トピックス

標的型攻撃対策としてのIT全般統制
―侵入を前提とした内部統制による対応策―

今や全ての企業にとってのリスクとなっている標的型攻撃。侵入されないことへの対策のみフォーカスされがちだが、全ての攻撃を防ぐことは難しく、多層防御の観点から侵入された場合を前提とした対策を考える必要がある。本稿ではこれまで一部の企業にのみ求められてきた内部統制のうち、IT全般統制の仕組みが有効な対策となり得ることを紹介する。

NRIセキュアテクノロジーズ ソリューションビジネス三部
上級セキュリティエンジニア
橋本（はしもと）　淳（じゅん）
専門は特権ID管理・アクセス制御ソリューションの企画、開発

全企業のリスクである標的型攻撃

標的型攻撃とは不特定多数ではなく特定の企業、組織の情報を搾取する目的で行われるサイバー攻撃のことである。その攻撃手法は日々巧妙化しており、防御の困難さが増している。特に近年では、標的型メール攻撃と呼ばれる巧妙に偽装されたメールを起点とした攻撃が目立っており、実際に不審なメールを受信された読者も多いのではないか。

一見すると差出人は取引のある企業のドメインからのもので、文面も自然な日本語で、本文の最後には署名までついている。部署名も実在のものであろう。さらにPDFなどの通常のドキュメント形式に見えるファイルが添付されており、自然な誘導で当該ファイルを開くよう仕向けられている。

しかしながら、実際の送信元は海外のレンタルサーバーであったり、巧妙に偽装された文面であったり、通常のドキュメントファイルを装った実行形式のファイルであったりする。そしてファイルを開いた時点でマルウェアに感染、C&C（コマンド＆コントロール）サーバーとの通信が開始されて遠隔操作、侵入を許してしまう。そこからひっそりと偵察が行われ、重要情報に到達した際にはこれが抜き取られ、攻撃者の目的が達成されるのである。もちろん侵入手法はこれだけにとどまらないが、この手口が目立つのは各種報道によっても明らかである。

侵入を防ぐ対策から侵入を前提とした多層防御への意識転換

この標的型攻撃に対する関心は極めて高く、IPA（独立行政法人情報処理推進機構）が公表している「情報セキュリティ10大脅威2016」では、組織に対する脅威として1位に位置付けられている。そのためほとんどの企業、組織が対策にすでに着手しており、最優先項目として外部からの侵入防止やウイルスを検知するための対策を実施している。

このように侵入を防ぐ・検知するための対策はすでに浸透している感があるが、セキュリティ対策には多層防御という基本的な考え方がある。つまり侵入を前提とした対策を考

えるべき段階に入っているのだ。

IT全般統制によるセキュリティ対策

侵入を前提とした対策を考える際、内部統制の一部である「IT全般統制」の仕組みが有効な対策となる。米国のSOX法に準じて2008年度から適用が開始された「金融商品取引法」は、情報システムに関する内部統制が明確な形で取り入れられている。その内部統制は「全社統制」「業務処理統制」「IT全般統制」に分けられ、このうちIT全般統制では全社統制で策定された戦略やルールや、業務処理統制で定義された業務統制などが、適切に実行される環境を構築、維持管理することが求められる。定めたルールを、当たり前に実施することはセキュリティ対策において重要だ。ここではその具体策例とセキュリティ対策としての効果を見ていきたい。

①情報資産の棚卸し

守るべき情報資産（重要情報）を明確にする目的で、棚卸しを行い、各資産に対しての侵害時リスクを明確にする。

②洗い出した資産保護対策の定義

次に資産を守るための具体策をリスクに応じて定義する。重要情報が格納されている基幹系ネットワークと情報系ネットワークとを分離して強力な認証、権限に応じたアクセス制御を行い、さらにアクセスログを取得して定期的にモニタリングする、などが挙げられる。

③定義した対策の実装・運用

②で定義した対策を各資産へ実装する。また、対策が有効に機能しているかどうかの定期的な確認も必要である。

これらの対策が整っているIT全般統制が機能している環境であれば、仮に攻撃者に侵入を許したとしても以下のような防御や検知が可能となる。

- ネットワーク分離による不正防御
- アクセス制御（ユーザー認証、申請・承認など）による不正防御
- 定期的なログモニタリングによる迅速な不正検知

ソリューションを有効に活用する

これらの対策をいかに低負荷で効率良く、かつ確実に運用するかが極めて重要である。そのためには、細かなアクセス制御やログ管理が可能なソリューションやサービスの活用が有効である。具体的には分離されたネットワーク間でゲートウェイとして動作し、確実なアクセス制御、ログ取得が可能となるソリューションが望ましい。機能として強力なユーザー認証、権限・ロール管理や申請承認によるアクセス制御の実現に加えて、「抜け漏れ」のないログ取得やレポーティングの実現も不可欠だ。このようなソリューションの活用により、アクセス制御を強制し、かつそれらを効率的に管理、モニタリングすることが可能となる。

NRIセキュアテクノロジーズでは国内250社以上の実績があるソリューション、特権ID管理システム「SecureCube / Access Check」を持ち、豊富な実績を基に実効性、効率性を両立させた提案に力を入れている。■