ssh®
Securing the path to your information assets

データシート

SSH Risk Assessor™

Secure Shell 環境におけるリスクとコンプライアンスに関する問題に対処

世界の大多数の大企業及び政府機関は、ビジネスに重要な IT 機能の機密性及び完全性の確保に Secure Shell (SSH) を利用しています。SSH は自動化されたアプリケーション間のプロセスにセキュリティを提供します。さらに IT スタッフは日々のオペレーティング・システム及びアプリケーションの管理にも SSH を使用しています。しかし、SSH はプロトコルであり、それ自体がセキュリティ・ソリューションなわけではありません。SSH の管理が不十分な状態で環境内に展開されている場合は、データー漏洩、サービス提供の妨害、コンプライアンスへの義務違反に直面することになります。

SSH の通信では、公開秘密鍵を使用してアプリケーション間のプロセスの自動化やインタラクティブなユーザー・アクセスが認証されます。しかし、これらの鍵を適切に管理している企業はまれです。不十分な鍵の管理は、企業を様々な ID 及びアクセス管理の問題にさらすことになります。これらの問題は、説明責任の不足、可視化（見える化）の不足、誰が何時どのリソースにアクセスしているかに関するコントロールの不足、に集約することができます。

第一ステップ－可視化

内部及び外部のセキュリティ監査官はこれらの問題を認識していますが、該当する IT インフラにおいて、問題の範囲及びその重大さを決定する為の現実的で、かつ既存のシステムに影響を与えずにこれを解決する手段を持っていません。結果として、問題の対処に高い優先度を与えるか、または対応時期を延ばすことが可能かに関し、事実を基にした提言を行う技術的手段が不足した状態におかれています。

SSH コミュニケーションズ・セキュリティ社の SSH Risk Assessor (SRA) は SSH における ID及びアクセス管理のコンプライアンス及びリスクレベルに対する十分な情報をセキュリティ監査官に提供することを可能にするコンパクトなレポートツールです。

SRA は SSH のユーザー及びホスト鍵をスキャンします

SRA によるリスクレポートの内容

- SSH のユーザー及びホスト鍵をスキャン
- 以下の項目を示したレポートを作成：
  - 鍵及びその鍵に関連するユーザー
  - ホスト OS 及び SSH のバージョン
  - 既知及び未知の信頼関係
  - ルート権限の数
  - コマンド制限のないユーザー鍵
  - ソース・アドレスあるいはホスト名の制限のないユーザー鍵情報
  - 複製あるいは共有されている秘密鍵の情報
  - パスフレーズで保護されていない秘密鍵
  - 鍵年齢、鍵アルゴリズム、鍵長
  - 非ルート所有のディレクトリーにある鍵及び非ルート権限で書き込みが可能な鍵の情報
  - 到達範囲の分析。漏洩した秘密鍵によって到達できる可能性がある範囲を表示
- 比較検出
  - 認識されていない又は権限がない鍵を識別するために現行の IAM を追跡調査
  - SSH バージョン及びアクセス・ポリシー
  - 鍵の暗号化ポリシー
  - 鍵の更新

SRA により以下のコンプライアンスに対応するレポートを作成

- SOX DS 5.8セキュアな鍵の保管及び失効に関する暗号鍵の管理
- 鍵の保護、強度、年齢、アクセス及び監査に関するHIPAAの情報アクセスに関する要件
- 鍵の割り当て、配布、追跡、 鍵のアルゴリズムの強制及び追跡に対する構成また記録手順に関する NIST/FISMA の C.2.2 章の要求。
- NERC CIP-007-4 R5 のアカウント管理の用件
- PCI section 8.5.x 章のアクセス制御（PCI バージョン3では SSH に対しても検討中）

適用範囲および仕様

スキャン対象のプラットフォーム	• HP-UX 11iv1, 11iv2, 11iv3 • IBM AIX 5.3, 6.1, 7.1 • Oracle Solaris 8, 9, 10, 11 • Oracle Enterprise Linux 5.4, 5.5, 5.6, 5.7 • Red Hat Enterprise Linux 4, 5, 6 • SUSE Linux Enterprise Server 9, 10, 11
サポート対象の SSH のバージョン	• Tectia 6.0 もしくはそれ以降のバージョン • OpenSSH もしくはそれ以降のバージョン
システム依存性	• 全てのスキャン対象システムにPerl 5.6もしくはそれ以降のバージョンのインストールが必要です
サポート対象プラットフォーム及び解析ツールとの依存関係	• Red Hat Enterprise Linux 6 もしくは SUSE Linux Enterprise Server 11 • Python 2.6 もしくはそれ以降及び Perl 5.8 もしくはそれ以降及び OpenSSH ssh-keygen がインストールされていること

次のステップ

SRA はセキュリティ担当者や社外監査官が環境内の IT セキュリティやコンプライアンスの問題を発見し対処する際に使用するために開発されました。SRA は無償で提供されるツールです。SRA の詳細情報及び入手方法に関しては **www.ssh.com/sra** をご参照下さい。

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