マネジメント講座

サイバーリスク対策入門 ④

ホームページ改ざん

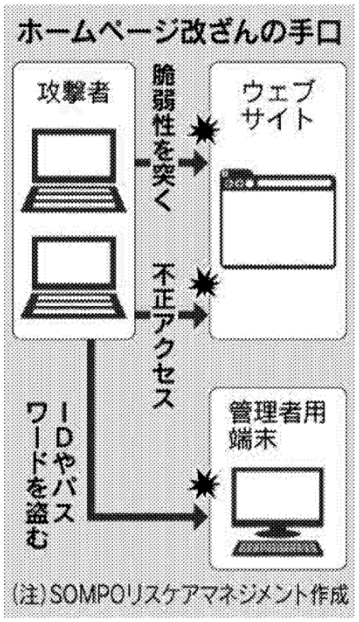
企業のEC（電子商取引）サイトが改ざんされ、情報漏洩した事例などを報道で目にすることも多い。ホームページ（HP）改ざんは企業を狙ったサイバー攻撃で頻繁に発生している。改ざんにより別のサイトへのリンクや参照先ファイルの書き換えを行い、HPを閲覧する利用者のパソコンにウイルスを感染させてアカウント情報や機密情報を盗むことがある。

入手したアカウント情報で不正ログインし、クレジットカードの不正使用によりユーザーに金銭的な損失を与えることもある。改ざんされたHPを運営する企業にとっては、調査・復旧作業のためにHPの公開を停止することによるビジネス機会損失や、情報漏洩に伴う損害賠償の損害が生じることはもちろん、顧客や取引先からの信頼の失墜や風評被害などを被ることにもつながる。

改ざんの手口は様々であるが、大きく2つに分類される。1つはシステム上の脆弱性を狙ったもの。もう1つは管理者のIDやパスワードの乗っ取りである。前者は、HPで使用しているソフトウエアの脆弱性やウェブサーバー上の脆弱性を突いてくる。基本的な対策としては基本ソフト（OS）を常に最新バージョンに更新しておくことや脆弱性診断を定期的に受けて発見された脆弱性に迅速に対応することなどが挙げられる。また、最新バージョンに更新できない状況では、WAF（ウェブ・アプリケーション・ファイアウオール）などを導入することによって監視を行い、不正アクセスを検知して被害の拡大を早期に防ぐことも有効な対策である。

経営層は、HPが改ざんされることによる影響を分析・評価し、セキュリティー対策を「投資」と捉えて予算や要員を確保することが重要である。

（SOMPOリスケアマネジメント取締役　宮崎義久）



2018年6月19日
日経産業新聞