ネットワーク セキュリティ：概要

この数年間、インターネットに対応したビジネス、つまり e- ビジネスによって企業の効率および収益が大幅に向上しています。e- コマース、サプライチェーン管理、リモート アクセスなどの e- ビジネス アプリケーションを使用すると、プロセスの合理化、運用コストの低減、および顧客満足度の向上が可能になります。このようなアプリケーションには、音声、画像、およびデータのトラフィックに対応可能なミッションクリティカル ネットワークが必要です。また、このネットワークは、容易に拡張して、ユーザ数の増加や、キャパシティとパフォーマンスの向上に対応できる必要があります。しかし、対応アプリケーション数およびユーザ数が増加するにつれて、ネットワークは、多様化するセキュリティの脅威にこれまで以上にさらされます。今日のネットワークでは、これらの脅威に対抗し、e- ビジネス トランザクションへの侵入を防ぐために、セキュリティに関するテクノロジーを重視する必要があります。

ネットワークに安全性が要求される理由

攻撃

適切に保護されていないと、どんなネットワークでも、あらゆる部分に攻撃または不正アクセスを受ける恐れがあります。高度な知識を持ったハッカー、競合企業、時には、社内にいる社員が、ルータ、スイッチ、およびホストのいずれにも侵入する可能性があります。実際、いくつかの調査によると、ネットワーク攻撃の半数以上は、社内から行われています。サンフランシスコの Computer Security Institute（CSI）は、ネットワークの悪用の 60 ～ 80 % は、社内から発生していると推測しています。IT 管理者は、ネットワーク攻撃を防ぐ最善の方法を判断するには、調査可能な攻撃のタイプと、この攻撃による e- ビジネス インフラストラクチャへの被害を理解する必要があります。最も一般的なタイプの攻撃には、Denial of Service（DoS; サービス拒絶）攻撃、パスワード攻撃、および root アクセス攻撃があります。

DoS 攻撃は、侵入者は特定のデータへのアクセス権を入手しないものの、IS リソースを「占有」することで、正規ユーザによるアプリケーションの利用を妨害するため、特に悪質です。この攻撃は、通常、企業ネットワークまたはインターネットに接続されているマシンに対して、ハッカーが無意味または処理不能な大量のデータを送り付ける方法で行われます。さらに悪質なものには、攻撃者が複数のマシンやホストに侵入する Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃があります。Computer Security Institute（CSI）と FBI がまとめた 2001 年の『Computer Crime and Security Survey』によると、2000 年の 11 % に対して、38 % の回答者が DoS 攻撃を検出しています。

パスワード攻撃は、ネットワーク パスワードを不正に入手して機密情報に侵入する、最も一般的なタイプの攻撃です。正規ユーザのパスワードを「破る」と、ハッカーは、そのユーザのネットワーク リソースにアクセスできると同時に、このネットワークの残りの部分にアクセスするための強力な足掛かりを手に入れます。たとえば、2000 年 12 月には、シアトルのワシントン大学医療センターからハッカーがユーザ パ

スワードを盗み出し、約 5000 人分の患者に関する機密データが含まれているファイルにアクセスする事件が起きました。多くの場合、ハッカーは容易にパスワードを入手します。パスワードには一般的な語句または数が選択されることが多いので、ソフトウェア プログラムを使用して機械的にパスワードを割り出すことが可能になるからです。また、ハッカーがソーシャル エンジニアリングという手法によってパスワードを入手する場合もあります。ソーシャル エンジニアリングは、非技術的な手法によって機密性の高いネットワーク セキュリティ情報を入手する行為であり、急速に広がっています。技術サポートの担当者を装ったり、社員に直接電話をかけてパスワード情報を収集するなどの手法があります。

ネットワーク上に電子メール サーバしかなかったインターネットの初期の時代から、ハッカーの最終目的は、アプリケーションが実行されている UNIX ホストの root アクセス権を手に入れることでした。root アクセス権があれば、システムを完全に制御でき、多くの場合、このネットワークの残りの部分および他のパートナー ネットワークにアクセスするための十分な情報を収集可能です。e- ビジネス アプリケーションのホストが増えたため、ハッカーの標的の数が増加しています。これらのホストのオペレーティング システムまたはアプリケーションにおいて、システム管理者が防護策を講じていないセキュリティの脆弱性、つまり、セキュリティ ホールがハッカーによって不正利用されることが多くあります。ハッカーは、バッファ オーバーフローやトロイの木馬などの一般的な手法を使用して、他の攻撃を開始するための足掛かりとして利用するホストの制御権を入手します。このような行為が原因で 1 つの組織全体の IS インフラストラクチャが脆弱になり、深刻な金銭的な損失または法的責任が発生する可能性もあります。

