セキュリティトレンド

標的型メール攻撃対策の勘所

メールを用いて特定の組織や人の情報を搾取する諜報活動として「標的型メール攻撃」が急増している。攻撃の対象は全業種に渡り、金融機関も例外ではない。攻撃の対象を調査しつくした上で行われる本攻撃への対策を進める際の勘所は、システム・人の両面から、いかに効率的に現行対策の問題点を把握できるかである。

「標的型メール攻撃」とは急増するサイバー攻撃の一種である。攻撃者が特定の企業・組織、個人に関係者を装い電子メールを送付し、受信者がメールに記載されたURLにアクセス、または添付ファイルを開くと、情報漏洩等に繋がるウイルスに感染する仕組みが施されている。メールを利用する特性上、巧妙に細工された個人宛の標的型メールによる攻撃は発見されにくく、攻撃が成功すると機密情報を盗まれる事例も多い。昨今のサイバー攻撃の中でも特に注意すべき攻撃の一つである。

当社が行った調査[1]では、「標的型攻撃を経験したことがある」と回答した企業は全体の20.7%、このうち「過去1年以内に経験」は82.9%に上り、30.7%の企業では「これまでに受けた標的型攻撃による実被害」があった。

標的型メール攻撃への対策

内閣官房情報セキュリティセンター（NISC）[2]はサイバー攻撃による脅威を分類・分析した「重要脅威カタログ」[3]で、標的型メール攻撃を重要脅威の一つとしている。現場レベルでの具体的対策法は、情報処理推進機構（IPA）[4]がガイド[5]を公表している。筆者はその作成に携わったが、ここでその内容を紹介したい。

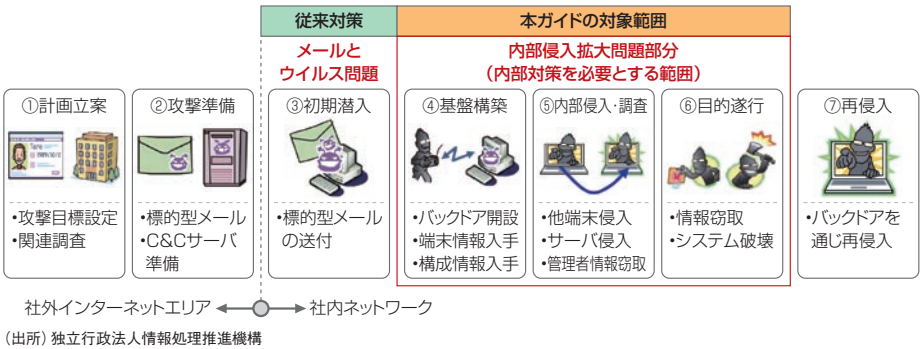
図表は標的型メール攻撃における7つの攻撃段階を示している。一昔前の多層防御の考え方では、外部からの脅威をブロックすることを目的とした「従来対策」（③）のみに頼ってきた。しかし標的型メール攻撃が出現し、「内部対策」（図表④～⑥への対策）を考える必要が出てきた。外部からの潜入の防止が難しくなり、組織内部から重要情報を漏えいさせない方策が極めて重要となったからである。

IPAのガイドでは、標的型メール攻撃で実際に利用された検体を用いた実機検証による分析結果も加え、「内部対策」として、通信経路における8つの対策[6]をまとめている。これは、標的型メール攻撃を受けたユーザがマルウェアを実行してしまったとしても、2重3重の対策（多層防御）を用意しておくことで、標的型メールをトリガーとした高度なハッキングによる重要情報の漏洩を防ぐことを目的に検討された対策である。ただし、「内部対策」を行うために業務で利用しているネットワークの通信要件を変えることは、本来許可されていた業務通信をブロックしてしまうリスクが伴う。このため、「内部対策」を実施するには、業務要件を十分に考慮したうえで対策設計を施す必要がある。

