報道関係者各位

2014 年 2 月 26 日

中小中堅企業(SMB)が知っておくべき セキュリティに関する 10 のヒント

中小中堅企業において、情報セキュリティの脅威から会社を守るためのいくつかのヒントを紹介します。

サイバー犯罪者にとって、社内セキュリティチームを有する可能性の高い大企業よりも、むしろ相当な資産を保有しながらセキュリティ管理を行っていない中小中堅企業が絶好のターゲットとなり得ます。サイバー犯罪者の目的は金銭であり、それを簡単に手に入れられる方を選ぶからです。

パッチをすぐに適用する

ソフトウェア・メーカーは、製品に脆弱性が見つかると、修正パッチを開発し、それをすべての登録ユーザに送信します。この更新をスタッフに任せている企業もあれば、集中管理によって更新している企業もあります。いずれの場合もパッチはすぐに適用する必要があります。公開された脆弱性は、サイバー犯罪者がその存在を認識しているセキュリティホールであり、彼らは、パッチを適用しないケースが非常に多いことを知っています。すべてのコンピュータにパッチが適用されない限り、セキュリティ侵害から逃れることはできません。

Windows XP を早急に変更する

マイクロソフトは 4 月に Windows XP のサポートを終了します。XP に関しては、今後いかなる脆弱性も修正されません。つまり、これらの不具合を発見したサイバー犯罪者が、それを悪用してマルウェア経由で侵入することが可能になるということです。サイバー犯罪者は、これらの不具合の多くをすでに発見しているものの現時点ではそれを隠し、4 月まで待ってから世界中にサイバー攻撃を次々としかける可能性が高いのです。被害を避ける唯一の方法は、サポートが終了する前にこのオペレーティングシステムを変更することです。Windows XP の後継のオペレーティングシステムは、セキュリティを優先して設計されているため、XP よりはるかに優れたものになっています。

モバイルおよびタブレットも保護が必要

サイバー犯罪者にとって、保護されていないモバイルデバイスも悪用の接点になります。一般の人々は、まだモバイルデバイスの保護という概念に慣れつつあるという段階です。だからこそビジネス用のデバイス上のデータ（連絡先、E メールなど）に犯罪者がアクセスし、さらにネットワーク上のデータが悪用される可能性を防止する必要があります。デバイスが会社から支給されたものであれ、個人所有のものであれ、これらすべてのデバイスでモバイルセキュリティを実行していなければなりません。

バックアップおよび同期

ここ 1 年の間にランサムウェアの攻撃が相次いで起こっています。攻撃を受けると、ファイルまたはコンピュータが暗号化されたことを告げるメッセージが画面上に表示され、アクセスの復旧と引き換えに金銭を要求します。このような攻撃に備えて、自動的にすべてのコンテンツのバックアップを取っておくことをお勧めします。

最新のアンチウイルスソフトウェアを使用する

新たなマルウェアがコンピュータまたはモバイルデバイスへアクセスしようとしていることが検出されると、そのマルウェアは隔離され、検査および解読のためにアンチウイルスラボに送られます。ウイルスのシグネチャが確認されると、将来この新たな脅威からユーザを保護するため、ソフトウェアの各登録ユーザに送信されます。最新のアンチウイルスソフトウェアがなければ、このような保護は受けられません。

クラウド環境および仮想環境も確実に保護する

仮想化技術は、パフォーマンスの向上と費用削減のために、中小中堅企業でも一般的なものになっています。これらの環境を保護することもまた、個々の企業情報に対する不正なアクセスを防ぐために重要です。

従業員にプライバシースクリーンフィルタを配布する

プライバシースクリーンフィルタは、ノートパソコンの画面上、またはモバイルデバイスに簡単に装着できるフィルタです。ユーザが正面から画面を見ているときはその違いに気づくことはありませんが、隣にいる人には画面が黒く見えるだけで他には何も見えません。

パスワード

もっとも多く使用されているパスワードが、「Password」でなくなったということは喜ばしいことですが、残念なことにそのパスワードは「123456」に変わっただけです。サイバー犯罪者は、パスワードの解読に複数の組み合わせを試すツールを使用します。よく使われるパスワード（例えば「123456」など）は、最初に試されます。その後、オンラインで見つけた対象者の誕生日といった情報を手掛かりにするなどして、文字の組み合わせを試します。パスワードを解読されにくくするには、記号や数字を加えることが有効です。

データは自分で思うよりもはるかに関心を持たれている

中小中堅企業の間ではしばしば、自社のデータには誰も関心を持たないから保護する必要がないという漠然とした意識があります。しかし例えば、競合他社がそのデータを得ることで、入札の際により低い金額を提示することも可能です。またサイバー犯罪者は、金融口座にアクセスするなど金銭的な目的で狙っています。自社の価値を決して過小評価してはいけません。

デバイスは紛失したり盗難に遭う可能性が常にある

デバイスの紛失や盗難は、誰にでも起こり得ることなので、常に備えておく必要があります。データのバックアップを取っていれば、紛失した場合の時間とコンテンツの損失は、回避できます。

エフセキュア株式会社 会社概要

http://www.f-secure.co.jp/

エフセキュア ー かけがえのないものを守る

エフセキュアは、お客様が重要なアクティビティに専念できるよう、コンピュータでもスマートフォンでも、オンラインでの保護と安全をお約束します。また、バックアップを提供するとともに、重要なファイルの共有も可能にします。エフセキュアのサービスは、200 以上の通信事業者を通じて世界で提供されており、数百万のホームユーザ、ビジネスユーザから信頼を受けています。1988 年創業のエフセキュアは、NASDAQ OMX Helsinki Ltd に上場しています。

エフセキュア株式会社は、エフセキュア社 100%出資の現地法人として設立され、以降、増収を続けながら順調に企業規模を拡大しており、2009 年 5 月に日本法人設立満 10 周年を迎えました。

会 社 名:	エフセキュア株式会社
カントリーマネージャ:	アリエン・ヴァン・ブロックランド
所 在 地:	〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
設 立:	1999 年 5 月
事業内容:	セキュリティ関連製品・サービスの販売およびサポート

本件に関するお問合せ先
エフセキュア株式会社
マーケティング部
Tel: 03-5545-8942 Fax: 03-5545-8945
Email: japan@f-secure.co.jp
〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
URL: http://www.f-secure.co.jp/
Blog: http://blog.f-secure.jp/