手軽に社員の能力アップ（第2回）

こんなときこそ気を付けたい。標的型メール対策

2020.04.15

標的型攻撃がサイバー脅威の最上位にランクしている。情報処理推進機構（IPA）は毎年、社会的に影響が大きい情報セキュリティ関連の事案をピックアップし「情報セキュリティ10大脅威」にまとめる。2020年版の「組織」部門の脅威のトップは「標的型攻撃による機密情報の窃取」だった。実は標的型攻撃は組織部門ができた2016年から、5年連続で1位にランクし続ける。国内で企業や団体などの組織が、最も注意すべき脅威は標的型攻撃なのだ。

標的型攻撃という言葉は目にしても、内容まではきちんと理解していないかもしれない。簡単に標的型攻撃の概要を説明しておこう。従来型のサイバー攻撃の多くは「バラマキ型攻撃」だった。コンピューターウイルスに代表される、悪意あるソフト「マルウエア」をメールやWebサイトに仕掛け、引っかかったパソコンやシステムに悪さをするものだ。特定の個人、企業や団体を狙ったものではなく、不特定多数を対象にした攻撃で、バラマキ型と呼ばれる。

一方で、標的型攻撃は、特定の企業や団体を狙う。機密情報などを窃取するのを目的に、攻撃する対象を十分に調べた上で、通常の業務のやり取りで“ありそうな相手”からの業務メールを装って攻撃を仕掛ける。

あなたの企業や組織にぴったりフィットさせたテーラーメードの攻撃というわけだ。こればかりは、ぴったりフィットしていると喜んでいられない。2020年初頭には、日本でも複数の防衛関連企業が不正アクセスを受けていた報道が出たように、セキュリティ対策意識の高い企業や団体でも、標的型攻撃に狙われると守りきれないケースがある。

調査で判明。8割の中小は社員教育未実施で社員の意識低い… 続きを読む