標的型メール訓練から見る経営層のセキュリティ意識

訓練において経営層の標的型メールの開封率は一般従業員の1.5倍に上っている。サイバー攻撃から組織を守るためには、経営層の理解のもと、社を挙げた体制の構築が求められる。

標的型サイバー攻撃の隆盛

標的型サイバー攻撃の勢いがとどまるところを知らない。2014年に発生した米Home Depot社を標的としたサイバー攻撃ではおよそ5600万件の顧客クレジットカード情報が漏えいし、米ソニー・ピクチャーズエンタテインメント社を標的としたサイバー攻撃では未公開の映画コンテンツを始めとした大量の機密情報が漏えいした。日本でも2015年に発生した、およそ125万件の個人情報が漏えいした日本年金機構に対するサイバー攻撃は記憶に新しい。

これら標的型サイバー攻撃が企業の経営にまで影響を与えるリスクの一つとなって久しい。2013年末におよそ4000万件のクレジットカード情報を漏えいした米Target社は事件発生後の決算で情報漏えい関連の費用として6100万ドルを計上し、その責任を取る形でCEOは退任を余儀なくされた。また情報漏えいの影響は一過性の損失にとどまらない。金融系の業種では、情報漏えいにより、既存顧客のおよそ5.6%が利用サービスを解約するという調査結果も報告されている[1)]。これらのリスクを避けるためにも、標的型攻撃への対策を準備しておくことは、経営者の重要な責務となっていると言えるだろう。

標的型サイバー攻撃とメール

標的型サイバー攻撃の多くは標的組織内部のPCにマルウェアと呼ばれる悪意のあるアプリケーションを実行（＝感染）させることで実施される。そのためには、マルウェアを組織の内部に送り込む必要がある。この組織の内部にマルウェアを送り込む手法の一つが標的型メール攻撃である。これは一見関係ないファイルに偽装したマルウェアをメールに添付し、組織内部の人間に送付することで、誤って添付ファイルを実行したPCをマルウェアに感染させる手法である。

「怪しいメールは開かないように」というフレーズは多くの方が何度も耳にされているだろうし、怪しいメールをいまさら開封する人間もいないと思われるかもしれない。しかし当社が2012年度から2014年度までの3年間に実施した標的型メール訓練[2)]では、訓練メールを送付したおよそ41万人の対象者のうち19%がメールに添付されたファイルを実行している[3)]。セキュリティ技術は日々進歩しているが、この人間の脆弱性を利用する原始的な手法は、残念ながら、未だ攻撃者にとって有用な手段の一つである。

CSIRTの流行

標的型サイバー攻撃にはどのような対策を取るべきだろうか。標的型サイバー攻撃への対策には、インターネット境界面における「入口対策」「出口対策」、組織内部における「エンドポイント対策」など様々なアプローチが存在し、それらを組み合わせて組織を守る専門性が求められる。また、ひとたびサイバー攻撃が発生した場合は、それを迅速に検知したうえで、数多くの関係部署とコミュニケーションをとり、適切に対応を実施していく必要がある。このようにサイバー攻撃への対策には、高い専門性とコミュニケーション能力を兼ね備える必要がある。

NOTE

1) 2015 cost of data breach study, IBM, 2015
2) 疑似マルウェアを添付した標的型メールを、お客様組織に対して実際に送付することで、サイバー攻撃に対しての気づきを与え、組織のセキュリティレベルを向上させるサービス。
3) サイバーセキュリティ傾向分析レポート2015, NRIセキュア, 2015
4) 企業における情報セキュリティ実態調査2014 第2版, NRIセキュア, 2015

そのような背景のもと、昨今のサイバー攻撃対策のトレンドと言えるのが、CSIRT（Cyber Security Incident Response Team）の設立である。CSIRTはその名の通り、サイバー攻撃の監視、検知、および発生時の対応を目的とするチームである。近年、多くの企業で組織内CSIRTが設立されている。当社が実施した上場企業を中心とする660社情報システム・セキュリティ担当者へのアンケート調査によると、組織内にCSIRT機能を有する企業の割合は2012年に8%であったものが、2013年には22%、2014年には42%にまで増加している[4)]。日本企業においてサイバー攻撃が自社に与えるリスクが認識されてきた表れといえるだろう。

経営層はサイバー攻撃のリスクを認識できているか

アンケート結果からも、情報システム担当者の現場層ではサイバー攻撃のリスクは認識されてきていると考えられる。しかし、日本の経営層はどうだろうか。先に紹介した標的型メール訓練のうち、対象者が役員であるデータを抽出した結果、対象者763名の開封率は29%に上昇した。今回集計したデータは一般従業員、役員の区別なく、同一条件で訓練を実施しているが、この値は先の一般従業員の開封率19%と比較して、およそ1.5倍程度高い値である。

もちろん標的型メールを開封することが、即企業の経営リスクにつながるわけではなく、万一、マルウェアを実行してもアンチウィルスソフトが感染を防いでくれる可能性もあり、万一、感染したとしても、マルウェアが実行する外部との通信から検知、対策できる可能性もある。しかし、サイバー攻撃が経営に与えるリスクを十分に認識できている人間であれば、標的型メールは開封することなく対応するだろう。この結果は、日本の経営層において、サイバー攻撃が経営に与えるリスクが充分認識されていない可能性を示している。

全社一丸の体制構築を

CSIRTは設立がゴールではない。CSIRTが効果的に動けるようになるまでには、十分な人的リソース、金銭的リソースをかけて、内部の人間、そして組織を育成する必要がある。しかし、企業によっては、「旧来の情報システム部にCSIRTの役割と責任が与えられたが、特にリソースの補充はない」「所属者の全員が事業部との兼任であり、ほぼCSIRTの活動はできていない」等の理由により、設立はしたものの、十分な活動ができていない例も見受けられる。CSIRTをはじめサイバー攻撃に関する対策は、企業の中ではコストとみなされることが多い。コスト部門に資源を集めるには、経営層の十分な理解とサポートが必要となるだろう。

サイバーセキュリティに限らず、想定リスクを上回る投資はすべきではない。しかしサイバー攻撃のリスクは年々拡大の一途をたどっている。サイバー攻撃から自社を守るためにも、今一度リスクを見つめなおし、経営層も含め全社一丸となったセキュリティ体制を構築することが求められているのではないだろうか。

Writer's Profile

寺村 亮一 Ryoichi Teramura
NRIセキュアテクノロジーズ　テクニカルコンサルティング部
セキュリティコンサルタント
専門はサイバーセキュリティ
focus@nri.co.jp