ネットワーク セキュリティ ポリシー： ベスト プラクティスのホワイト ペーパー

目次

概要

セキュリティ ポリシーがない場合、ネットワークのアベイラビリティが損なわれる可能性があります。 ポリシーは、ネットワークへのリスク評価、および応答するためのチームの構築から開始します。 ポリシーを続行するには、セキュリティの変更管理プラクティスを実施し、セキュリティ違反についてネットワークを監視する必要があります。 最後に、レビュー プロセスが、学習したレッスンに合わせて既存のポリシーを変更します。

このマニュアルは、 準備、防止、および対応の 3 つのセクションに分かれています。 これらのステップについて詳細に説明します。

準備

セキュリティ ポリシーを導入する前に、次を実行する必要があります。

- 利用ポリシー ステートメントの作成
- リスク分析の実施
- セキュリティチーム構造の確立

利用ポリシーステートメントを作成する方法

シスコは、セキュリティに関するユーザの役割と責任の概要を示す利用ポリシー ステートメントを作成することを推奨します。 開始時点では、企業内のすべてのネットワーク システムとデータ

を包含する一般的なポリシーを使用できます。 この文書によって、セキュリティ実施方法を改善するためのセキュリティ ポリシー、目的、ガイドライン、および各自のセキュリティ上の責任が一般のユーザ コミュニティで理解される必要があります。 会社で従業員に対して処罰や懲戒処分が発生する可能性のある行動が規定されている場合は、これらの行動およびそれを回避するための方法をこの文書に明記する必要があります。

次の手順は、パートナーのアクセプタブル ユース文書を作成し、パートナーが入手可能な情報、それらの情報の取り扱いについて自社の従業員の行動と同様に理解してもらうことです。 セキュリティ攻撃として識別されるすべての特定の行為およびセキュリティ攻撃が検知された場合に実施される処罰行為について明確に説明する必要があります。

最後に、管理者のアクセプタブル ユース文書を作成し、ユーザ アカウントの管理、ポリシーの適用、および権限の確認の各手順について説明します。 会社で、ユーザ パスワードまたはそれ以降のデータの取り扱いに関する特定のポリシーが規定されている場合は、それらのポリシーも明確に組み入れます。 パートナーのアクセプタブル ユース ポリシー文書およびユーザのアクセプタブル ユース ポリシー文書のポリシーを確認し、画一性を確保してください。 アクセプタブル ユース ポリシーにリストされている管理者の要件がトレーニングの計画とパフォーマンス評価に反映されていることを確認します。

リスク分析を行う

リスク分析では、ネットワーク、ネットワーク リソース、およびデータに対するリスクを識別する必要があります。 これは、リスクの可能性のあるすべてのエントリ ポイントおよび攻撃の可能性のあるすべての方法を識別する必要があることを意味するわけではありません。 リスク分析の目的は、ネットワークの各部分を識別し、脅威レーティングを各部分に割り当て、適切なセキュリティ レベルを適用することです。 これは、セキュリティと必要なネットワーク アクセスの間の実行可能なバランスの維持に役立ちます。

各ネットワーク リソースに、次の 3 つのリスク レベルのうちの 1 つを割り当てます。

- **低リスク** システムやデータが危険にさらされている（不正な個人によるデータ表示、データの破損、またはデータの消失）場合に、ビジネスを中断しない、または法的あるいは財務上の問題が発生しません。 ターゲット システムまたはデータは簡単に復元することができ、その後の他のシステムからのアクセスを許可しません。
- **中程度のリスク** システムやデータが危険にさらされている（不正な個人によるデータ表示、データの破損、またはデータの消失）場合に、ビジネスである程度の中断、小規模の法的あるいは財務上の問題が発生し、そうならない場合はその他のシステムへのアクセスが提供されます。 ターゲットのシステムやデータを復元するためにある程度の労力を必要とし、復元プロセスによってシステムが中断されます。
- **高リスク** システムやデータが危険にさらされている（不正な個人によるデータ表示、データの破損、またはデータの消失）場合に、ビジネスで最大規模の中断が発生し、大きな法的あるいは財務上の問題を引き起こし、または個人の健康および安全を脅します。 ターゲットのシステムやデータを復元するために大量の努力を必要とし、復元プロセスによってビジネスまたは他のシステムが中断されます。