可能性はゼロではない

金融情報システムセンター（FISC）[7]が昨年発行した

図表　標的型メール攻撃　攻撃段階と対策の範囲



（出所）独立行政法人情報処理推進機構

NOTE

1) NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2013」
http://www.nri-secure.co.jp/security/report/index.html
2) 2005年4月、情報セキュリティ対策の中核組織の必要性を重視して日本政府が設置した、我が国における情報セキュリティ政策の基本戦略を遂行する機関。
3) 内閣官房情報セキュリティセンター「各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討（リスク要件リファレンスモデルドキュメント集等の作成）総括報告書」2010年3月
http://www.nisc.go.jp/inquiry/pdf/1_soukatsu.pdf
4) サイバー攻撃情報などの収集・評価・分析や、対策方法の提案・実施・普及、ソフトウェアの信頼性向上に向けたツール群の提供、情報処理技術者試験の実施等によるIT人材の育成などを推進している。
5) 「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」2011年11月、「『標的型メール攻撃』対策に向けたシステム設計ガイド」2013年8月
http://www.ipa.go.jp/security/vuln/newattack.html
6) 8つの対策：バックドア通信を止める対策として、「サービス通信経路設計」「ブラウザ通信パターンを模倣するhttp通信検知機能の設計」「RATの内部proxy通信（CONNECT接続）の検知遮断設計」、システム内拡散を止める対策として、「最重要部のインターネット直接接続の分離設計」「重要攻撃目標サーバの防護」「ソフトウェア等でのVLANネットワーク分離設計」「容量負荷監視による感染活動の検出」「P2P到達範囲の限定設計」
7) 金融情報システムや電子商取引などについての調査・提言を行なっている。

「金融機関等コンピュータシステムの安全対策基準・解説書（第8版追補）」では、標的型メール攻撃への対策として、従業員に対する標的型メール訓練や教育等の定期的実施を奨励している。しかし、訓練や教育は、攻撃によるリスクを低減できるが、完璧な防御策ではない。標的型メール攻撃は、標的となる企業を攻撃者が徹底的に調査し尽くして攻撃してくる。つまり、本攻撃に対して「人」の面で耐性を高めたとしても、従業員が標的型メールに添付されたマルウェアを実行してしまう可能性を「ゼロにすることはできない」のだ。

ひとたび攻撃の対象となり、高度な標的型メール攻撃を受けた場合は、マルウェアをトリガーとした不正侵入が起きる危険性が確実に高まる。ゆえに、標的型メール攻撃（による高度なハッキング）から重要情報を守るには、まず「システム」面の耐性をチェックすることから進めるべきである。そのうえで、従業員の啓蒙・訓練によって気付きを与える演習を継続し、「人」の練度を高めていくことで、サイバー攻撃に対する一段上の組織耐性を整備するべきであろう。

外部ベンダーを活用した「内部対策」状況のチェックの効率化

「内部対策」を行うためには、稼働中の既存のネットワーク設計を見直し、リスク分析を行う必要があるが、システム運用担当者や運用委託先にとっては、莫大な時間と労力（コスト）がかかる作業である。この問題の解決策の一つとして、当社では「システム」と「人」の両面から標的型メール攻撃への耐性を確認するサービスを提供している。

「マルウェア感染後の侵害シミュレーション」は、実機を用いてハッカーが利用する一般的な侵入行為をシミュレーションし、本攻撃におけるマルウェア感染後の脅威に対する「システム」面の耐性を確認できる。「人」への耐性は「標的型メール攻撃被害シミュレーション」で確認する。前述したFISCの安全対策基準・解説書の「標的型メール訓練や教育」に該当するものである。従業員に疑似標的型メールを送り、添付ファイルの開封状況をチェックし、状況に沿った教育を行うことで、本攻撃に対する従業員の耐性を上げることが目的である。

これらのサービスを活用することで、短時間に少ない労力（コスト）で、「人」と「システム」の両面における現行対策の問題点を効率よく確認することができる。

前述のIPAのガイドには、「攻撃を解析する専門家とシステム全体を設計・運用する専門家と連携することで、現実の組織において攻撃からどのように守ると効果的であるかを詳細に検討することができます。」と記載されている。サイバー攻撃は巧妙化、高度化の一途を辿っており、攻撃の対策を行っている企業であっても、すでに内部で攻撃が進行している状況を把握することさえ困難な状況にある。専門家に相談できる環境は、安全な情報システムを構築する上で重要な要素となるはずである。是非、自社の状況に合わせ、情報セキュリティベンダーを活用し、堅牢なシステムを構築して頂きたい。

Writer's Profile
小林 克巳 Katsumi Kobayashi
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