



セキュリティ導入の手引き: 小規模企業における インターネット・セキュリティの理解

本書の内容

- 1 概要: 小規模企業におけるインターネット・セキュリティ
- 2 インターネット・アクセス— 新しいビジネス機会
- 3 新しいリスクにも成りえる価値あるツール
- 4 ネットワークを保護する適切なセキュリティの実践
- 5 信頼できるアドバイザー
- 6 まとめ



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

概要: 小規模企業におけるインターネット・セキュリティ

コンピュータ・ネットワークは、社員の生産性を高め、製品やサービスを市場に提供する新しい方法を企業に与える強力なビジネス・ツールです。しかし、インターネットに接続されているコンピュータが一台だけであったとしても、何らかのセキュリティが必要です。情報やインターネット接続に対する企業の依存度が高まるほど、セキュリティ対策を講じておくことが重要になります。この場合、セキュリティ対策とは何であり、一般的な小規模企業において、適切な保護が確信できる方法は何によってでしょうか? 本書では、すべての小規模企業がインターネット・セキュリティについて必要な知識を解説します。

インターネットへのアクセス— 新しいビジネス機会

コンピュータの価格とインターネットへのアクセス料金が以前に比べて手ごろになった今、あらゆる小規模企業でインターネットに接続することが容易に可能となりました。実際、多くの小規模企業にとって、インターネットに接続することは、電話やファックスやコピー機のように必要不可欠な存在となってきました。小規模企業は、インターネットをビジネス・パートナーや顧客との通信手段として利用し、情報提供により自社のビジネスの認知度を高めることや、販売サイクルを短縮し、オンラインで取引を成立させることもできます。

新しいリスクにも成りえる価値あるツール

インターネットは、新しく強力なビジネス・ツールですが、企業にこれまでにないリスクをもたらします。リスクには、単に迷惑を被るだけでなく、破壊的でダメージを与え、企業のデータやビジネスの機密性と整合性を脅かすものもあります。

脅威は、ハッカー、サイバー・テロリスト、産業スパイ、不満を持つ社員、トレーニングされたスタッフなどによってもたらされます。この中には、一般的な小規模企業に無縁で見当違いのグループがあると感じるかもしれませんが、悪意のあるグループは巧妙かつすきを見て行動し、個人的に中小企業や大企業を狙う可能性があります。さらに、経験が乏しくトレーニングが十分でない社員は、ネットワーク・セキュリティの実施に精通していないため、他人につけ込むすきを与え、他のグループと同様にリスク要因ともなります。

ネットワークを保護する適切なセキュリティの実践

インターネットに接続している企業はどこもリスクに直面しているため、インターネットを使用している企業はすべて、何に対して安全対策を講じるべきかを知るために、自社に関係あるリスクを具体的に理解する必要があります。企業は、以下の質問に答えることによって、情報リソースの重要性を明らかにし、どの情報リソースを保護すべきかを理解することができます。また、企業は信頼できるアドバイザー(「信頼できるアドバイザー」のセクションを参照)に全体的かつ専門的なセキュリティの査定を依頼することも検討する必要があります。

保護すべき情報リソースはどれか?

たとえば

- ・ 社員情報または患者の記録、銀行の口座番号、設計図面やデザインを保護する必要があるか?
- ・ 政府または他の管轄機関の要件に従う必要があるか?

価値ある情報リソースは何か?

それらのリソースはどのような脅威に直面しているか(破損、盗難、改ざんなど)?

脅威が現実となる可能性はどの程度か?

脅威が発生した場合、ビジネスにどのような影響があるか(将来の収益の損失)?



Intelligent Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

まず、セキュリティ上の目標や目的とその達成計画を具体的に文書化することをお勧めします。これらの情報に基づいて企業のセキュリティ・ポリシーを作成し、目的、および目的を達成するために社員が貢献できることを理解し易く、認識を広げる必要があります。以下では、企業がセキュリティ上の目的を達成するために利用できる方法とツールについて説明します。

予防策

企業が情報を保護するための基本ステップには、次のようなものがあります。

重要なデータのバックアップ

企業は、情報の重要性和情報の変更頻度に応じて、毎週、毎日、または時間単位で、重要なデータを定期的にバックアップする必要があります。バックアップ・プロセスは、バックアップの実施予定時刻を含め、明確に文書化します。また、なるべくランダムな時刻でテストを実施し、正しいデータが適切にバックアップされているかの確認を行うことをお勧めします。

