最新セキュリティマネジメント（第39回）

長期休暇前後のセキュリティ対策

2024.08.19

夏休み、年末年始、ゴールデンウイークなど、従業員が長期休暇を取得する時期が年に何回かある。その場合、セキュリティ上ではどんな点に注意が必要になるのだろうか。独立行政法人情報処理推進機構（IPA）が発信する情報をベースに、日常とは異なる注意すべきポイントを考えてみたい。

休暇期間が長くなるとインシデント発生率が上昇

従業員が長期休暇を取得する際には、通常とは異なる点に注意する必要がある。特にシステム管理者の不在時には、セキュリティインシデントの対応に苦慮するケースも考えられる。IPAでは「長期休暇における情報セキュリティ対策」という記事で、システム管理者と利用者、個人に分けて解説している。

システム管理者向けに長期休暇前の対策として挙げているのは、「緊急連絡体制の確認」「社内ネットワークへの機器接続ルールの確認と遵守」「使用しない機器の電源OFF」の3点だ。

緊急時における連絡体制の整備や確認、社内ネットワークの接続ルールについては普段からきちんと対応しておくべきだが、改めて確認するとよいだろう。注目したいのは、「使用しない機器の電源OFF」だ。「長期休暇中に使用しないサーバー等の機器は電源をOFFにしてください」とある。

これは、最近増えている「ネットワーク貫通型攻撃」を意識したものだ。ネットワーク貫通型攻撃は、インターネットに接続された機器、装置類の脆弱（ぜいじゃく）性を悪用する攻撃で、情報が改ざんされたり不正な通信の中継点にされたりする場合がある。「電源OFF」は、不測の事態に対するリスクを少しでも減らす配慮が必要だと訴えている。

長期休暇明けの対策としては、「修正プログラムの適用」「定義ファイルの更新」「サーバー等における各種ログの確認」を挙げている。いずれも通常であれば日々当たり前のように行われているが、確認しない期間が長期に及ぶほどインシデントが発生する確率は高くなる。

特に重要なのは修正プログラムの適用と定義ファイルの更新だ。管理者が休み明けに出社した際には、まずこの2つをクリアしてから業務につくべきである。その上でサーバーのログをチェックし、不審な点があったらすぐに調査に着手したい。

長期休暇明け、通常業務に戻る際の注意点… 続きを読む