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 ホワイト ペーパー

内容

概要

セキュリティ ポリシーを使用しない場合は、ネットワークの可用性が侵害される可能性があります。ポリシーは、ネットワークに対するリスクを評価し、対応チームを編成することから始まります。ポリシーを持続させるためには、セキュリティ変更管理活動を実践し、ネットワークのセキュリティ違反をモニタする必要があります。最後に、レビュー プロセスを通して既存のポリシーを修正し、教訓を反映させます。

このドキュメントは、準備、防止、対応の 3 つのエリアに分かれています。それぞれの手順について、詳しく説明していきます。

準備

セキュリティ ポリシーを実装するには、まず次の作業を行う必要があります。

- 利用ポリシー ステートメントを作成する。
- リスク分析を実施する。
- セキュリティ チーム構造を確立する。

利用ポリシー ステートメントの作成

セキュリティに関するユーザの役割と責任を要約した、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。社内のすべてのネットワーク システムとデータを対象とした一般的なポリシ

一から着手してください。このポリシーでは、一般的なユーザ コミュニティを対象に、セキュリティ ポリシーとその目的、セキュリティ業務を改善するためのガイドライン、セキュリティ上の責任の定義について明記します。従業員に対する処罰または懲戒処分につながる特定の行為が会社ですでに規定されている場合は、該当する行為とその回避方法をこのドキュメントに明示する必要があります。

次に、自社の従業員の行為に加え、パートナーが利用可能な情報、入手した情報の適切な取り扱いについてパートナーが把握できるように、パートナーのアクセプタブル ユース ステートメントを作成します。セキュリティ攻撃として認識されている特定の行為、およびセキュリティ攻撃が検出された場合に取られる罰則措置を明確に示す必要があります。

最後に、ユーザ アカウント管理、ポリシーの適用、および権限の確認に関する手順を説明した、管理者のアクセプタブル ユース ステートメントを作成します。ユーザ パスワード、またはデータの後処理に関して会社固有のポリシーが規定されている場合は、これらのポリシーも明確に提示してください。ポリシーをパートナーおよびユーザのアクセプタブル ユース ポリシー ステートメントと照合し、均一性を確保します。アクセプタブル ユース ポリシーに記載されている管理者の要件が、トレーニング プランおよび業績評価に反映されていることを確認します。

リスク分析の実施

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特定する必要があります。これは、危険性のあるすべてのネットワーク エントリ ポイントや、考えられるすべての攻撃手段を特定する必要があるという意味ではありません。リスク分析の目的は、ネットワークの各部分を識別し、それぞれに脅威レーティングを割り当て、適切なセキュリティ レベルを適用することです。これにより、セキュリティと必要なネットワーク アクセスの実用的なバランスを維持することができます。

各ネットワーク リソースに次の 3 つのリスク レベルのいずれかを割り当てます。

- **低リスクシステムまたはデータが侵害されても（不正ユーザによるデータの閲覧、データの破損、データの損失など）、ビジネスが中断されたり、法律上または財務上の問題が発生したりする可能性がない。**対象システムまたはデータは簡単に復元でき、他のシステムにさらに侵入されることはない。
- **中リスクシステムまたはデータが侵害された場合（不正ユーザによるデータの閲覧、データの破損、データの損失など）、ビジネスのある程度の中断や法律上または財務上の軽度の問題が発生したり、他のシステムにさらに侵入される可能性がある。**対象システムまたはデータの復元に多少の手間がかかるか、または復元プロセスによってシステムに悪影響が及ぶ。
- **高リスクシステムまたはデータが侵害された場合（不正ユーザによるデータの閲覧、データの破損、データの損失など）、ビジネスの著しい中断や法律上または財務上の重大な問題が発生したり、個人の健康と安全が脅かされたりする可能性がある。**対象システムまたはデータの復元にかなりの労力がかかるか、または復元プロセスによってビジネスまたは他のシステムに悪影響が及ぶ。

リスク レベルを割り当てるリソースには、コア ネットワーク デバイス、ディストリビューション 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 モニタと RMON プローブ）、ネットワーク セキュリティ デバイス（RADIUS と 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 と 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 サーバとネットワーク FAX 装置）などがあります。

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から、ネットワ

ークにさらに侵入される可能性があるため、これらは中リスクまたは高リスクのデバイスです。また、機器の破損によって、ネットワーク自体が機能しなくなることもあります。このような障害はビジネスに多大な悪影響を及ぼしかねません。

リスク レベルを割り当てたら、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。最も一般的なユーザ タイプを 5 つ示します。

- **管理者ネットワーク リソースを管理する内部ユーザ。**
- **特権より広範囲にアクセスする必要がある内部ユーザ。**
- **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にアクセスする必要がある外部ユーザ。**
- **その他外部ユーザまたは顧客。**

