事例で学ぶセキュリティインシデント（第9回）

対策の不備が信用問題になりかねないWebサイトの改ざん

2024.02.15

I社のWebサイト担当者から慌てた声で内線電話がかかってきた。

「Webサイトを更新しようとしたら、パソコン画面にウイルス感染の警告が出ました。すぐに見てもらえませんかっ！」

問い合わせを受けたIT担当者は「まずは落ち着いて」と声をかけ、Webサイトのサーバーをすぐにネットワークから切り離すように指示し、電話を切った。そして、Webサイトが何者かに攻撃され、改ざんされた可能性があることを悟ったーー。

サイトの改ざんでネット販売を一時停止

大阪で小売業を営むI社は、商業施設に出店するショップの他に自社で構築・運用するWebサイトを活用して海外の生活雑貨を中心に商品の宣伝・販売を行ってきた。近年はネット販売の売上比率も高くなり、Webサイトを訪れる消費者が商品を検索、注文しやすいようにユーザーインターフェースを工夫するなどネットに力を入れている。

I社は専任のIT部門はなく、管理部門の社員が社内システムの運用などを担当してきた。Webサイトをはじめ、情報システムのセキュリティ対策にも目を配り、これまで特にインシデントが起こるようなことはなかった。だが、近年他社のWebサイトが改ざんされ、ネット販売などサービスの一時停止が余儀なくされるケースは耳にしており、IT担当者は「ついにうちもやられたか」という思いだった。

Webサイトの改ざんでは、コンテンツ管理システム（CMS）のぜい弱性を悪用して攻撃する手口が知られている。また、Webサイト管理者のアカウントを盗み取り、サイトに不正なリンクを埋め込んで改ざんする手口もある。利用者はそれとは知らずに不正なWebサイトへアクセスし、パソコンがウイルス感染するなど、Webサイトを運営する企業のみならず、利用者にも被害が広がる恐れがある。また、企業の「顔」とも言えるWebサイトの改ざんは信用問題にもなりかねない。

ネットショッピングなどのWebサイトでは会員の氏名や住所、電話番号、購入履歴、クレジットカード番号などの個人情報がデータベースに登録されている。データベースと連携するWebアプリケーションのぜい弱性を悪用し、データを不正利用する「SQLインジェクション」や、Webページに悪意のあるスクリプトを埋め込む「クロスサイト・スクリプティング」などの手口は以前から知られ、データベースに蓄積された個人情報などが不正に閲覧されたり、情報が改ざんされたりするなどの危険性がある。

重要になるWebアプリのセキュリティ対策… 続きを読む