リスク レベルを割り当てる対象になるものには、 コア ネットワーク デバイス、配信ネットワーク デバイス、アクセス ネットワーク デバイス、ネットワーク モニタリング デバイス（SNMP のモニタおよび RMON プローブ）、ネットワーク セキュリティ デバイス（RADIUS および TACACS）、電子メール システム、ネットワーク ファイル サーバ、ネットワーク プリント サーバ、ネットワーク アプリケーション サーバ（DNS および DHCP）、データ アプリケーション サーバ（Oracle などのスタンドアロン アプリケーション）、デスクトップ コンピュータ、およびその他のデバイス（スタンドアロン プリント サーバおよびネットワークのファックス機器）が

あります。

スイッチ、ルータ、DNS サーバ、および DHCP サーバなどのネットワーク機器は、その機器を越えてネットワーク内へアクセスすることを許可できます。このため、中程度または高度なリスクのデバイスです。 また、この機器の破損がネットワーク自体の破綻の原因になる可能性があります。 このような障害はビジネスに最大規模の中断をもたらします。

リスク レベルを割り当てた後は、そのシステムのユーザ タイプを特定する必要があります。 最も一般的なのユーザ タイプは、次の 5 種類です。

- **管理者** ネットワーク リソースを担当する内部ユーザ。
- **特権** 広範囲のアクセス権が必要な内部ユーザ。
- **ユーザ** 一般的なアクセス権を持つ内部ユーザ。
- **パートナー** 一部のリソースへのアクセス権が必要な外部ユーザ。
- **その他** 外部ユーザまたはカスタマー。

次のセキュリティ マトリクスは、各ネットワーク システムに必要なリスク レベルとアクセスのタイプの識別を基に作られています。 セキュリティ マトリクスは、各システムのクイック リファレンスとして使用でき、ネットワーク リソースへのアクセスを制限するための適切な計画の作成などの追加のセキュリティ対策の開始点となります。

システム	説明	リスク レベル	ユーザ タイプ
ATM スイッチ	コア ネットワーク デバイス	高	デバイス設定に関しては管理者（サポートスタッフ専用）、 転送に関しては他のすべてのユーザ
ネットワーク ルータ	配信ネットワーク デバイス	高	デバイス設定に関しては管理者（サポートスタッフ専用）、 転送に関しては他のすべてのユーザ
クローゼット スイッチ	アクセス ネットワーク デバイス	中間	デバイス設定に関しては管理者（サポートスタッフ専用）、 転送に関しては他のすべてのユーザ
ISDN またはダイヤルアップ サーバ	アクセス ネットワーク デバイス	中間	デバイス設定に関しては管理者（サポートスタッフ専用）、 特別のアクセスに関してパートナーおよび特権ユーザ
ファイアウォール	アクセス ネットワーク デバイス	高	デバイス設定に関しては管理者（サポートスタッフ専用）、 転送に関しては他のすべてのユーザ
DNS サーバと DHCP サーバ	ネットワーク アプリケーション	中間	設定に関しては管理者、 使用に関しては一般ユーザおよび特権ユーザ
外部電子	ネットワ	低	設定に関しては管理者、 イ

メール サーバ	ーク アプリケーション		ンターネットおよび内部メール サーバ間のメール転送に関してはすべての他のユーザ
内部電子メール サーバ	ネットワーク アプリケーション	中間	設定に関しては管理者、 使用に関しては他のすべての内部ユーザ
Oracle データベース	ネットワーク アプリケーション	中または高	システム管理に関しては管理者、 データの更新に関しては特権ユーザ、 データ アクセスに関しては一般ユーザ、 一部のデータ アクセスに関しては他のすべてのユーザ

セキュリティチーム構造の確立

セキュリティ マネージャがリーダーとなり会社の各事業部からの参加者をメンバーとする組織にまたがったセキュリティ チームを作成します。 チームの担当者はセキュリティ ポリシー、およびセキュリティの設計と実装の技術的な側面に注意する必要があります。 多くの場合、この目的でチーム メンバーに対する追加トレーニングが必要となります。 セキュリティ チームには、3 つの担当領域があります。 これは、ポリシー作成、実施、対応です。

ポリシー作成の目的は、会社のセキュリティ ポリシーを確立およびレビューすることです。 少なくとも、リスク分析およびセキュリティ ポリシー両方を毎年レビューします。

実施は、セキュリティ チームがリスク分析を実行し、セキュリティの変更要求を承認し、ベンダーおよび CERT メーリング リストの両方のセキュリティ アラートを確認し、そして普通の言葉でのセキュリティ ポリシー要件を特定の技術的な実装に置き換えるまでの段階です。

