

セキュリティ最前線 (2008年3月7日号)

目次:

- 1. 個人情報の流出:激増する情報漏えいの恐怖 P.1
- 2. いかにネットワークからの情報流出を防ぐか P.3
- 3. 2007年の主要な情報漏えい事件 P.5

1.個人情報の流出:激増する情報漏えいの恐怖

個人情報漏えいに関する事件は、米国では増加し続けており、個人や企業の双方において一件につき31,000米ドルもの被害額に及ぶといわれています。[*1] 個人情報漏えいは、財布やクレジットカードの請求書等の盗難により発生しますが、今日、企業の顧客情報が大量流出するような脅威にまで発展し、事態は非常に深刻化しています。業界監督機関 Attrition.org は、2007年度に1億6200万件にも及ぶクレジットカード情報や社会保障番号(Social Security Number)の被害があったと報告しています。これは、前年度の4900万件という同報告の被害件数に比べても激増していることが分かります。また、ITRC (Identity Theft Resource Center)では、2007年12月18日までに米国で7900万件以上もの情報漏えいの被害があったと報告しており、これは、2006年に報告された被害数2000万件のおよそ4倍となっています。[*2]

情報漏えい:広範囲に及ぶ問題

情報漏えいは、企業と顧客双方にとって非常に深刻な問題です。米国では毎年、ソフトウェア、製品デザイン、契約書、設計図、製剤法、ビジネスプラン等に関する取引上の機密情報等が不正に複製流出し、知的所有権上、数十億米ドルもの被害が報告されています。また驚くべきことは、こうした企業関連の被害のほとんどが、社内の重要人物が原因であるという点です。こうした人々の方が重要なデータに簡単にアクセスできるということも一因のようです。Ponemeon Instituteでは、情報漏えいの78%は、社内の重要人物に起因していると報告しています。[*3]

企業では、VPN(Virtual Private Networks)や、ファイアウォール、ネットワークモニタリング等のセキュリティ対策を講じて、企業専有情報への外部からの不正アクセス防止に努めてきました。しかしながら、こうした対策も内部者の犯行による脅威には無力です。情報の流出は、むしろ、財務情報の不正入手のような内部犯行、顧客情報の入ったノートPCやUSBメモリを社員が紛失するような事故でもたらされる場合が多いようです。

こうした内部犯行や不注意による事故のほかには、情報流出が発生するケースとしては、ハッカーたちによる企業ネットワークへの侵入や、実際に企業の敷地内に侵入してデータを入手するという盗難の場合もあります。また、こうした犯罪者たちは、企業からノート PC や USB メモリを不正入手するだけでなく、盗まれたデータを別の犯罪者たちから購入する場合があります。言うまでもなく、サイバー犯罪者たちは、不正プログラムを利用した情報収集活動も行います。この場合、収集した情報を外部へ送信する際にも同じ不正プログラムが利用されます。

オフィスと自宅の境界があいまいに

各種メッセージングシステムや、無線 LAN、USB メモリの利用が激増し、企業の機密情報保護は非常に困難になってきました。また、社員の移動頻度や在宅勤務者数が増加するにつれ、オフィスと自宅の境界もあいまいになり、モバイル機器の使用、機密情報がメールを介して双方を行き来するといったことも頻繁化してきました。こうした状況において社員や請負業者による企業情報の漏えいや紛失をいかに防ぐか。これは今日の企業にとって非常に大きな問題となっています。

セキュリティの問題

今日の“バーチャル”なオフィス空間においては、業務用メール、Web メール、FTP、インスタントメッセージ（IM）、Wi-Fi、USB ディスク、デジタルカメラ、携帯電話、PDA、ノート PC、録音・録画可能な CD/DVD-RAM、iPod 等、多種多様なモバイル機器があふれています。このような状況においてセキュリティを確実にすることは至難の業とさえいえます。この点からも総合的なソリューションの導入が非常に重要になってきています。こうしたソリューションの導入により、コンピュータ上の各ポート、企業内の各エンドポイント、社内および公共のネットワーク等から社内の機密情報や顧客情報等が流出するのを阻止できるからです。

参考：

*1) “Identity Fraud Trends & Patterns,” October 2007, Center for Identity Management and Information Protection (CIMIP) at Utica College, NY,
<http://www.utica.edu/academic/institutes/cimip/publications/index.cfm>.

*2) Mark Jewell, AP, “Groups: Record Data Breaches in 2007,”
<http://attrition.org/news/content/08-01-03.html>.

*3) Eric Sinrod, CNET News, “Going after the Bigger Insider Threats,”
http://www.news.com/Going-after-the-bigger-insider-threats/2010-1029_3-6117692.html, September 20, 2006.

