



**ソーシャルメディアリリース：
WatchGuardが中小企業への脅威トップ10を発表**

ソーシャルメディアリリース:

WatchGuardが中小企業への脅威トップ10を発表

シアトルー2008年9月9日

大規模のエンタープライズ組織と異なって、中規模・中小企業(SMB)では、資産、データ、および顧客情報の保護のための限られたリソースで、複数のセキュリティ脅威に対応しなければいけない。

WatchGuardの調査では、SMBに対するセキュリティ脅威のトップ10を特定した。

10) 内部スタッフ - SMBの多くでは、ビジネス記録と顧客情報が一人のスタッフによって管理される場合が多い。ネットワークシステムログ、自動レポートなどの適切なチェックとバランスがない場合、内部からのデータ損失が長期間に渡って発生することがある。

9) 危機管理計画がない - SMBに対する脅威の一つは、ハッキング、侵入、ウィルスなどが起こった後のビジネスへの影響である。SMBの多くは、データ損失後のポリシー、または復旧プランがないため、ビジネスの回復が遅れ、活動を再開することが出来ないことがある。

8) 機器情報が工場出荷設定のままである - ハッカーたちは殆どのネットワーク機器の工場出荷設定のログイン情報(ユーザーネームとパスワード)を把握し、仲間内で交換しているため、もし機器の設定が工場出荷設定から変更されていない場合、ハッカーは簡単にその機器のコントロールを乗っ取ることが出来る。

7) 自宅がセキュアではない - 中小企業の多くでは、多くの社員が自宅で仕事をするために、ノートパソコンを持ち帰ることがある。セキュアではない自宅のネットワーク環境で、仕事用のパソコンがウィルス、攻撃、マルウェア・アプリケーションなどの脅威にさらされている。

6) 公共ネットワークを不用心に使う - 攻撃者がよく行う方法の一つに、セキュアではないワイヤレスのアクセスポイントを「無料アクセスポイント」として提供し、ネットワークへのアクセスポイントを探しているモバイルユーザを待ち構えるということがある。パケット・スニッファーを起動することによって、攻撃者は自らを見られることがなく、入力された情報を見ることができ、そしてその情報を悪用することが可能となる。

5) ポータブル・デバイスの紛失 - 紛失されたノートパソコン、モバイル・デバイス、忘れられたUSBメモリなどによって、毎年、多くのSMBの情報が流出している。モバイル・デバイスのデータを暗号化し、強力なパスワード保護をおこなうことによって、これらの流出を止めることは可能ではあるが、SMBの多くはモバイル・デバイスとデータをセキュアに保護することをやっていない。

4) ウェブサーバーからの情報流出 - SMBの多くは自社のサーバーでウェブをホスティングしているが、適切な保護を行わないため、SQLインジェクション、ボットネット攻撃などの脅威からビジネス・ネットワークを守ることが出来ていない。

3) 不用心なネットサーフィン - 現在、普通に見えるウェブサイトにマルウェア、キーロッガー、スパムボットなどの脅威が隠されていることが多い。一見安全に見えるサイトへ不用心に訪問する社員によって、知らないうちにビジネスが脅威にさらされていることが多い。

2) **悪意のあるHTMLメール** - 企業への攻撃がメールに添付される悪意のあるファイルで行われることは少なくなっている。現在、脅威はHTMLメールの中に悪意の「地雷」サイトへのリンクとして隠されていることが多い。そのようなリンクを間違えてクリックしてしまうと、ダウンロードが自動的に開始されることがある。

1) **パッチが適用される前のセキュリティホールへの攻撃** - 90パーセント以上の自動攻撃は、既に知られているセキュリティホールを対象に行われる。パッチは定期的に提供されるが、ITスタッフが少ないSMB環境では、最新のアプリケーション・アップデートとパッチを自社のシステムに適用していないことが多く、本来であれば簡単に止められるはずの攻撃に対応できていないことがある。

コメント:

- Eric Aarrestad, Vice President of Marketing, WatchGuard Technologies.
「エンタープライズ企業と同じように、SMB に対するセキュリティ脅威は現実的に起きています。残念なことに SMB の多くは、これらの脅威に対応できる統合脅威管理 (UTM) アプライアンスを単純に知らないのです。」
- Carl Mazzanti, CEO, eMazzanti Technologies (管理セキュリティサービスプロバイダー)
「ネットワークをセキュアにすることによって、企業はより自由に生産性を高め、効率よく仕事をすることが出来ます。積極的にセキュリティを高める SMB 企業は、その業界内でリーダーになっていることがよく見られます。」

ウォッチガード・テクノロジー社について:

ウォッチガード・テクノロジー社は、1996年から、ネットワーク・セキュリティ・アプライアンスにおけるテクノロジー・リーダーとして、信頼性が高く管理しやすいセキュリティ・ソリューションを世界中の企業に対して提供しています。ウォッチガード統合脅威管理アプライアンス(有線とワイヤレス)およびウォッチガードSSL VPNリモート・アクセス・ソリューションは、拡張可能なネットワーク・セキュリティ、類を見ないネットワークの可視化、管理とコントロールを実現しています。ウォッチガード製品は、革新的なサポート、メンテナンス、教育プログラムである WatchGuard LiveSecurityによってバックアップされています。ウォッチガードは、米国ワシントン州シアトルに本社を置き、北米、ヨーロッパ、アジア太平洋、ラテン・アメリカ全域に支社があります。