最後の担当領域は対応です。 ネットワーク モニタリング中にセキュリティ違反を識別することがありますが、このような違反の実際のトラブルシューティングと修正を行うのはセキュリティ チーム メンバーです。 各セキュリティ チーム メンバーは、担当の領域内にある機器で提供されるセキュリティ機能について詳しく知っておく必要があります。

チームの責任は全体として定義していますが、セキュリティ ポリシーに基づくセキュリティ チーム メンバーの個々の役割および責任を定義する必要があります。

防止

防止は、2 つの部分に分けることができます。 1 つはセキュリティ変更の承認で、もう 1 つはネットワーク セキュリティのモニタリングです。

セキュリティ変更の承認

セキュリティの変更は、ネットワーク全体のセキュリティに影響する可能性のあるネットワーク機器への変更として定義されます。 セキュリティ ポリシーでは、特定のセキュリティ設定の要件を技術的な用語を使用せずに明記する必要があります。 つまり、「ファイアウォールを介した外部ソース FTP の接続は許可されない」と要件を定義する代わりに「外部接続でネットワーク内部

からファイルを取得できてはならない」のように要件を定義します。 組織にとって一意の 1 組の要件を定義する必要があります。

セキュリティチームは、普通の言葉で書かれた要件のリストを確認して特定のネットワーク設定や設計上の問題が要件を満たしていることを確認する必要があります。 セキュリティ チームでセキュリティ ポリシーを実装するために必要なネットワーク設定変更を作成したら、これを今後の設定変更に適用できます。 セキュリティ チームがすべての変更を確認することもできますが、この作業でセキュリティ チームは特定の処置を保証するために十分にリスクがある変更だけを確認することができます。

シスコでは、セキュリティ チームが次のタイプの変更を確認することを推奨します。

- ファイアウォール設定への変更
- アクセス コントロール リスト（ACL）への変更
- 簡易ネットワーク管理プロトコル（SNMP）の設定への変更
- 認定ソフトウェア リビジョン レベル リストと相違するソフトウェアでの変更または更新

また、次のガイドラインに従うことを推奨します。

- 定期的にネットワーク デバイスのパスワードを変更する。
- ネットワーク デバイスへのアクセス権を個人の認定のリストに制限する。
- ネットワーク機器とサーバ環境の現在のソフトウェア リビジョン レベルがセキュリティの設定の要件に従っていることを確認する。

これらの認可のガイドラインに加え、変更管理の承認委員会で確認するすべての変更をモニタするために、セキュリティ チームからの担当者をこの委員会に加えてください。 セキュリティ チームの担当者は、セキュリティ チームによって許可されるまで、セキュリティの変更として考慮されているどの変更も拒否できます。

ネットワークセキュリティのモニタリング

セキュリティ モニタリングは、セキュリティ違反を示すネットワーク内の変更の検出を目的にしている以外は、ネットワーク モニタリングに似ています。 セキュリティ モニタリングの開始点は、違反が何であるかを決めることです。 「リスク分析を行う」で、システムに対する脅威に基づいて必要なモニタリングのレベルを確認しました。 「セキュリティ変更の承認」では、ネットワークへの特定の脅威を確認しました。 これら 2 つのパラメータによって、モニタリングの対象および頻度を明確にイメージできます。

リスク分析の表では、ファイアウォールは高リスクのネットワーク デバイスと見なされ、リアルタイムでのモニタリングが必要と示されています。 「セキュリティ変更の承認」セクションで、ファイアウォールへの変更をモニタする必要があることがわかります。 これは、失敗したログイン、通常でないトラフィック、ファイアウォールへの変更、許容されたファイアウォールへのアクセス、およびファイアウォールを介した接続設定などを SNMP のポーリング エージェントがモニタする必要があることを意味します。

この例に従って、リスク分析で識別される各エリアのモニタリング ポリシーを作成します。 シスコは、低リスクの機器を毎週、中程度リスクの機器を毎日、そして高リスクの機器を毎時モニタすることを推奨します。 より迅速な検出が必要な場合は、より短い時間間隔でモニタします。

最後に、セキュリティ ポリシーでセキュリティ違反のセキュリティ チームへの通知方法を指定しておく必要があります。 多くの場合、ネットワーク モニタリング ソフトウェアが最初に違反を検出します。 これによってオペレーション センターへの通知がトリガーされ、これがセキュリティ チームに通知されます。必要な場合は、ポケットベルが使用されます。

