コンプライアンス・ホワイトペーパー

Secure Shell に対する新しい NIST のガイドラインについて CISO が知っておくべきこと

ssh®

目次

SSH Communications Security 社について:

1995年に設立されたSSHコミュニケーション・セキュリティ社は、データ転送のセキュリティ・ソリューションとしての標準プロトコルであるSSHプロトコルを発明・開発した企業です。フォーチュン10に数えられる企業の内の7社を含む世界中の3,000社以上の顧客が、SSH 社の情報保証プラットフォームを採用しています。SSH 社のプラットフォームは、あらゆる業種や規模のビジネスの外部及び内部環境でのデータをデータ損失から保護し、境界セキュリティを強化します。また、同社の二要素認証システムや内部セキュリティ制御管理ソリューションを併せて利用することで、ユーザー鍵の管理やネットワークにおける管理者の通信の監視も含め、より簡単に通信データの保護を強化することができます。

はじめに

米国国立標準技術研究所 (NIST)は米国の革新性と産業における競争力に責務をもつ米国の政府機関です。NIST が対応する1つの領域はサイバーセキュリティ標準の確立及び米国の連邦政府機関のためのガイドラインの確立です。この責務は 2002 年の連邦情報セキュリティマネジメント法 (FISMA) によりその権限を委任されたものです。これらの標準の根本理念が NIST Special Publication 800-53 となります。NIST 800-53 は、管理、機密性、完全性を保護するための運用上、技術上の保護手段及び情報システム、電子情報の可用性について明確に規定しています。要するに、2002 年の FISMA 条例の要求に従い、連邦機関が実装しなくてはいけない IT セキュリティ管理について記述するものです。

2014 年 8 月 20 日に、NIST の CSD Computer Security Division が Interagency Report 7966 (NISTIR 7966) を発表しました。この報告書は、Secure Shell(SSH) を使用した自動化されたアクセスの管理のためのセキュリティ ・ ガイドラインを提供するものです。この報告書では、これらのガイドラインが、NIST800-53 で義務付けられたセキュリティコントロールや大統領が発行したサイバーセキュリティフレームワークにいかに対応しているかを説明しています。

NIST のこれらの新しい展開は、IT セキュリティの責任者である CISO やその他の経営陣に対して大きな意義があります。本ホワイトペーパーでは、なぜ NIST がこれらのステップを取ったか、またそれが連邦政府機関内だけでなく、その他企業の IT セキュリティ管理において何を意味するかを説明します。

なぜ NIST が Secure Shell に焦点を当てるのか

Secure Shell とは、データ転送、アプリケーション・トンネリング、リモート・システム管理を安全に行うための一連のプロトコル及びソフトウェアです。Secure Shell は Unix、Linux、IBM メインフレームでは予めインストールされており、Windows でも利用可能です。Secure Shell は数百万台のサーバーに展開されており、データセンター環境の約 90 パーセントで利用されています。システム管理者やアプリケーション開発者といった特権ユーザーはインタラクティブなアクセスに Secure Shell を使用します。それ以上に Secure Shell はバックアップ、データーベースの更新、システムの死活監視を行うアプリケーション、自動化されたシステムの管理を含むシステム・プロセスを自動化するためのシステムに幅広く利用されています。要するに、Secure Shell は現在の高度に自動化されたデータセンターで極めて重要な役割を背負っているということです。

しかし、Secure Shell は「土管、配管の一部」というような印象を与え、運用上のリスクとしての注意を得ることは滅多にありません。NIST の言葉を借りれば、「SSH を使用した自動アクセスのセキュリティは今までほとんど無視されてきた」ということになります。この盲点は、多くの価値の高いあるいは大きな損害をもたらすようなデータに対する侵害の一因となっています。結果として、NIST の CSD は、IT環境内での貧弱な Secure Shell アクセス・コントロールは、運用上の大きなリスクとなると結論を下しました。これに対応するため、NIST は連邦政府機関及びその他企業が採用すべき包括的なガイドラインとコントロールを発表しました。