侵入によるコスト

ネットワーク攻撃により、数時間から数日にわたるダウンタイムが発生したり、データの機密性および完全性が著しく侵害されます。ネットワーク攻撃の影響は、単なる迷惑行為から徹底的な破壊まで、攻撃の程度や侵入された情報の種類によって異なります。また、攻撃からの復旧に要するコストにも、数百ドルから数百万ドルという幅があります。

ネットワーク攻撃によってアプリケーションのアベイラビリティが損なわれると、1 時間当たり数百万ドルの損失が発生する可能性があります。たとえば、e- コマース Web サイトを運営している企業は、カスタマーが他の調達先から製品およびサービスを購入するたびに、利益を失います。情報提供型の Web サイトの場合、広告のための貴重な時間が失われます。また、サプライチェーン管理のアプリケーションを利用している製造業の企業は、原材料に関する情報にアクセスできないため、生産ラインの停止に追い込まれる可能性があります。

データの機密性が損なわれると、即座に影響が出るとは限りませんが、大きなコストが発生する可能性があります。たとえば、ある組織の電子メール システムにハッカーがアクセスし、組織の競争力を支えている機密情報が盗まれた場合、この地位を確立するために投入されてきた研究開発費の損失になります。

データの完全性が損なわれると、攻撃による影響を修正するために、高額なコストが発生する場合が多くあります。たとえば、悪質なハッカーが、Web サイトに変更を加え、情報を無意味または有害な内容に置き換える場合があります。この場合、サイトの所有者には、サイトを修正するコストだけでなく、対外的な印象の悪化に対処するコストも発生します。

データの機密性および完全性の侵害に対する法的措置にも、莫大なコストがかかる可能性があります。米国政府は、電子情報のプライバシーに関する法規制を成立させ、現在もその整備を進めています。実際、米国議会には、オンライン上のプライバシーとセキュリティに関する約 50 件の法案が提出されています。既存の法規制および審議中の法規制では、一般に、違反した組織には一定の罰則が科される可能性があることが規定されています。たとえば、米国の金融機関を対象とする複数のプライバシー規制が盛り込まれているグラム リーチ ブライリー法に違反した組織には、FDIC 保証の停止から最大 100 万ドルの罰金に至る罰則が科される場合があります。

外部のハッカーによる犯行であっても、情報が十分に防御されていなかった場合、法廷では情報を保管している企業側に過失が認められる可能性があります。さらに、データの完全性に被害を受けた企業は、誤ったデータまたは不快なデータによって悪影響を受け、損害賠償または懲罰を求めるカスタマーからの訴訟にも対処する必要がある場合があります。

セキュリティ インフラストラクチャの設計

ネットワーク セキュリティの目的は、ネットワークとそのアプリケーションを攻撃から保護し、情報のアベイラビリティ、機密性、および完全性を確保することです。組織がこの目的を達成するためにネットワーク セキュリティのアーキテクチャを設計する際には、多くの要素を考慮する必要があります。攻撃を受けるリスクや、攻撃による被害の修復に要する潜在的なコストは、必ずしもすべてのネットワークおよびその関連アプリケーションについて同一ではありません。このため、費用便益分析を実施して、ネットワーク セキュリティに関するさまざまなテクノロジーおよびコンポーネントの投資効果と、これらを実装しない場合の機会費用を比較する必要があります。この過程では、ネットワーク セキュリティの実装を、顧客、社員、およびパートナーを引き付けられる優れた競争力として検討することが重要です。

セキュリティ ポリシー

通常、ネットワーク セキュリティを実装するための最初の前提条件はセキュリティ ポリシーであり、セキュリティ ポリシーからセキュリティ設計のプロセスが始まります。セキュリティ ポリシーとは、社内のリソースにアクセスする社員が遵守する規則について、経営陣の支持を受けた正式な文書です。セキュリティ ポリシーでは、2 つの主な問題に対処する必要があります。これらは、組織のビジネス上のニーズに基づくセキュリティ要件と、使用可能なテクノロジーに関する実装のガイドラインです。これらの問題に対処するために、セキュリティ ポリシーには、通常、いくつかの項目が含まれています。たとえば、セキュリティ ポリシーでは、認証ポリシーの項目を設けて、ユーザのタイプ（社内、リモート、ダイヤルイン、VPN など）ごとに必要なパスワードと権限のレベルを定義するのが一般的です。ビジネス上の要件およびセキュリティに関するテクノロジーは進化し続けているので、セキュリティ ポリシーは、生きた文書として定期的に更新する必要があります。

