マネジメント講座

サイバーリスク対策入門 ② 標的型攻撃による情報流出

標的型攻撃は最も頻発している攻撃手法である。従来、DOS攻撃（サービス妨害攻撃）に代表されるように、サーバーダウンによるサービス停止を目的とするものが多かったが、最近では攻撃者がウイルスを仕込んだ添付ファイルやウイルスをダウンロードさせるウェブサイトのアドレスを電子メールで標的企業に送り付け、これを開かせることでパソコンなどをウイルスに感染させる巧妙な手法が増えている。1台でも感染すると、パソコンやネットワークに関する情報を収集し、これを踏み台として他のパソコンに不正アクセスし、最終的には標的企業内の複数のパソコンを制御して、電子メール、文書ファイルの情報を窃取する。狙われる情報は個人情報に限らず、システム破壊や業務妨害を目的とするアカウント情報、企業秘密なども含まれる。大量の個人情報を持たない中小企業であっても、安心できない。

標的型攻撃により情報を流出させた企業は、多くの場合、情報の取り扱いがずさんであると見られ、顧客や取引先からの評判や信頼を損ねる。メディアやSNSで報じられると情報管理についての信頼低下だけでなく、サービス品質全般が疑われる風評被害につながる可能性もある。損害賠償などの損失に加え、信頼失墜から生じる利益喪失も免れないことを認識しなければならない。

被害を最小限に抑えるには①侵入を防ぐ対策、②侵入を検知する対策、③検知した場合に適切に対処する対策を多層的に行うことが重要である。役職員の意識向上も重要。防災訓練のように「標的型攻撃メール訓練」を行い、不審メールを受信した時にどう動くかを一人ひとりが繰り返し体験することで被害を低減できる可能性が高まる。

（SOMPOリスケアマネジメント取締役　宮崎義久）

多層防御の考え方

多層防御

視点の異なる対策を幾重にも施すことにより被害の発生確率を低減させる考え方

1 侵入を防ぐための対策
- OS・ソフトウエアの更新
- セキュリティーソフトの導入・更新 など

2 侵入を検知する対策
- ネットワークの監視・防御
- エンドポイントの監視
- 防御機器の導入 など

3 検知した場合に適切に対処する対策
- 重要サーバーをネットワークから分離
- ログの相関分析 など

（注）SOMPOリスケアマネジメント作成

2018年6月5日
日経産業新聞