セキュリティ・アップデートの定期的なダウンロードとインストール

最も広く世間を騒がせている攻撃、ウイルス、ワームなどは、通常、一般的なソフトウェアのよく知られているセキュリティ・ホールを悪用します。ビジネス・ソフトウェアにセキュリティ・アップデートをダウンロードしてインストールするだけで、セキュリティ上の脅威を防ぎ、前向きな戦略で大多数の競合会社をリードすることができます。もちろん、これは使用しているセキュリティ製品についても同様です。ベンダは、セキュリティ製品を常に更新しているため、使用中のセキュリティ製品を最新の状態にしておくことが、脅威に打ち勝つ簡単な方法です。情報セキュリティで変わらないことが1つあるとすれば、それは、セキュリティ・リスクと脅威は絶えず現れ、変化し続けているということです。

適切なパスワードの取扱い方法の確立

大多数のハードウェアおよびソフトウェア製品は、出荷時に簡単によく知られているパスワードがあらかじめ設定されているため、製品を設置またはインストール後すぐに、デフォルトのパスワード設定を変更する必要があります。新しいパスワードを決めるときは、人名のようにすぐにわかるようなパスワードは避けるべきです。パスワードは、最小限の長さ(通常6文字以上)を持ち、数字と文字を組み合わせます。パスワードが決定したら秘密にしておく必要があるため、コンピュータのモニタにメモを貼り付けたりするような行為は避けてください。最後に、パスワードは数ヶ月に1回変更するなど、定期的に変更する必要があります。

情報の保護

ファイアウォール

多くの人々にとって、ウイルスやアンチウイルス・ソフトウェアは広く馴染みがありますが、ビジネス・ネットワークを保護する場合、ファイアウォールを最前線に置いて防御する必要があります。では、ファイアウォールとは何でしょうか? ファイアウォールは、コンピュータ・ネットワークとネットワーク上のリソース(PC、サーバ、個人データなど)を保護するセキュリティ装置です。

より正確に述べると、ファイアウォールは通常、公共のインターネットとプライベートなビジネス・ネットワークという2つのネットワークを接続するゲートウェイとして使用され、アクセスを制御します。ファイアウォールは、セキュリティ・ポリシーに基づいてこの2つのネットワーク間を通過するあらゆる通信(電子メール、Webページ、ファイルのダウンロードなど)を検査し、通信を通過させるか、させないかを決定します。ファイアウォールのセキュリティ・ポリシーは、企業のセキュリティ・ポリシー、すなわち企業がセキュリティ上の目的を達成するために実施する計画から直接作成する必要があります。



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

ファイアウォールの種類

チェック・ポイント社は、10年前にはじめて商用の製品ファイアウォールを市場に紹介しました。今日、市場にはファイアウォールによる保護を企業や個人に提供する無数の製品があります。しかし、セキュリティ・ポリシーを実施するファイアウォールで使用されている事実上の標準技術はステートフル・インスペクションで、チェック・ポイント・ソフトウェア・テクノロジーズが開発し、特許を取得した技術です。ステートフル・インスペクションを使用したファイアウォールは、個々のデータ・パケットを徹底的に検査し、最近通過した通信に関する情報を保持するため、ネットワークに最高水準のセキュリティを提供します。ファイアウォールは、この情報をすべて使用して、新しい通信が適切かどうかを判断します。

ファイアウォールは、適切なビジネス・セキュリティの確保に極めて重要な役割を果たすため、補助的な製品の中には、機能の一部に「ファイアウォール機能」を装備していると主張しているものがあります。これらの製品が実際に何をするかを明らかにするために、製品について少し説明します。

今日よく見かける種類の製品にPCファイアウォールがあります。これらの製品は、ネットワーク全体を保護するものでないため、本当の意味でのゲートウェイ・ファイアウォールとは言えません。PCファイアウォールは個々のコンピュータで実行され、そのコンピュータのみを保護します。このタイプのファイアウォール製品は、1台のコンピュータを保護するためには有益ですが、ネットワークが構築されているビジネス環境ではあまり効果的ではありません。これらの環境では、セキュリティ・ソフトウェアを複数のコンピュータにインストールして設定、管理することは、管理部門にとって非常に頭の痛い問題です。1人がコンピュータ上のセキュリティを停止したり、変更したりすると、ネットワーク全体のセキュリティが損なわれるおそれがあります。