セキュリティ アーキテクチャ

セキュリティ アーキテクチャは、ネットワーク設計チームと IT セキュリティ チームの両者によって作成される必要があります。セキュリティ アーキテクチャは、通常、既存の企業ネットワークに統合されます。また、ネットワーク インフラストラクチャ経由で提供されている IT サービスに依存しています。それぞれの IT サービスについてアクセス要件およびセキュリティ要件を定義した後、明確な信頼レベルに基づいてネットワークを複数のモジュールに分割する必要があります。それぞれのモジュールを個別に扱い、異なるセキュリティ モデルを割り当てます。侵入が「成功」しても、そのアクセスをネットワークのごく一部に制限するために、セキュリティの階層を構築することが目標です。船の隔壁設計が浸水を封じ込めて沈没を防ぐ役割を果たすのと同様に、階層型のセキュリティ設計では、セキュリティ侵害がネットワーク全体の健全性に与える損害が制限されます。また、このアーキテクチャでは、ネットワーク全体にわたって実装される共通セキュリティ サービスを定義します。標準的なサービスには、以下のものがあります。

- パスワードの Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）
- Virtual Private Network（VPN; バーチャル プライベート ネットワーク）による機密性
- アクセス（Trust Model）
- 侵入検知システム（IDS）によるセキュリティ モニタリング

主な決定を下した後、段階的に、最も重要な分野から順にセキュリティ アーキテクチャを展開します。

セキュリティ テクノロジー

前述したとおり、ネットワーク セキュリティを設計するには、実装に対する投資額と、防御可能になる侵入の総コストを割り出す必要があります。次に、ネットワークの安全性を十分に確保するために、ネットワーク セキュリティに使用可能な予算の配分を決定する必要があります。できる限り包括的なレベルでの保護を行うため、すべてのネットワークには、ネットワーク セキュリティに関する次の 5 つの点に対応するセキュリティ コンポーネントを含める必要があります。

識別 （Identity）

ID は、ネットワーク ユーザ、ホスト、アプリケーション、サービス、およびリソースの正確かつ絶対的な識別証明です。識別メカニズムは重要であり、認証されたユーザが必要とする企業のコンピューティング リソースへのアクセスを得る一方で、権限のないユーザはアクセスを拒否されます。シスコシステムズのネットワークは、Cisco Secure Access Control Server（ACS）の AAA 機能を使用して、ユーザを認証してアクセス レベルを決定し、すべての必要な監査とアカウンティングのデータを保管する基盤を提供します。

境界セキュリティ

境界セキュリティ ソリューションでは、正規のユーザと情報だけがネットワークを介して渡されるように、重要なネットワーク アプリケーション、データ、およびサービスへのアクセスが制御されます。このアクセス制御は、Access Control List（ACL; アクセス コントロール リスト）を備えたルータとスイッチ、およびファイアウォール専用装置によって処理されます。ファイアウォールでは、ネットワーク境界を横断するトラフィックのバリアが提供され、事前に定義されているセキュリティ ポリシーに応じて、認証されているトラフィックだけが通過を許可されます。ウィルス スキャナ、コンテンツ フィルタなどの補足ツールも、ネットワーク境界の制御に使用されます。ファイアウォールは一般的に、組織がセキュリティ態勢を強化するために展開する最初のセキュリティ製品です。シスコは、組織のファイアウォールの選択においてきわめて高い柔軟性を提供します。Cisco PIXR Firewall は、先進のファイアウォールであり、あらゆる規模のお客様のネットワークに比類のない信頼性、スケーラビリティ、および機能性を実現します。Cisco IOSR Firewall では、ルーティングおよびスイッチ型のインフラストラクチャに組み込みのファイアウォール機能を提供します。

接続の安全性

企業は送信中の傍受や改ざんから機密情報を保護する必要があります。Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を実装することで、公共のネットワーク（通常はインターネット）上で私設の安全な通信を確立し、社内ネットワークをリモート オフィス、モバイル ユーザ、在宅勤務者、エクストラネットのパートナーに拡張できます。暗号化テクノロジーでは、メッセージおよびその添付データを「スクランブル」する高度な数学的アルゴリズムを使用することで、VPN を経由して移動するメッセージが、認証されている受信者以外の何者かに傍受されたり、読まれたりすることがなくなります。Cisco VPN 3000 Concentrator シリーズは、優れたリモートアクセス VPN ソリューションです。独自の専用アーキテクチャにより最先端のアベイラビリティの高い機能が組み込まれた Cisco VPN 3000 Concentrator を使用することで、企業は高性能でスケーラブルで強固な VPN インフラストラクチャを構築し、ミッションクリティカルなリモートアクセス アプリケーションをサポートできます。サイト間に VPN を構築するには、Cisco 800、1700、2600XM、3700 および 7200 ルータなどの Cisco VPN に最適化されたルータを使用する方法が適しています。