Secure Shell の ID の管理が不十分な場合の隠れたリスク

Secure Shell は主に、リモート・サーバーのアプリケーションやサービス・アカウントにログインする際に使用されます。Secure Shell はパスワード、トークン、デジタル証明書、公開鍵等の認証方法をサポートします。公開鍵認証では、ID 鍵となる小容量のファイルから成る秘密鍵がクライアント側（多くの場合サーバーマシーン）に保存され、承認済みの公開鍵がサーバー側に置かれます。秘密鍵ファイルはパスフレーズを使用して暗号化することもできます。但し、自動化システムで使用する秘密鍵には通常パスフレーズは使用されません。これはプロセスを自動実行するにはパスフレーズ自身をファイルに保存するか、スクリプトに直接記述する必要性が発生するためです。

公開/秘密鍵による認証は本質的には、パスワード等の他の認証方式より安全な方式です。これが公開鍵の使用を NIST が勧める理由であり、プロセス・オートメーション環境では特にこの使用を支持しています。また実際に、鍵ベースの認証は政府及び企業双方共に非常に広範囲に使用されています。ただし、残念なことにマイナス面もあります。管理が不適切な場合、攻撃者が Secure Shell の鍵を使用して IT インフラストラクチャを貫通することができるのです。たった 1 個の秘密鍵を侵害するだけで、これを利用して特権アクセス管理ソリューションをバイパスし、また大規模攻撃を行い、データ侵害を実行するための発見しづらいバックドアを作ることができます。

NIST は企業・組織がしばしば露呈する弱点及びセキュリティ査定で評価すべき点として以下の項目を特定しています。

- 脆弱性のある SSH の実装（安全ではないバージョン、設定における弱点）。
- 盗難、漏洩、失効させていない SSH ユーザー鍵（鍵のライフサイクル管理の可視性とプロセス管理の不足）。
- バックドア（未承認のユーザー鍵）。
- ユーザー鍵の意図していない方法での利用（責務の分離の不十分、未承認の特権エスカレーション）。
- 正しくない場所へのユーザー鍵の保管（鍵ファイルへのアクセス・コントロールの欠如、不足）。

これらの脆弱性は表 1 に表示されるリスクを生みます。

何年も前に解約した業者や退職した従業員のアクセス権が重要なシステムにまだ残っている場合。これは企業がデータを損失する、または他の悪意ある行為を受ける原因となります。
システム、アプリケーション、ユーザーアカウントに不必要な鍵が承認された状態のまま残っている場合。各公開鍵ベースの認証は、対応する秘密鍵が侵害された場合に、システムの乗っ取りや情報漏洩の問題を誘発します。
承認されていない秘密鍵のコピーが利用もしくは循環、流通している場合。一般に、秘密鍵の所持者はたとえこれが会社のポリシー違反であったとしてもコピーすることができてしまいます。中央での監視及びコントロールを行うことで、承認されていない鍵の使用の可能性を減少、もしくは無くすことができます。
パスフレーズで保護されていない秘密鍵がある場合。秘密鍵の保護に対するポリシーの施行が不十分な場合、クレデンシャルが悪用されるリスクが増大します。
鍵が規則正しく更新さていない、または全く更新されていない場合。ほとんどの組織がエンド・ユーザーに規則正しくパスワードを変更するように要求しているのと同様、鍵の更新はクレデンシャル保護の為の基本的な要求です。
意図していないアクセスのエスカレーションがなされている場合。Secure Shell の構成管理はユーザーが特権をエスカレートさせ、他のアカウントにアクセス権を付与することを防ぐために必要です。
責務の分離が行われていない場合。金融業界でよく見られる問題です。これは開発から運用サーバーへシステムを拡張する際に、鍵の権限のコントロールが不十分なことによってしばしば引き起こされます。
テスト及び本番環境間に意図しないアクセスが許可されている場合。
信頼関係の可視性が不足している場合。
監査要求を満たすことができない場合。これはすべての信頼関係や操作ログのレポートといった基本的な事項にまで及びます。
手作業での鍵の設定及び除去プロセスの際の人為的過失がある場合。これは承認されていないアクセスに権限を与えたり、必要な権限の削除を行わなかったりすることによる問題の原因となります。
Secure Shell ソフトウェアの設定ミスがある場合。ネットワークの内側もしくは外側からの VPN アクセスに関する禁止事項のポリシー違反をユーザーに許可することとなります。
永続的な信頼関係を作成することができる管理者の人数が多い場合。アクセス・コントロールの破綻の原因となります。

