ユーザ事例

大手金融サービス企業の外部委託先に対する可視性とコントロール

世界の上位50行の銀行のうち45行に対して、国際的な金融サービスを提供する本企業は、重要な IT インフラのセキュリティ及びコンプライアンスの監査の問題に直面していました。監査官は特権アクセスの監視、管理に関する厳格な要件を提示し、同社のデーターセンターで作業する外部委託企業を確実に監視、管理する必要性があることを認識しました。

ネットワークの途中経路に配置して透過的に特権アクセスを管理、コンプライアンスに対応、そして顧客データを保護するために SSH コミュニケーションズ・セキュリティ社の CryptoAuditor® が選択されました。

機密情報を扱うシステムへのアクセスは、通常暗号化ツールで保護されています。これらツールは中間者攻撃、スニファー攻撃等の一般的な攻撃ベクトルに対するセキュリティを提供します。一方で、暗号化ツールをシステムへの不正アクセスやデータを盗み出すために悪用することもできます。攻撃者が悪意ある内部人員や契約業者であることもよくあることです。

特権ユーザのセキュリティーツール（SSH、SFTP、HTTPS、RDP）は ICT インフラのへのアクセス、管理、サポートに使用されます。暗号で保護された機密データには、多層防御や監査ツール（SIEM、IDS、DLP システム）も役に立ちません。

解決すべき課題

特権アクセスは日々進化しています。企業環境が拡大するため、従来の境界が徐々に浸食され、多くの企業が監視のための新たな困難に直面しています。暗号通信を利用して重要なシステムにアクセスするリモート管理者や外部委託企業をどのように監視、管理、監査したらよいのでしょうか。

この金融サービス企業にとって、機密データへのアクセス管理はビジネス上のセキュリティにとって重要なだけでなく、国内また国際的な法令規制においても要求されている重要事項です。毎日数十億ドルに及ぶ数十万回の取引で、非常に大規模な、大量の暗号化通信が行われています。

多くの内部及び外部のシステム管理者が昇格した特権を利用して、SSH や RDP の暗号プロトコルで共有のシステムアカウント（例えば Windows administratorや Unix root アカウント）にアクセスし、サーバーの管理をおこなっています。

法令、セキュリティ双方の仕様が、これら特権アクセスへの可視性及びコントロールを要求しています。監査の仕様は使用する特権アカウントと個々のユーザ間の信頼のおける対比付けも要求しています。更に、企業のセキュリティ・ポリシーを強制し、高い価値のある資産へのアクセス監視の実施も必要です。

ソリューションに対する要求のまとめ：

- 今後のフォレンジックに備えた特権ユーザのRDP や SSHのセッションの完全な記録
- 特権ユーザ認証のための Active Directory との統合
- （共有）特権アカウントを特定の人間であるユーザに振り当てるマッピング機能
- RDP や SSHセッションのきめ細かい制御及び監査
- クリップボードやドライブのリダイレクトチャネルの制御、SSH トンネルと SFTP ファイル転送での制御
- 特権による通信に関する定期的なレポート
- エンドユーザーのツールやワークフローに影響を与えない簡単でゼロインパクトでの設置展開
- ビジネス継続性を維持する高可用性及びパススルーでのフェイルオーバー

ソリューション

同社は以下の理由で CryptoAuditor を選択しました。

- 広範な監査機能、プロトコルレベルでの制御機能、エンドユーザーに影響を与えないシンプルなゼロインパクトでの設置展開
- CryptoAuditor は共有アカウント管理を行うソリューションを提供し、この際複雑なパスワード保管システムの設置を必要としない
- ゲートウェイまたはエージェント・ベースのソリューションでは展開に何週間もかかるが、CryptoAuditor のインストール及び展開は数日間で完了

同社は、CryptoAuditor の Vault 及びHound を個別に展開する方法を選択し、1+1の高可用性構成のブリッジモードで Hound を実装しました。Hound は Active Directory と接続され、Vault コンポーネントは別の管理ネットワークに展開されています。

メリット

CryptoAuditor には以下のようなメリットがあります。

- 広範なセッションの記録、保管、検索及びセッションの再生機能
- Active Directory 及び企業のアクセス権限データベースとの簡単な統合
- 特権アカウントに対する共有アカウントのマッピング機能
- 専用ゲートウェイまたはジャンプ・ホストへログインするユーザのみではなく、SSH、SFTP、SSL、RDP を利用した特権 ID の通信を監視する機能
- AV、IP、DLP及び他のレイヤーのセキュリティ・ソリューションへの拡張性
- 最も一般的な業界屈指のファイアウォールソリューションとの統合及び互換性
- ポートフォワーディング等のファイアウォールを迂回する策やバックドアの脅威を削減することでのセキュリティレベルの向上

CryptoAuditorを利用することで、同社は法規制に準拠し、社内外からの脅威から自身を保護し、重要なシステムやデータの誤用を防止する能力を手に入れまた。