重要情報の扱いを考え直す（第3回）

パソコンに保存した重要情報が狙われる

2018.02.14

不正アクセスされてパソコンに保存していた情報が流出したり、情報漏えいに至らないまでも、外出先でパソコンを置き忘れたりする事象は後を絶たない。企業では顧客情報や機密情報の保護が最優先に近い課題となっている。

攻撃者はパソコンを不正操作し情報を盗み取る

一方、「どこまでセキュリティ対策を講じればいいのか分からない」という経営層の声も聞かれる。攻撃者の手口は日々進化しており、OSなどのセキュリティアップデートの前にOSの脆弱性を狙って攻撃を仕掛けるゼロデイ攻撃や、セキュリティ会社が配布する定義ファイルをすり抜ける未知の攻撃でマルウエアに感染させるなど、攻撃を完全に防御するのは困難な状況だ。

攻撃と一口に言ってもさまざまな手口がある。企業は何を守るかによって対策のメリハリを付けることが肝要だ。例えば、インターネットを使って商取引を行う企業では、Webサーバーが攻撃されるとビジネス停止のリスクが高くなる。Webサービスを妨害するDDoS攻撃などへの対策を強化すべきだろう。ただ、万一攻撃されてもシステムを復旧すればビジネスは再開できる。

被害の中でも、取り返しがつかないのが重要情報の漏えいだ。標的型攻撃メールでは、攻撃者は企業が保有する顧客情報や機密情報などを盗み取り、第三者に転売する金もうけを目的に企業を攻撃する。

顧客情報は、営業担当者などのパソコンに保管されているケースも多い。パソコンに保管された顧客情報は、机の中に名簿をしまっておくのと同様に犯罪者に簡単に見つけられ、盗まれるリスクが高くなる。

そこで、まずはパソコンのセキュリティ対策が重要になる。その理由は、標的型攻撃メールの手口にある。攻撃者はマルウエアに感染させたパソコンをインターネット経由で外部から不正に操作し、どこに顧客情報などの重要情報が保管されているかを調べる。そして、攻撃に成功したパソコンを経由して、ほかのパソコンにも重要情報がないか探していく。すべて遠隔操作で顧客情報を盗み取るのだ。

仮想化技術を利用してパソコンを攻撃から守る… 続きを読む