加害者にならないためのサイバー攻撃防止法（第1回）

「ついうっかり」が命取り。今こそ社員の意識改革

2015.09.16

毎日大量に受信するメール。中には取引先や上司・同僚ではなく、誰が送信者なのか分からないメールもあるだろう。そんなメールに付いてくる添付ファイルをついうっかり開いてしまったことはないだろうか。もっともらしい文面に油断して、あまり深く考えずに開いてしまい、慌てた経験を持つ方も少なくないはずだ。

去る2015年5月、日本年金機構で保有する個人情報125万件が外部に流出した事件は、まだ記憶に新しい。この情報漏えいの原因は、職員が悪意を持って送信された電子メールの添付ファイルを開封したこと。それをきっかけにネットワークに侵入され、大切な情報が盗まれてしまった。誰でもやってしまいそうな「誤操作」が、大事件の引き金になったのである。

情報漏えいが会社の危機を招く。被害者から加害者へ

個人情報をはじめとする機密情報などの情報漏えい事件が明らかになるにつけ、対策への意識は高めざるを得ない。だが事件の発生そのものは、そんな状況下でも後を絶たないのが実情だ。

こうした事件は、外部の悪意ある者からのサイバー攻撃によって引き起こされる。したがって、攻撃を受けて情報を漏えいさせてしまった企業は、理屈からいえば被害者だ。しかし、個人情報保護法の施行以来、企業は情報を安全に管理し外部に漏えいさせないよう努めるべき、との考えが主流となっている。情報漏えいを起こした企業は、当然のやるべき防止策を怠っていたということで加害者として扱われ、場合によっては賠償責任さえ生じるようになった。

日本年金機構のニュースがまさしくこの構図になっている。年金機構は個人情報を盗まれた被害者ではなく、管理を怠って情報を流出させた加害者という扱いだ。被害者は漏えいされた情報の主、つまり国民であるという取り上げ方だ。

あなたの会社が、何らかのサイバー攻撃を受け、社内にある顧客情報や取引先の情報、企業上の機密情報などを盗まれてしまったという事態を想定してみよう。

情報漏えいを引き起こしてしまったら、故意によるものか否か、どれだけ必死に予防対策を行っていたかなどは関係ない。漏えいしたという事実によって、悪者扱いされてしまう。それによる得意先や顧客に対するイメージの悪化は避けられない。そうなると、今までと同じような取引をしてもらえるだろうか。失った信頼や企業イメージをどう回復していけばいいのか。考えただけでぞっとしてしまう。

標的型攻撃は大企業や中堅企業だけでなく中小企業を狙う傾向も… 続きを読む