最新セキュリティマネジメント（第34回）

企業に必須の情報セキュリティ対策の基本

2024.03.14

前回のコラムで、独立行政法人情報処理推進機構（以下、IPA）が「情報セキュリティ10大脅威2024」を発表したと紹介した。1位は4年連続で「ランサムウェアによる被害」だった。

発表から約1カ月後の2月29日には3つの解説書を公開している。この中には「情報セキュリティ10大脅威2024版 セキュリティ対策の基本と共通対策」という解説書もある。この解説書を元に、今、企業に求められるセキュリティ対策の基本について考えてみたい。

共通する攻撃の糸口から対策のあり方を考える

「セキュリティ対策の基本と共通対策」では、10大脅威以外にも多数の脅威が存在するものの、攻撃の糸口は似通っているとして5つに分類している。ここから情報セキュリティ対策を考えるとよいだろう。

攻撃の糸口の1つ目は「ソフトウェアの脆弱性」だ。利用しているソフトウエアの不備などを狙った攻撃がこれに相当する。セキュリティの専門家の多くは日々ソフトウエアを検証しており、脆弱性が見つかった場合にはIPAなどの団体やそのメーカーに連絡している。ソフトウエアを更新したり適切な対策を講じたりすればリスクを低減できる。

2つ目に「ウイルス感染」を挙げている。ウイルス感染は最もよく知られている攻撃手法だが、いまだに脅威をふるっている。対策としてはアンチウイルスソフトを導入したり、セキュリティ診断サービスを利用したりしてセキュリティレベルを上げておくとよいだろう。セキュリティソフトを利用して攻撃をブロックできればウイルス感染を防止できる。

3つ目は「パスワード窃取」で、対策の基本としてパスワードの管理・認証の強化を上げている。前回のコラムで取り上げたように、情報リテラシーの向上には従業員へのセキュリティ教育も必要だ。パスワードの重要性についても認識を深めてもらおう。

4つ目は「設定不備」だ。サーバーやクライアントデバイス、ネットワーク機器などの設定を誤ると、攻撃の糸口を与えてしまう場合がある。攻撃者は常に弱いところを洗い出しているのだ。普及が加速するクラウドサービスを利用する場合にも、適切な設定を行う必要がある。

5つ目は「誘導（罠にはめる）」という攻撃手法だ。攻撃者は偽のメールをクリックさせたりフィッシングサイトに誘導したりして、IDやパスワードを盗み取ったりマルウエアを送り込もうとしている。ここでもセキュリティ教育の徹底が重要なポイントになる。

組織として講じる対策、従業員に求めるべき対策… 続きを読む