「ビルトイン・セキュリティ」を主張するタイプの製品は、ブロードバンド・ネットワーク・デバイスです。これらのデバイスには、通常、ネットワーク機能にファイアウォールの小さなサブセット機能が付け加えられています。これらのデバイスは、インターネットのゲートウェイに設置されますが、ネットワークに真のステートフル・インスペクションに基づくファイアウォール機能を提供しません。多くの場合、これらの製品は、ネットワーク・アドレス変換 (NAT) と呼ばれる技術を使用しているのみです。NATは、コンピュータがインターネット上で通信するときに、コンピュータのネットワーク・アドレスを隠します。NATは、あらゆるコンピュータのアドレスを隠して、ハッカーがネットワーク上のコンピュータを見つけるのを困難にするため、セキュリティの向上が図れます。NATは重要なセキュリティ技術ですが、ファイアウォールの全体的な保護水準を高めるために、ステートフル・インスペクションなどの機能と組み合わせる必要があります。

バーチャル・プライベート・ネットワーク (VPN)

ファイアウォールは、ビジネス・ネットワークを保護しますが、ビジネス通信が社内ビジネス・ネットワークを離れて、たとえば企業から社員または企業から企業などのように、インターネット内を移動する場合、何を使用してビジネス通信を保護するのでしょうか？これは、出張中の社員、在宅勤務者、コンサルタント、ビジネス・パートナーなど、ビジネス・ネットワークへのアクセスが必要なユーザが存在する小規模企業にとって非常に重要な問題です。その解決策は、「バーチャル・プライベート・ネットワーク」すなわちVPNの導入です。VPNは、通信がインターネット内を移動するときに、情報を暗号化して他人に読めないようにします（「プライベート」と呼ばれるのはこのためです）。

VPNはリモート・ワーカーやモバイル・ワーカーなどの個人がビジネス・ネットワークにアクセスする必要がある場合や、社内ネットワークを、支社やビジネス・パートナーなどの別のネットワークに接続する必要があるときに、ビジネス情報を保護します。

VPNは、ビジネス通信を保護するばかりでなく、通信コストも大幅に削減します。VPNにより、リモート・ワーカーやモバイル・ワーカーがビジネス・ネットワークに接続する場合、専用のダイヤルアップ回線ではなく、低コストのインターネット・アクセスを利用することができます。また、複数のビジネス・ネットワークを接続する場合も同様で、ポイント・ツー・ポイント型の専用線接続の代わりに低コストの高速インターネット・アクセスを使用することができます。



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

電子メールの保護

電子メールは、ほとんどの企業で使用されている最も一般的なネットワーク・アプリケーションです。このため、電子メールはセキュリティ上の脅威を与えたり、迷惑行為を企てる犯人に頻繁に悪用されます。電子メールを保護する最も効果的な方法は、アンチウイルス・セキュリティ・ソフトウェアを使用することです。アンチウイルス・ソフトウェアのベンダは、電子メールによって運ばれるコンピュータ・ウイルスを絶えず追跡し、セキュリティ製品を更新して、ユーザのコンピュータにウイルスが感染する前に脅威を取り除きます。

アンチウイルス・ソフトウェアは、企業の個々のコンピュータにインストールすることも、インターネット・ゲートウェイなどの主要な場所にインストールすることもできます。たとえば、チェック・ポイントのファイアウォールは、アンチウイルス・セキュリティ・ソフトウェアと統合されて、ウイルスがネットワークに侵入する前にインターネット・ゲートウェイでブロックするため、管理が簡単になります。

ウイルスに感染していない電子メールもセキュリティを脅かす場合があります。スパムという大量にばらまかれる不要な"ジャンク"メールには、ほとんどすべての電子メール・ユーザが悩まされています。通常、スパムは広告に利用されますが、どのような場合でもスパムに回答すると、電子メール・アドレスが有効であることを相手に知らせることになります。それだけで、そのアドレスがより多くのスパムを送るターゲットにされるだけでなく、悪意のある攻撃者からさらに攻撃を受ける可能性が出てきます。このため、知らない人からの電子メール、特に添付ファイルは開かないことが安全につながります。ウイルスと同様、スパムに対処するアンチスパム製品があります。

ワイヤレス・セキュリティ

ワイヤレス・ローカル・エリア・ネットワーク(WLAN)は、あらゆる規模の企業で使用されるようになってきました。WLANにより、社員はオフィス内で自由に移動できるようになり、生産性が向上しました。しかし、ワイヤレス・ローカル・エリア・ネットワークは、セキュリティ・リスクにもなりえます。たとえば、外部の人がワイヤレス・デバイスを企業のネットワークに接続して、WLANトラフィックを監視することが考えられます。そのため、企業はWLANを保護することが重要です。WLANを安全にする簡単な方法は、VPNをWLANとともに使用することです。VPNを使用することにより、WLAN上の通信は暗号化されます。

