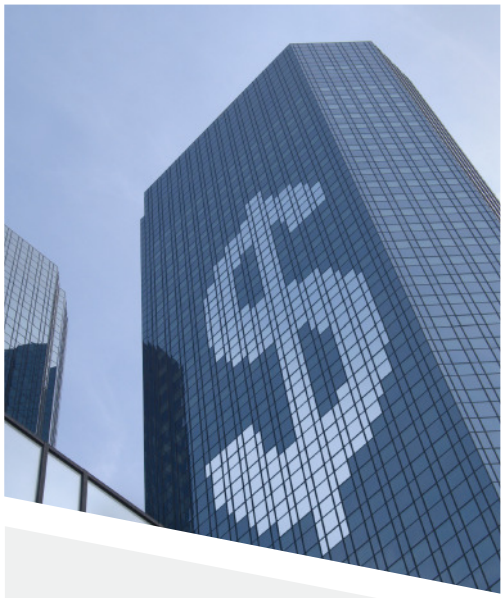
問題

トップ5に数えられるグローバルなこの銀行*では、セキュリティ監査により、SSH のユーザー鍵に関するガバナンスの欠如によるリスクやコンプライアンスの問題に対し対処するようにとの問題提起がなされました。なぜならこれらの鍵は、システムへのアクセスを許可し銀行の業務に関わる重要な機能を利用可能にするものだからです。監査では経営陣に対し、この管理されていない認証システムは法規制（MAS及びSOX）に違反するだけでなく、組織自体を脅威にさらすことになると忠告しました。

主要なサーバー・インフラにルート・アクセスを許可する鍵の内の一つでも悪用されると、銀行の情報の漏洩、改ざん及び損失が可能となり、バックアップされたデータさえ失う危険があります。運用スタッフは、SSH インフラが法規制に適応するよう、解決策を探すように命じられました。

> 「検出フェーズの際に、問題の範囲と程度が明らかになりました。長期に渡る運用で、SSH の鍵数は、処理不可能なまでのレベルに達しており、各鍵が何を実行しているかという可視性も無くなっていました。SSH 使用の85パーセント以上が重要なアプリケーション間のデータ転送であるため、まず第一歩として行ったことは、鍵間の信用関係を明らかにすることでした。その後新しい鍵を再発行・展開しましたが、この際システムの停止を行わずに実施することができました。」
>
> – ジョー・スカッフ、SSH テクニカル サービス ディレクター談

銀行及び金融サービス



概要:

環境の規模及び種類:
OpenSSH を利用した10,000台を超えるホスト

ユーザー数:
20,000人以上

アプリケーション数:
500以上

鍵の数:
150万

要対応コンプライアンス:
SOX、 MAS規制

ソリューションの選択

同行は、SSH の鍵管理製品を単に提供する企業ではなく、SSH 環境全体を改善する方法や設計構築をアドバイスできるパートナーを必要としていました。同行は、SSH の長年の利用にわたり拡大していた問題を処理できる充分な SSH の専門知識や技術を行内で持ち合わせていないことに気づいていたのです。複数のベンダーと接触した後に、同行は SSH コミュニケーションズ・セキュリティ社を選択しました。

> 「SSH コミュニケーションズ・セキュリティ社が最初に行ったことの一つは、問題の範囲を示すことでした。SSH 鍵の検出ツールは、監査官が提起した内容よりも問題がより一層広範囲にわたり、重大な状況であることを示しました。同社の技術チームは、弊行環境内に150万以上のユーザー鍵が展開されており、そのユーザー鍵の内15万個がルート・アクセスを許可されているが、これに対応する秘密鍵の保持者が誰であるかに関する記録が一切ないという状態を明らかにしました。」
>
> 「テスト環境と実稼働環境を確実に分離するという我々の重要なセキュリティポリシーの一部が、SSH を経由することで簡単に破れるということもわかりました。SSH コミュニケーションズ・セキュリティ社の Universal SSH Key Manager 製品と同社のプロフェッショナル・サービスはどのようにこれらを制御できる状態に回復できるかを示してくれました。他のベンダーはこれを実施する製品あるいは専門的技術を持っていませんでした。」
>
> – 同行のプロダクト マネージャー談

参考文献

- 「SSH ユーザー鍵の是正措置：企業のセキュリティに潜む重大な脅威のうちの一つを管理・制御」
- 「PCI-DSSのコンプライアンスを実施する環境でのSSH のユーザー鍵とアクセス制御」
- 「公開鍵認証の技術的な複雑さ及びリスク」

明確で高度に構成されたアプローチ

鍵の検出は第一歩にすぎません。鍵使用を理解することは、どの鍵が自動化プロセスに必須であるかを識別することでもあり、是正措置もしくは運用の改善を行えるようになる前に必要となる次のステップなのです。Universal SSH Key Manager 製品は鍵がどのように運用されているかを確認するためのモニター機能も提供します。不必要な鍵を削除し、利用されている鍵を管理下に置き制御します。また、鍵の使用、鍵のライフタイム、鍵作成における権限のポリシー・コントロールを確実に実施するために、中央からの管理機能を提供します。さらに、ポリシー違反をセキュリティ管理者に警告として通知します。同行は、本ソリューションを2012年11月に購入し、SSH のインフラストラクチャをコントロールするプロジェクトをさらに進めています。

> 同行のプロジェクト・マネジャーは「SSH コミュニケーションズ・セキュリティ社は真のパートナーです。彼らの専門技術と詳細にまで渡る配慮は、我々がこの大きなリスク及びコンプライアンスの問題に立ち向かうために不可欠なものです。」と述べています。

＊ 同行の依頼により行名は匿名となっておりますが、内容は事実に基づいています。

販売代理店

株式会社 ディアイティ
http://www.dit.co.jp

〒135-0016 東京都江東区東陽 3-23-21 プレミア東陽町ビル
Tel. 03-5634-7651 Fax. 03-3699-7048