水野施設長の介護マネジメント塾
3 月号

ソニー情報流出事件に学ぶ

はじめに

皆さん、こんにちは。

以前ソニーが、最大約 7700 万人の個人情報が漏洩したと発表。さらには、米国子会社でもハッカーの不正侵入を受けて、個人情報が流出した恐れがあると発表し、これで延べ 1 億人を超えるかというネットワークビジネス史上最大最悪規模で、途方もないスケールの個人情報流出事件に発展したことから、今回は、その問題点と、対応策についてお話ししていきたいと思います。

ソニー問題とその原因

ソニー情報流出事件の原因は、不正アクセスということがわかっており、その手口についても判明しているといいますが、根本的な原因は、アプリケーションサーバーの脆弱性に対処していなかったことにあることもわかっています。

脆弱性とは、脅威の発生を誘引するようなセキュリティ対策上の欠落点のことで、この対処がされていなかった点が問題になっているのですが、一般的に対処は難しく、わかっていても直すためのプログラムがなかったり、システムの更新ができなかったりなどの問題で対処できないこともあるものです。

しかし、ソニーは過去にプレイステーションネットワークに対する DDos 攻撃（データを集中的に送って利用不能にする攻撃）などによって、被害を受けていることから、わかっていて更新できなかったのではなく、脆弱性に対処していなかったことが大きな問題なのです。

脆弱性は別の言い方をすれば、本来、セキュリティ対策が導入されるべきなのにまだ導入されていない部分、組織的対策や技術的対策から不十分な部分であることから、問題を放置していたことになるわけで、「世界のソニー」とまで言われている巨大なネットワークを運営している大企業にもかかわらず、脆弱性に対処していなかったのは、素人目に見ても疑問符をつけざるを得ないといえます。

個人情報漏洩と対応策

内部の機密情報が外部に漏れることを「情報漏洩」、特に個人情報が漏れることを「個人情報漏洩」ということはいうまでもありませんが、インターネットを中心とした情報化社会は利便性を高める一方で(個人)情報漏洩の危険を高めており、データを預かる組織は、内部データを安全に保護する仕組みを持っていなければなりません。

例えば、PC や USB メモリの紛失、ウィルス感染によるデータの流出などは個人の不注意や管理の仕組みに問題がある場合に発生します。こういうケースでの流出をシステムで抑制することには限界があり、最終的には組織内のルールの策定と遵守の徹底で予防するしかありません。

現実的には USB メモリの使用禁止や PC およびメモリの持ち出し禁止を徹底し、業務用 PC を持ったままでの外出先からの直帰を禁止するなど「○○の禁止」という事項が並ぶようになるため、結局は守る側の意識の高さに任せるしかないというのが現状です。

データの悪用を目的として、故意にデータを持ち出すケースも多々あります。PC やメモリの盗難など物理的に何かを持ち出すこともあれば、ハッキングのようにインターネット経由で不正にデータにアクセスする方法も採られます。また、データの不正持ち出しについては悪意を持った第三者が関係する場合を考えがちですが、実際には情報漏洩の 80%が内部の人間が関与しての犯行と言われており、組織は、スタッフのデータアクセスに関しても十分な注意を払う必要があります。

データ保護の最も分かり易い方法として、データにアクセスする必要のない人間をデータの置かれている場所に物理的に近寄らせないことや、社員証を見える場所に携帯することで社員と外部者を区別できるようにするという基本的な処置に加えて、システム的にデータ漏洩を防止する方法として、外部からのネットワークアクセスを遮断するためのファイアウォールがあり、実際に組織のデータに辿り着くまでにサーバ認証やユーザー認証の仕組みを設けることで、不正アクセスを防止することが可能になります。また、データを暗号化しておくことにより、データを持ち出す事ができたとしても内容がばれないようにしておくことも有効な方法です。

また、不正アクセスを未然に防ぐという考え方と同時に、万が一の事故や事件が発生したときのためにアクセスログを残しておく事も検討すべきです。あるファイルが流出するか不正な改竄がなされたときに、そのファイルに対する最終アクセスや最終更新がいつ誰によって行われたのかをトレースできる仕組みが必要になってきます。

このような収集機能を持つソリューションは、今ではソフトウェアでもアプライアンスでも複数存在しているので、事故後の対応をスムーズにして混乱を最小限に抑えたいならば、導入を検討すべきといえるのではないでしょうか。

今後の課題

ロシア・モスクワに本社を置く コンピュータセキュリティ会社カスペルスキーのホームページで「セキュリティの総括と予測を発表～脅威の巧妙化が新たなレベルに達した 2010 年とサイバー犯罪の新概念「スパイウェア 2.0」が生まれる 2011 年」というレポートが報告されています。

レポートでは、段々とマルウェアとかも進化しており、今後はソーシャルネットワークや iPhone、Android を標的とした脅威も間違いなく出現してくると断言しています。

今までは、一般的には Windows や Office 等のマイクロソフト製品の対策というのがソフトウェアの脆弱性対策と考えられていて、マイクロソフト製品以外は後回しにしていた企業もありますが、すでに、昨年にもありましたが Adobe 製品や Apple 製品の脆弱性を狙うマルウェアなどが増えてくるでしょう。これは、利用頻度が高い製品は大手企業だけでなく中堅・中小企業でも多く使われています。つまり、企業や個人で利用頻度が高く、取り扱いも容易な製品は、攻撃対象になり易いことを意味しているわけですから、そういった製品の脆弱性が発見された時には速やかにアップデートを行うようにしていくことが大切だと言うことです。

ITへの依存度を高め、文明の利器の恩恵を最大限に享受しようとする動きの一方で、法整備や安全面への技術対応が追いつかず、個人情報や企業機密情報の漏洩事故、情報システムへの不正アクセスやコンピュータウイルスの感染等による情報システムの停止、さらには、天災・人災による情報システム停止に伴う社会機能麻痺への不安など、様々な脅威に晒されることになってしまいました。

そして、私達は情報化社会の中で生き抜くために、それら様々な脅威から身をかわす術を身に付ける必要に迫られ、情報セキュリティを意識せずにはいられない環境に置かれることになったということを、認識しなければならないということを、福祉施設、事業所においても例外ではなく、ソニー情報流出事件で学ばなければならないのではないでしょうか。

[参考サイト]

Kaspersky Lab：セキュリティの総括と予測を発表～脅威の巧妙化が新たなレベルに達した 2010 年とサイバー犯罪の新概念「スパイウェア 2.0」が生まれる 2011 年～
http://www.kaspersky.co.jp/news?id=207582671