気になる！技術・サービス

情報セキュリティの動向

1．はじめに

クラウドサービス提供の動きが本格化するなど、インターネットを前提としたシステム利用が多くなる中で、情報システムにおけるセキュリティ対策はますます重要になってきています。この数年におけるマルウェアの動向など、改めて情報セキュリティについて考えてみます。

2．情報セキュリティの基本

最近のセキュリティトピックスとして次の３つを検証します。

(1) インターネットからの「標的型攻撃」
(2) クラウド利用におけるリスク
(3) スマートフォンの業務利用について

3．インターネットからの「標的型攻撃」

インターネットの利用に伴う外部からの攻撃は年々高度化してきており、その対応には最新の注意が必要です。特に最近では「標的型攻撃」と呼ばれる手法で大きな被害が出ています。「標的型攻撃」は、複合的な手法を用いて、計画的かつ継続的に攻撃されることが特徴です。「標的型攻撃」は一般的に次の３つの段階があり、早い段階の対応が被害防止に有効です。

最初は事前調査です。通常の公開サーバの脆弱性を調査する方法と、個人のメールアドレスを探し出してニセメールで騙すことで内部から調査する手法があります。インターネットの法人会員や論文発表の問合せ先などに、会社のメールアドレスを公開している場合などは簡単にターゲットとなります。同窓会名簿なども事前調査に利用されることがありますので、会社のメールアドレスを外部に公表する場合には、ピリオド「.」や「@」を大文字にするなどの工夫も防止効果があります。

次が「初期潜入」です。関係者を装ったメールの送信などで返信を要求したり、関係するURLへの接続を促すなどの手法があります。この段階では、最近のフィルタリング製品である程度防御することができますが、そのようなメールに対する注意喚起や、対応方法の周知・徹底を定期的に実施して関係者の意識を高めておくことが防御としては最も有効です。

最後が「攻撃基盤の構築」です。パソコンをウィルスに感染させることで、外部との不正な通信が行えるようにします。乗っ取られるパソコンの多くは家庭パソコンですが、もし、企業のパソコンが乗っ取られてしまうと企業の信頼失墜や犯罪に巻き込まれるなどのリスクが伴います。

4．クラウド利用におけるリスク

グループウェアなどの情報共有機能においてクラウドサービスの利用が立ち上がりつつあります。しかし、その利用の普及と比例するようにクラウド利用におけるトラブルも発生しています。

＜事例１＞クラウド提供事業者によるデータ消失

システムの機能強化を行うための作業において、作業ミスにより大量のデータを消去してしまう事件が発生しています。

＜事例２＞サービス事業者の内部からの情報漏えい

サービスを提供している事業者で勤務していた関係者が、顧客のメールアドレスを流出させる事件が発生しています。

２つの事例は、クラウドサービスを利用すれば、最新のセキュリティを施した安心したシステムの利用が簡単に実現できるという、クラウドサービス利用の理想的な姿を現実に示す内容でした。セキュリティレベルを高度に維持するためにはコストがかかります。多くのユーザ情報をあずかるクラウドサービスにおいては、より高度なセキュリティを確保するためにコストがかかるはずであり、そのサービスには料金が必要になることは一般的に想定されます。安価なサービス料金の場合は、セキュリティレベルやバックアップサービスの範囲などを事前確認することの重要性が認識されつつあります。

5．スマートフォンの業務利用について

業務におけるスマートフォンの利用については、全ての社員にスマートフォンを提供できない、個人のスマートフォンでは利用環境やバージョン管理が担保できないなどの理由で、普及がなかなか進みません。しかし、実態としては私物のスマートフォンにてスケジュール管理や携帯電話番号やメールアドレスを管理している場合が多くあります。

(1) スマートフォンはパソコンと同等

スマートフォンは、パソコンと同程度の機能が利用できますが、逆にマルウェアのターゲットであるという認識を持つことが必要です。つまり、ウィルスに感染しているスマートフォンを利用して社内のグループウェアなどを使うと、社内にウィルスが蔓延する場合も想定されます。

(2) スマートフォンとクラウドサービス

そこで、クラウド環境においてグループウェアなどの情報共有サービスの利用が検討されますが、まだ、スマートフォンを前提としたクラウドサービスは本格的な利用が始まったばかりです。前述のようにサービスを比較する場合には、セキュリティの担保がどこまで規定されているかを確認する必要があります。

(3) 機器としてのセキュリティリスク

また、スマートフォンは機器としての特徴により、技術的に完全にデータ消去を行うことが困難な端末です。このため、個人情報や社内機密資料などについては情報共有の対象外にするなどの対応が必要です。

6．今後の情報セキュリティに関する方向性

これまでも情報セキュリティに関する法律だけでなく、多くの基準やガイドラインが公表されてきましたが、日本は情報セキュリティ対策の分野で遅れていると言われています。その理由の一つが、これまでは自治体システムと企業システム、通信と機器といった個別の対応が検討されてきたことにあると考えられています。今回「国民を守る情報セキュリティ戦略」において大きな方針が示されました。また、平成24年５月には不正アクセス禁止法が改正され、多様化、高度化する不正アクセスの手法にも対応できるようになりました。

具体的な実現には数年の時間が必要と思いますが、情報セキュリティにおいても世界に先進技術を誇れるようになることを期待します。