2. いかにネットワークからの情報流出を防ぐか

いかに情報漏えいに対処するかということは、今日多くの企業にとっての非常に重要な問題となっています。実際、2007年に実施された King Research の調査では、「もし大規模な情報漏えい事件が発生したら自分たちの仕事に深刻な影響を与えるだろうとほとんどの IT 専門家が考えている」と報告しています。同時に「IT 専門家たちは、こうした情報漏えい事件に対処するための設備が個人レベルでも企業レベルでも不十分であると感じている」とも報告しています。また、同調査に回答してくれた 250 人の IT 専門家たちのほぼ 3 分の 4 が、「自分たちが働いている企業で大規模な情報漏えい事件でも発生したら職を失ってしまうだろうと心配している」とのことです。[*4]

各種規制に関する問題

企業が情報流出を防ぐ理由には、顧客情報保護の問題に加えて、政府関係の各種規制順守に関する問題があります。「グラム・リーチ・ブライリー法 (Gramm-Leach-Bliley Act)」、「EU データ保護条令 (European Union Directive on Data Protection)」、「サーベインス・オクスレー法 (Sarbanes-Oxley)」、「医療保険の携行と責任に関する法律 (HIPAA: Health Insurance Portability and Accountability Act)」といった各種規制は、これらを順守せずに情報流出が発生した場合、罰金や訴訟の原因になりかねないばかりか、企業のイメージが損なわれることにもなります。

多層的な防御戦略

たった 1 つの製品や技術でデータ流出阻止が万全ということは決してありません。最善策としてお奨めできることは、利用中に情報漏えいの可能性がある各箇所を監視できるような防御法を設置することです。この点からもトレンドマイクロでは、理想的には以下の全てをカバーできる多層的な防御戦略を推奨しています。

1. データ流出を防ぐソフトウェア: 工作中に扱う情報が機密情報であることを社員にリアルタイムで知らせてどのような情報処理ポリシーを適用すべきかを判断してくれるソフトウェアのことです。トレンドマイクロの場合、「Trend Micro LeakProof™ 3.0」[*5] がこれに相当します。このソフトウェアは、「DataDNA™」という高精度のフィンガープリント法とエンドポイント実行を組み合わせることで情報流出を阻止します。情報漏えい防止に携わる機関が、ポリシー施行や情報内容のフィルタリングを代行し、同時に「DataDNA™」のサーバが、ポリシー運営や違反行為に関する監視を行います。
2. 暗号化: 情報保護のためには最も重要な手段の 1 つです。これにより、機密情報が外部者の手に渡ってしまうことを阻止できます。ただし暗号化の手段は、言うまでもなく、暗号を知る内部者には無力です。内部者が誤って情報を紛失、あるいは内部者の犯行によって情報が流出するような場合には役に立ちません。
3. ウイルス対策: 不正プログラムも、社員や請負業者の不注意による情報流出と同様、大きな損害を与える要因となります。こうした点からも、ウイルス対策製品やサービスを社内ネットワークおよびその周辺機器内にインストールしておくことは不可欠です。これにより、不正プログラムのシステムへの侵入を未然に防ぐことができます。
4. アクセス制御: 企業においてアクセス制御を正しく実行することは、情報流出を防ぐうえでも非常に重

要です。ネットワーク、アプリケーション、システム等へのアクセスを特定の許可された社員のみを制限しておくことで、情報流出のリスクを減らすことができます。

5. 業務規定: 社内の業務規定を明確にし、特定の機密情報にアクセスする社員には厳守させ、同時に社内全体に周知させておくことでも、情報流出のリスクを減らすことができます。
6. 社員教育: 情報漏えいの多くは、社員の不注意により発生しているという事実からも、社員教育を徹底し、厳守すべき手順を明確に設定することは極めて重要です。企業内で情報漏えい問題に関する危機意識を促して社員に自覚させることは、多層的防御における不可欠な要素でもあります。

参考:

*4) Enterprise Networks and Servers, "IT Professionals Fear Security Breach Could Cost Them Their Jobs, According to Recent Survey,"

<http://www.enterprisenetworksandservers.com/newsflash/art.php?724>, April 30, 2007.

*5) Trend Micro™ LeakProof™ 3.0

<http://us.trendmicro.com/us/products/enterprise/leakproof/index.html>

3. 2007 年の主要な情報漏えい事件

以下は、2007 年、世界的に報道された大規模な情報漏えい事件です。

ボーイング社の情報漏えい事件

ボーイング社の社員による犯行を伝える警察の報告では、犯人は社内のコンピュータの背後に USB メモリを密かに接続し、USB メモリ本体を犯人の机の引き出しの中に隠していたとのことです。[*6] この事件からも、リムーバブルドライブやその他の携帯機器の蔓延により情報流出の阻止がいかに困難になったかを理解することができます。

