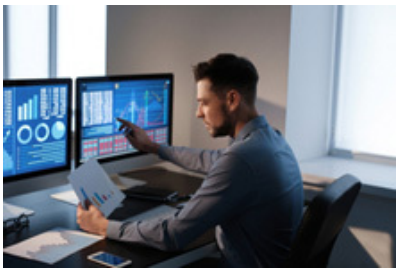
人手不足時代の業務効率策（第5回）

メール訓練、出入り口防御、サポートまで“任せる”

2020.04.15

2020年初頭、複数の防衛関連企業が標的型攻撃による不正アクセスを受けたニュースが相次いだ。日本を代表する大企業でも、一度標的にされたらサイバー攻撃から完全に身を守るのは難しい現実を目の当たりにさせられた。対象の状況を入念に調べて抜け穴になりそうな部分を徹底的に突く標的型攻撃は、防御が難しい面がある。



総務省の「国民のための情報セキュリティサイト」でも、「標的型攻撃は、狙われた組織向けに巧妙に作り込まれているため、完璧な防御対策を立てることは困難であるのが現状です」と指摘する。そのため、攻撃の侵入を防ぐ「入り口対策」、侵入後に被害の発生を防ぐ「出口対策」、さらに「社員・職員への教育」をバランス良く行う重要性を説く。情報システムを構成する機器のセキュリティ対策をサポートするソリューションに加え、標的型攻撃の主な侵入経路であるメールを実際に取り扱う社員・職員への教育が必要なのだ。

同サイトでは、「実際に想定される標的型攻撃のメール文を見せながら、典型的な手口や、開封してしまった場合の対応などを啓発するような教育が効果的です」とも指摘する。標的型メール攻撃対策は、訓練と機器サポートの両面から行うとよい。

多くの企業が標的型攻撃対策ソリューションを提供

標的型攻撃メールへの対応に代表される、標的型攻撃から企業・組織を守るソリューションは、数多くの製品やサービスがある。例えば、NEC、富士通ソーシアルサイエンスラボラトリ、日立ソリューションズ、東芝デジタルソリューションズといった大手のシステム事業者が「標的型攻撃対策ソリューション」を提供する。さらにセキュリティベンダーのラックやトレンドマイクロ、通信事業者のNTTコミュニケーションズ、ネットワークベンダーのネットワールドなども製品やサービスを提供しており、その種類は枚挙にいとまがない。

こうしたベンダーのソリューションでは、基本的に入り口対策や出口対策といった機器サポートの側面で、多くの製品やサービスを組み合わせて標的型攻撃対策の多層防御態勢を確立する。ソリューションによっては、標的型攻撃メールへの対策としての教育・訓練のソリューションも併せて提供する。また、人的な教育・訓練ソリューションを既存の機器サポート体制と組み合わせてトータルソリューションを構築するケースもある。

しかし、中小企業には大手ベンダーのトータルソリューションの導入、運用は荷が重い。求められるのは機器サポートと人的教育・訓練の両面を、まとめて手軽にかつ低コストで導入できるソリューションだ。

手軽に導入できるトータルパッケージ… 続きを読む