表 **1:** 露呈する主なリスク

ベストプラクティス

これらのリスクの深刻さを認識し、NIST IR 7966 は Secure Shell の ID（公開鍵、秘密鍵）を管理するための一連の推薦ベスト・プラクティスを提供します。これらのベスト・プラクティスは、NIST800-53 で義務付けられたセキュリティコントロールや大統領が発行したサイバーセキュリティフレームワークに対応しています。ベスト・プラクティスの要約は、以下の通りです。

1. 鍵の構成を環境全体にわたり標準化する。
2. 承認済みの鍵ファイルにはエンド・ユーザーに書き込みアクセス権を許可しない。
3. 中央での鍵のプロビジョニング（個人に「セルフサービスでのプロビジョニング」を許さない）。鍵のプロビジョニングは中央で行い、これによりルート・レベルの管理者を少ない人数に制限する。
4. 暗号の設定ー強力な暗号と指定した鍵長のみ許可する。
5. 秘密鍵にはパスワード保護を要求する。
6. Secure Shell の操作に関するログを要求する
7. 承認済みの鍵ファイル及びホーム・ディレクトリがセキュアでない場合、Secure Shell サーバーが動作しないようにする。
8. プロセスのスポウニングによる特権エスカレーションを防ぐ。
9. システムアカウントと人のアカウントを分離する。
10. 特定のコマンド及びソース・アドレスに対し制限を行うように Secure Shell のアクセスを制限するための手段を使用する。
11. 鍵を更新する。
12. 不必要なユーザー鍵を削除する。
13. 鍵の使用を文書化する。
14. 定期的な監査の実施。

CISO への宿題

NIST の CDS からの推奨は、米国の連邦政府内の CISO への直接の呼びかけです。これはまた企業の CISO のための行動への直接の呼びかけでもあります。連邦政府と取引していない企業であっても、NIST 800-53 とその関連する政府機関のレポートは広く受け入れられている業界標準のベスト・プラクティスです。

朗報としては、これらの問題に取り組むためのの第一歩は難しくなく、また費用もかからないということです。第一歩はシンプルで、どの範囲で組織がリスクにさらされているかを NIST が示したリスクと照らし合わせこれを見つけ出すことです。適切なツールをもつ熟練した社員ならば、数日間でこれをなし遂げることができます。もしこれらのリソースが内部にない場合でも、素早くそして効率的に内部スタッフと協力してこのジョブを完了することができる認定された第三者機関も存在します。いずれにしても、CISO はスタッフに以下を要求するべきでしょう。

1. 推薦された NIST 800-53 のコントロールに対しての現状の評価及びベンチマーク
2. リスクの評価
3. 一連の推薦事項

上記内容を基本要件として、担当者は重要なコンプライアンスとリスクを扱うための行動要綱を構築することができます。

SSH コミュニケーションズ・セキュリティ社は NIST が提起した問題を企業・組織が扱う助けとなるトレーニング、サービス、製品を提供します。貴社スタッフとの共同作業を行うことで、現在の環境の包括的な評価を提供し、是正の為の効果的なアプローチを推薦します。

参考文献

>> NISTIR 7966

>> NIST 800-53

ssh®

www.ssh.com /lang/jpn