Fidelity NIS 社の情報漏えい事件

情報漏えいの検出を避けるため、犯人である社内の IT アドミニストレーターは、収集した情報をメールで外部に送信するのではなく、リムーバブルドライブを利用して外部に持ち出したとのことです。[*7] この情報漏えい事件は、Fidelity NIS 社の関連会社である Certegy Check Services 社において発生しました。この事件では、内部社員の犯行手口がいかに巧妙化してきているかを物語っています。この場合、犯人の IT アドミニストレーターは、社内のセキュリティ対策にメールおよびネットワークのフィルタリングが設置されているのを知っており、これによる検出を避けるため、別の手段を講じたということです。

ファイザー社の情報漏えい事件

2007 年 7 月、ファイザー社の社員によりファイルが奪われ、34,000 人が個人情報偽証の危険にさらされました。しかもこれは同社で過去 3 カ月に生じた三度目の情報漏えい事件でもありました。この事件により、社員の氏名、社会保障番号(Social Security Numbers)、さらには住所、電話番号、ファックス番号、メールアドレス、クレジットカード番号、銀行口座番号、パスポート番号、運転免許証番号、軍隊認証番号(Military Identification Numbers)、誕生日、署名、退職理由等の情報までが流出しました。[*8]

GAP 社のセキュリティギャップ

2007 年 9 月、GAP 社の請負業者のノート PC が盗難に遭い、同社の店舗採用に応募した 80 万人もの履歴情報が流出し、個人情報偽証の危険にさらされました。同社は、被害を受けた応募者を特定し、彼らに対して一年間無料で、クレジットカード使用履歴の監視、個人情報偽証に対応するためのサポート、さらに 24 時間のオンラインヘルプデスクサービスを実施するとの声明を発表しました。[*9]

英国政府での情報漏えい事件

2007 年、英国の政府機関 HMRC (HM Revenue & Customs) では、2500 万人にも及ぶ児童手当受給者の機密情報が含まれた CD が紛失しました。ここには、受給者の氏名、住所、誕生日、国民保険番号等、HMRC 児童手当データベース内の情報のほとんどが含まれていました。また、ここには、700 万人以上の保護者や介護者たちの銀行口座等の情報も含まれていました。[*10]

内部犯行の増大が今日の情報漏えい事件の蔓延と深刻さを示していることが、最近の調査でも明らかになっ

ています。市場分析を行う Enterprise Strategy Group が 2007 年 6 月に実施した調査では、全企業のほぼ 3 分の 1 が過去 12 カ月の間に社内で情報漏えいを経験しているといえます。さらに驚くべきことには、調査に協力したセキュリティ専門家の 10% もの人々が、過去 12 カ月の間に社内で情報漏えいが発生したかどうかさえ定かでないという回答しているのです。

また同調査では、回答者の 40% が、情報漏えいによりデータ紛失や、アプリケーションの不稼働、顧客満足度の低下等が引き起こされると指摘しています。さらに回答者の 30% が、情報漏えいにより「企業は直接的な損益を招く」と述べています。

こうしたデータ流出をどのように防ぐかは、企業にとって非常に深刻な問題です。とりわけ、内部者による犯行はコントロールが難しく、状況は改善するどころか悪化の一途をたどっています。トレンドマイクロの多層的アプローチを実行すれば、企業もこうした困難な状況に対しても一定のコントロールを行うことができます。「Trend Micro LeakProof」のようなツールを利用すれば、エンドポイントにおけるデータの保存中・使用中・移動中といった広範囲に渡る防御を施すことができます。さらに、同ツールにおけるインタラクティブな警告機能は、社員のセキュリティ教育にも役立ちます。こうして企業は、不注意による情報漏えいを回避し、顧客情報や企業情報の双方をしっかりと守ることができます。

参考:

*6) Sharon Gaudin, Information Week, “Boeing Employee Charged with Stealing 320,000 Sensitive Files,”
<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201000820>,
 July 11, 2007.

*7) CSO Magazine, “Millions of Records Stolen from Fidelity Subsidiary,”
http://www2.csoonline.com/blog_view.html?CID=33034, July 3, 2007.

*8) Information Security Magazine, “Data Security Breach at Pfizer Affects Thousands,”
http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1270736,00.html, September 5, 2007.

*9) Bill Brenner, Information Security Magazine, “Gap Security Breach Exposes Data on 800,000,”
http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1274757,00.html, October 1, 2007.

*10) Christian Annesley, ComputerworldUK, “Chancellor Faces up to UK’s Worst-ever Data Breach—HMRC under Pressure after 25 Million Records Go Missing,”
<http://www.computerworlduk.com/management/government-law/public-sector/news/index.cfm?newsid=6298>,
 November 20, 2007.

※ セキュリティ最前線は、米国トレンドマイクロで発行しているニュースレター「*First Line Of Defense (FLOD)*」(英語)を元に翻訳したものです。

※ お申し込み:「*F.L.O.D. Threat Watch Newsletter Signup*」(英語)
[<http://us.trendmicro.com/us/newsletter/>](http://us.trendmicro.com/us/newsletter/)