シスコの対応

対応は、3 つの部分に分けることができます。 これは、セキュリティ違反、復元、およびレビューです。

セキュリティ違反

違反が検出されると、ネットワーク機器の保護機能で、不正侵入の範囲が判断され、迅速な判断に基づいて通常の動作を回復します。 これらの判断を事前に行っておくと、不正侵入に対する対応が管理しやすくなります。

不正侵入の検出後の最初のアクションは、セキュリティ チームの通知です。 所定の手順を踏まない場合、正しい対応を適用できる正しい人間の確保にかなりの遅延が発生するおそれがあります。 1 日 24 時間、1 週間に 7 日いつでも使用できる手順をセキュリティ ポリシーで定義します。

次に、変更を行うセキュリティ チームに与える認証レベル、およびどの順序で変更を行うのかを定義する必要があります。 可能な対処方法は次のとおりです。

- 違反に対する今後のアクセスを防止するための変更を実装する。
- 侵入されたシステムを隔離する。
- 攻撃を追跡するために通信事業者または ISP に連絡する。
- 証拠を収集する記録デバイスを使用する。
- 侵入されたシステムまたは違反の発生源を切り離す。
- 警察またはその他の政府機関に連絡する。
- 侵入されたシステムをシャット ダウンする。
- プライオリティ リストに従ってシステムを復元する。
- 内部の管理者と法務担当者に通知する。

セキュリティ ポリシーで管理者の承認を得ずに実行できていた変更の詳細を確認してください。

最後に、セキュリティ攻撃中の情報を収集および維持する理由は 2 つあります。 まず、セキュリティ攻撃によって侵害されたシステムの範囲を判断するためで、次に外部違反を追跡するためです。 収集する情報のタイプと手段は目的に応じて異なります。

侵害の範囲を判断するためには、次を実行します。

- ネットワークのスニファ トレース、ログ ファイルのコピー、アクティブ ユーザ アカウント、およびネットワーク接続を取得してイベントを記録します。
- アカウントを無効にし、ネットワーク機器をネットワークから切断し、そしてインターネットから切り離して侵害が進まないように制限します。
- 侵害されたシステムをバックアップし、損害および攻撃方法の詳細な分析に役立てます。
- 侵入の他のサインを探します。 多くの場合、システムが侵害されると影響を受ける他のシステムまたはアカウントがあります。
- 攻撃の方法の証拠が見つかることがよくあるため、セキュリティ デバイスのログ ファイルおよびネットワーク モニタリングのログ ファイルを維持し確認します。

法的手段が必要と思われる場合は、法務部門で証拠収集の手順を確認し、当局の介入を得ます。 このような確認は法的手続きでの証拠の有効性を増加させます。 違反が実際には組織内だった場合、人事部門に連絡します。

復元

通常のネットワーク運用の復元は、すべてのセキュリティ違反の対応での最終的な目標です。 通常のバックアップの実行方法、セキュリティ方法、および使用可能にする方法をセキュリティ ポリシーで定義します。 各システムで独自のバックアップ方法および手順があるため、セキュリティ ポリシーは、バックアップからの復元が必要なセキュリティ条件をシステムごとに詳細に記述しているメタ ポリシーとして機能する必要があります。 復元が可能になる前に承認が必要な場合、承認を得るための手順も含めます。

リビュー

レビュー作業は、セキュリティ ポリシーの作成および維持における最終的な作業です。 レビューの対象となるのは、 ポリシー、ポスチャ、および実施の 3 つです。

セキュリティ ポリシーは常に変化する環境に対応する最新の文書である必要があります。 既知のベスト プラクティスに対して既存のポリシーをレビューして、ネットワークを最新状態に維持します。 また、CERT の Web サイト でセキュリティ ポリシーに組み込むことができる役立つヒント、推奨事項、セキュリティの向上、およびアラートを確認します。

また、目的のセキュリティ ポスチャを使用して、ネットワークのポスチャをレビューする必要があります。 セキュリティに特化した外部の企業はネットワークに精通しており、ネットワークのポスチャだけでなくセキュリティの対応もテストすることができます。 高可用性ネットワークの場合、このようなテストを毎年行うことを推奨します。

最後に、セキュリティ違反時に実行することを明確に理解していることを保証するために、サポート スタッフのドリルまたはテストとして練習問題が定義されています。 多くの場合、このドリルは管理者からの予告はなく、ネットワーク ポスチャのテストと結合して実施されます。 この確認によって、手順とトレーニングの差異を確認でき対処方法を実施できます。

関連情報

- White Paper：その他の最適な方法
- テクニカルサポート - Cisco Systems