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 タイプを特定すると、次のようなセキュリティ マトリクスの基盤が形成されます。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戦略を作成するなど、さらなるセキュリティ対策の起点となります。

システム	説明	リスクレベル	ユーザのタイプ
ATM スイッチ	コア ネットワーク デバイス	高	デバイス設定：管理者（サポート スタッフのみ）。トランスポートとして使用：他のすべてのユーザ。
ネットワーク ルータ	ディストリビューション ネットワーク デバイス	高	デバイス設定：管理者（サポート スタッフのみ）。トランスポートとして使用：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	デバイス設定：管理者（サポート スタッフのみ）。トランスポートとして使用：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	デバイス設定：管理者（サポート スタッフのみ）。特別なアクセス権：パートナーおよび特権ユーザ。
Firewall	アクセス ネットワークデバイス	高	デバイス設定：管理者（サポート スタッフのみ）。トランスポートとして使用：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	設定：管理者。使用：一般ユーザおよび特権ユーザ。

外部の電子メール サーバ	ネットワーク アプリケーション	低い	設定：管理者。インターネットと内部メール サーバ間でのメール転送：他のすべてのユーザ。
内部の電子メール サーバ	ネットワーク アプリケーション	中	設定：管理者。使用：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	Medium または High	システム管理：管理者。データの更新：特権ユーザ。データ アクセス：一般ユーザ。一部のデータ アクセス：他のすべてのユーザ。

セキュリティチーム構造の確立

会社の各事業部門から担当者が参加し、セキュリティ マネージャをリーダーとする部門横断的なセキュリティ 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設計と実装の技術面に通じている必要があります。このため、多くの場合はチーム メンバーへの追加トレーニングが必要になります。セキュリティ チームには、ポリシー作成、実施、対応という 3 つの職務があります。

ポリシー作成は、会社のセキュリティ ポリシーの確立およびレビューに特化されます。リスク分析とセキュリティ ポリシーの両方を少なくとも年に 1 回は見直します。

プラクティスは、セキュリティチームがリスク分析、セキュリティ変更要求の承認、ベンダーとCERTメーリングリストの両方からのセキュリティアラートを確認 、プレーン言語のセキュリティポリシー要件を特定の技術実装に変える段階です。

最後の職務は対応です。ネットワークのモニタリング中にセキュリティ違反が確認されることは珍しくありません。このような違反に対し、実際に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 チームのメンバーです。セキュリティ チームの各メンバーは、自身が担当する分野の機器で提供されるセキュリティ機能の詳細を把握しておく必要があります。

チーム全体としての責任について定義してきましたが、セキュリティ ポリシーに関してセキュリティ チームのメンバーが担う個々の役割と責任も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、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

セキュリティ変更は、ネットワーク全体のセキュリティに影響を与える可能性が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要件

を非専門用語で明記する必要があります。つまり、要件は「ファイアウォールを介した外部ソースの FTP 接続は許可されない」と定義する代わりに、「外部接続によって内部ネットワークからファイルを取得できないようにする必要がある」というように定義します。 組織に合わせた固有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、一般用語で記された要件の一覧を確認して、要件に一致する特定のネットワーク設定または設計上の問題を特定する必要があります。チームによって、セキュリティ ポリシーの実装に必要なネットワーク設定の変更が作成されたら、これを以降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、このプロセスによって、チームは特別な対処を要するだけのリスクがある変更のみを確認することができます。

セキュリティ チームによる確認が推奨される変更には、次のものがあります。

- 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
- Simple Network Management Protocol（SNMP）設定への変更
- 承認済みソフトウェア リビジョン レベルのリストと異な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を承認済みユーザ リストに制限する。
- ネットワーク機器および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要件を満たしていることを確認する。

これらの承認ガイドラインに加え、セキュリティ チームの担当者を変更管理承認委員会の一員にして、委員会が審査するすべての変更をモニタできるようにします。セキュリティ チームの担当者は、セキュリティ変更と見なされる変更がセキュリティ チームによって承認されるまで、これを拒否できます。

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変更をネットワーク内で検出することに特化している点を除けば、ネットワーク モニタリングと似ています。セキュリティ モニタリングでは、まず違反となる対象を決定します。「リスク分析の実施」で、システムへの脅威に基づいて必要なモニタリング 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。これらの両方の要素によって、モニタリングが必要な対象とその頻度を明確に把握できます。

リスク分析マトリクスでは、ファイアウォールはリアルタイムでモニタリングする必要がある高リスクのネットワーク デバイスとされています。「セキュリティ変更の承認」によると、ファイアウォールへの変更はモニタリングが必要であることがわかります。これは、SNMP ポーリング エージェントが、ファイアウォールに関して、ログイン試行の失敗、通常と異なるトラフィック、変更、許可されたアクセス、およびファイアウォールを介した接続設定などをモニタリングする必要があることを示しています。

