第1236回（2014年度 第7回）9月8日　会員セミナー

企業標的型サイバー攻撃の脅威とトップ・リスクマネジメントの重要性

講師：藤谷 護人 氏（弁護士法人エルティ総合法律事務所 所長 弁護士、公認システム監査人）

サイバー攻撃は、企業の社会的信用度の低下、顧客が被る経済的損害とそれに対する賠償責任など、経営上非常に大きなリスクとなる。年々激しさを増すサイバー攻撃について、IT紛争の解決に携わる弁護士の藤谷護人氏がその対策法を語った。

中小企業の研究開発者が狙われるケースも

新聞報道によると、電力・ガスなど国内の重要インフラ企業に対する標的型サイバー攻撃は今年4月から6月だけで226件も発生した。これは昨年度のほぼ一年分に相当する。

これら重要インフラ企業の従業員のID・パスワードが盗まれ、なりすまされて制御権を乗っ取られてしまえば、莫大な身代金を要求される。このような事例は海外でも報告されており、脅威は爆発的増加の様相を呈している。経営者は企業標的型サイバー攻撃の事例を知り、その内容を整理しておく必要がある。これは企業経営のトップ・リスクマネジメント以外の何物でもない。

攻撃の対象は大企業とは限らない。2012年に攻撃された企業を規模別に見ると、従業員2,500人以下の企業が50%で、そのうち250人以下の企業は31%を占めた。また、標的にされた役職別の比率では、研究開発者が最も高い27%を占めていた。ニッチで高度な技術を有する中小企業の研究開発者が狙われ、情報資産を盗み出される恐れがあるのだ。

サイバー攻撃が多様化しかも犯人の特定が困難

注意すべきは、サイバー攻撃の形態が多様化していることだ。これまでは、利用者が同じID・パスワードで複数のサービスを使うことを見越して、盗んだID・パスワードで他社へ不正ログインする「パスワードリスト攻撃」が多かった。しかし、最近はメールのやり取りを通じてウイルスを仕込む「やり取り型攻撃」や、標的企業にアルバイトなどの人材を送り込み、従業員らがよく利用するサイトに不正プログラムを仕掛ける「水飲み場型攻撃」が増えている。これらはいずれも意図を持って計画的に実行されている。

過去に起こった通販サイトのポイント情報窃取事件やオンラインショップの顧客クレジットカード情報窃取事件では、サービス提供会社やクレジットカード会社などに刑事および民事責任が適用されたが、いずれも本来責任を負うべき犯人の検挙は技術的に不可能だった。

真の脆弱性は経営トップのセキュリティマインドの欠如

それでは、何に注意すればよいか。まずは、リスクマネジメントについて整理しておく必要がある。

リスクをマネジメントするためにはリスクを認識、評価し、正常時の管理策を考えることが重要だ。その要点は防止策と抑制策を区別して機能させることにある。防止策はファイアウォールや入室規制を設定して、脅威が侵入するチャンスを狭める客観的な方法だ。一方、抑制策は主観的で、内部のアクセス権限を保持する人物が情報を持ち出すことを防ぐため、誓約書や就業規則で人間の心理に働き掛ける方法である。また、IPA（情報処理推進機構）が定期的に発する注意・警告に迅速に対応できる体制をつくることも企業の注意義務、リスクマネジメントである。

具体的には、脆弱性を指摘されたソフトウエアの改修、メンテナンスできずに放置したウェブサイトの閉鎖などの対策を採ることが有効だ。社員に対しては、ウェブサイトごとにID・パスワードを変えるよう指示する。特に、インターネット・バンキングは昨年7月以降、法人口座の不正送金被害が増加しているため、しかるべき対策を講じる必要がある。対策をせず被害に遭えば、必要な注意義務を果たしていたと見なされず、最低でも過失相殺を主張されるだろう。

重要なのは、トップが率先して経営に重大な影響を及ぼす恐れのある脅威を感じるセンスを磨き、組織のリスクマネジメント機能を作動させることだ。真の脆弱性は管理策や防護壁の穴ではなく、トップの心の穴、セキュリティ・マインドの欠如にあることを認識していただきたい。