セキュリティと望ましい慣行に関する社員教育

セキュリティ・リスクを査定し、セキュリティ・ポリシーを作成した後、社員教育を実施し、ポリシーと計画を推進することが大切です。すべての社員が個々のセキュリティ・リスクや自分たちがどのように保護されているかについて理解する必要はありませんが、社員がネットワーク・セキュリティに影響を与えることと、どのような方法でリスクの排除に協力できるかについて理解することは重要です。社員は、適切なパスワードの選択や電子メールの正しい扱い方などを通して、企業のセキュリティに大いに貢献することができます。

信頼できるアドバイザー

セキュリティ・リスクとその解決方法を理解することは、簡単ではありません。しかし幸いなことに、小規模企業のセキュリティに関するコンサルティングを専門に行っている企業があります。これらの企業は、リスクの査定、セキュリティ・ポリシーの作成、適切な製品の選択とインストール、セキュリティ・ポリシーの管理にいたるまで、さまざまな支援を行います。通常、これら企業の認定を取得したセキュリティの専門家により、上記の一部または全分野の指導が行われます。チェック・ポイントのパートナーで、セキュリティ・ソリューションを提供している企業の一覧については、www.checkpoint.co.jp/partner/index.htmlまたは、www.checkpoint.com/salesをご覧ください。この一覧で最寄りのソリューション提供会社をご覧ください。



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

まとめ

情報資産とコンピュータ・ネットワークへの企業の依存度が高まるに従って、ネットワークやインターネット・セキュリティは、あれば便利なものから必要不可欠なものとなりました。インターネット攻撃から電子メール・ウイルスにいたるまで、企業は何を保護するかと、どのように保護するかの両方を理解する必要があります。企業規模を問わず、セキュリティの必要性を評価し、適切なセキュリティ手順の実施とともに、ネットワーク・セキュリティに関する社員教育の必要性を強く認識することが求められます。

チェック・ポイント・ソフトウェア・テクノロジーズについて

チェック・ポイント・ソフトウェア・テクノロジーズは、インターネット・セキュリティ分野において世界をリードする企業で、VPNおよびファイアウォールの世界市場においてマーケット・リーダーとして評価されています。同社のセキュア・バーチャル・ネットワーク(SVN)アーキテクチャは、独自の技術により、安全で信頼性の高いインターネット通信を可能にするVPNおよびセキュリティのインフラストラクチャを提供します。SVNソリューションは、同社の次世代製品ファミリに組み込まれて、企業ネットワーク、リモート社員、ブランチ・オフィス、パートナーを結ぶエクストラネットにおけるビジネス通信とリソースを保護します。SVNの機能を拡張したものがチェック・ポイントのOPSEC(Open Platform for Security)で、業界をリードする325社以上の最高品質のソリューションを統合、相互運用するための業界のフレームワークを提供します。チェック・ポイントのソリューションは、149カ国で認定された2,500社のパートナーによって販売、統合、保守が行われています。詳細については、チェック・ポイントのWebサイト (<http://www.checkpoint.co.jp> または <http://www.opsec.com>) をご覧ください。

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F

<http://www.checkpoint.co.jp/> E-mail : info@checkpoint.co.jp Tel : 03(5367)2500

©2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Check Point Express, Check Pointのロゴ、ClusterXL、ConnectControl、FireWall-1、FireWall-1 GX、FireWall-1 SecureServer、FireWall-1 XL、FloodGate-1、INSPECT、INSPECT XL、InterSpec、IQ Engine、Open Security Extension、OPSEC、Provider-1、Safe@Office、SecureKnowledge、SecurePlatform、SecureXL、SiteManager-1、SmartCenter、SmartCenter Pro、SmartDashboard、SmartDefense、SmartLSM、SmartMap、SmartUpdate、SmartView、SmartView Monitor、SmartView Reporter、SmartView Status、SmartViewTracker、UAM、User-to-Address Mapping、UserAuthority、VPN-1、VPN-1 Accelerator Card、VPN-1 Edge、VPN-1 Pro、VPN-1 SecureClient、VPN-1 SecuRemote、VPN-1 SecureServer、およびVPN-1 VSXは、Check Point Software Technologies Ltd. およびその関連会社の商標、サービス・マーク又は登録商標です。その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668および5,835,726により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。記載された製品仕様は予告無く変更される場合があります。



Intelligent Security



Check PointTM
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail : info@checkpoint.co.jp Tel : 03(5367)2500

©2004 Check Point Software Technologies Ltd. All right reserved.
掲載内容を許可なく転載することを禁じます。