この例を参考に、リスク分析で特定された各エリアのモニタリング ポリシーを作成します。低リスクの機器は毎週、中リスクの機器は毎日、高リスクの機器は毎時モニタリングすることを推奨します。より迅速に違反を検出する必要がある場合は、モニタリングの間隔を短くしてください。

最後に、セキュリティ ポリシーでは、セキュリティ チームにセキュリティ違反を通知する方法を定義する必要があります。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。このソフトウェアによってオペレーション センターに通知が送信され、次にセキュリティ チームに通知されます。これには必要に応じてポケットベルが使用されます。

応答

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

セキュリティ違反

違反が検出された場合に、ネットワーク機器を保護し、侵入の程度を特定して、正常な動作を回復できるかどうかは迅速な判断にかかっています。事前にこれらの判断を規定しておくことで、侵入への対処はかなり管理しやすくなります。

侵入を検知した後でまず行うのは、セキュリティ チームへの通知です。手順が所定どおり行われないと、的確に対処できる適切な担当者の確保が著しく遅れることになります。セキュリティ ポリシーで、毎日 24 時間いつでも利用できる手順を定義します。

次に、変更を加えられるようにセキュリティ チームに与えられる権限レベルと、変更を行う順序を定義する必要があります。想定される修正措置は次のとおりです。

- 違反行為の再発を防止するための変更を実装する。
- 侵害されたシステムを分離する。
- 攻撃を追跡するために通信事業者または ISP に連絡する。
- 記録デバイスを使用して証拠を収集する。
- 侵害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。
- 侵害されたシステムをシャットダウンする。
- 優先順位リストに従ってシステムを復元する。
- 内部の管理担当者と法務担当者に通知する。

セキュリティ ポリシーには、管理者の承認なしで実行できる変更を詳しく記述してください。

最後に、2 つの理由から、セキュリティ攻撃中の情報を収集および保管します。1 つはセキュリティ攻撃によってシステムが侵害された範囲を特定するため、もう 1 つは外部違反の訴訟に備えるためです。収集する情報の種類とその収集方法は、目的によって異なります。

侵害の範囲を特定する方法は次のとおりです。

- 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の情報を取得して事象を記録する。
- アカウントの無効化、ネットワーク機器のネットワークからの切断、インターネット接続の解除によって侵害の拡大を阻止する。
- 損害および攻撃方法を詳細に分析できるように、侵害されたシステムのバックアップを作成する。
- その他の侵害の兆候を調査する（多くの場合、システムが侵害されると、他のシステムやアカウントも影響を受けます）。
- セキュリティ デバイスのログ ファイルとネットワーク モニタリングのログ ファイルは、攻撃方法を解明する手がかりとなる場合が多いため、保管して再度確認する。

法的措置が必要と思われる場合は、法務部門で証拠収集と当局の介入に関する手続きを確認してください。こうした確認によって、訴訟における証拠の有効性が向上します。内部的な性質の違

反であった場合は、人事部に連絡してください。

復元

セキュリティ違反に対応する上での最終目標は、正常なネットワーク運用の復元です。通常のバックアップの実行方法、保全方法、利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。バックアップの方法と手順は各システムで異なるため、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説明したメタポリシーとして機能する必要があります。復元を実行する前に承認が必要な場合は、承認を得るためのプロセスも示します。

詳細については、『

レビュー プロセスは、セキュリティ ポリシーの作成および維持での最後の取り組みです。レビューの対象となるのは、ポリシー、ポスチャ、演習の 3 つです。

セキュリティ ポリシーは、絶えず変化する環境に合わせて更新され続ける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見直すことで、ネットワークを最新の状態に保ちます。また、CERTのWebサイトでは 、セキュリティポリシーに組み込むことができる有用なヒント、プラクティス、セキュリティの改善、およびアラートを確認してください。

さらに、目的のセキュリティ ポスチャと比較してネットワークのポスチャを確認する必要があります。セキュリティを専門にする外部企業では、ネットワークに侵入して、ネットワークのポスチャだけでなく、組織のセキュリティ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は、毎年このようなテストを行うことが推奨されます。

最後の演習とは、サポート スタッフがセキュリティ違反の発生時に取るべき対応を十分に理解していることを確認するためのドリルまたはテストのことです。このドリルは、ほとんどが管理者から予告されることなく、ネットワーク ポスチャ テストと併せて実施されます。このレビューによって手順とスタッフ トレーニングのギャップを確認し、修正することができます。

関連情報

- その他のベスト プラクティスのホワイト ペーパー
- テクニカルサポート - Cisco Systems