セキュリティの監視

ネットワークの安全性を保つには、企業は攻撃を絶え間なく監視し、定期的にセキュリティ インフラストラクチャの状態をテストする必要があります。ネットワーク脆弱性スキャナは弱点のある部分を予防的に確認することを、また、侵入検知システムは監視とセキュリティ上の問題が発生した際の対応を可能にします。

侵入検知システムと脆弱性スキャナを使用することで、ネットワーク セキュリティに新たな層が加わります。ファイアウォールは送信元、送信先、ポート、または他の基準に基づいてトラフィックを許可および拒否しますが、実際に攻撃用のトラフィックを分析したり、ネットワークの既存の脆弱性を見つけるわけではありません。また一般的に、ファイアウォールは「関係者（insiders）」が引き起こす内部の脅威には対処していません。Cisco Intrusion Detection System（IDS）は、ネットワーク境界、エクストラネット、および脆弱さを増している内部ネットワークの保護を可能にする業界初のリアルタイムでのネットワーク侵入検知システムです。このシステムでは、高速ネットワーク専用装置であるセンサーを使用し、個別のパケットを分析して不審なアクティビティを検出します。ネットワーク内のデータ ストリームが、不正なアクティビティまたはネットワーク攻撃を示した場合、センサーはこの悪用をリアル タイムで検出し、管理者にアラームを転送してネットワークから違反者を排除します。Cisco Secure Scanner は、ハッカーがネットワークのセキュリティ ホールを見つける前に、管理者がそれらを特定し修正するためのエンタープライズクラスのソフトウェア スキャナ アプリケーションです。

セキュリティ ポリシー管理

ネットワークの規模が拡大し、複雑さが増すにつれて、セキュリティ要素を管理できる中央集中型のセキュリティ ポリシー管理ツールの要件が重要になっています。セキュリティ ポリシーの状態を特定、管理、および監査できるブラウザベースのユーザ インターフェイスを使用した最新ツールによって、ネットワーク セキュリティ ソリューションの利便性と有効性が強化されます。シスコでは、企業向けに中央集中型でポリシーベースのセキュリティ管理方法を提供しています。CiscoWorks VPN/Security Management Solution（VMS）は、企業ネットワーク内のシスコのセキュリティ要素をサポートしているため、包括的で一貫性のあるセキュリティ ポリシーの実装が可能になります。VMS を使用すると、数百台の Cisco PIX シリーズ、IDS センサー、および Cisco IOS ルータに対して、セキュリティ ポリシーの定義、配布、適用、監査を 1 箇所から集中的に行うことができます。

SAFE Blueprint による安全な e- ビジネス

SAFE とは、Cisco AVVID（Architecture for Voice, Video and Integrated Data）に基づく、包括的かつ堅牢なセキュリティ ブループリントです。SAFE ブループリントは、ネットワーク領域ごとの個別の要件に対処する複数のモジュールで構成されています。SAFE ブループリントを導入すると、ネットワークに新たなサービスを追加するたびにセキュリティ アーキテクチャ全体を設計しなおす必要がなくなります。モジュラ式のテンプレートにより、必要に応じて新しいサービスごとにセキュリティを確保したり、そのサービスをセキュリティ アーキテクチャ全体に統合することが簡単になっており、コスト効果も向上しています。

SAFE は、ネットワークのどの部分にどのセキュリティ ソリューションを組み込む必要があるのか、また、これらのソリューションを配備する理由について、厳密な推奨事項を示した業界初のブループリントです。SAFE ブループリントの各モジュールでは、企業のセキュリティと整合性を維持しながら、特に e- ビジネスのパフォーマンスの最大化を実現します。

SAFE プログラムには、以下の要素が含まれています。

- ビジネス上の要件に基づいて実用可能なセキュリティ ポリシーを作成する、経験の豊富なシスコのセキュリティ サービス パートナー。
- セキュリティ テクノロジーおよびセキュリティ製品に関するシスコ認定プログラム。シスコのパートナーによる、お客様のセキュリティ アーキテクチャの計画、設計、および展開を確実に行います。
- セキュリティ運営に関するさまざまなオプション。運用計画の作成および定期的な Security Posture Assessment(SPA) の実施について、包括的なアウトソーシング サービスからコンサルティング サービスに至る幅広いオプションがあります。

SAFE の詳細については、http://www.cisco.com/japanese/warp/public/3/jp/event/offer/powernow/security/technical/index.html を参照してください。

ネットワーク セキュリティの詳細については、http://www.cisco.com/japanese/warp/public/3/jp/event/offer/powernow/security/index.html を参照してください。

お問い合わせ先

シスコシステムズ株式会社

URL:http://www.cisco.com/jp/
問合せ URL: http://www.cisco.com/jp/service/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL 03-6655-4433
電話でのお問合せは、以下の時間帯で受け付けております。
平日 10:00 ～ 12:00 および 13:00 ～ 17:00

02.06