ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●新日本プロレスのWebサイトからクレジットカード番号11,155件他流出

http://www.itmedia.co.jp/enterprise/articles/1507/02/news123.html
http://www.njpw.co.jp/news/detail.php?nid=14324

このニュースをザックリ言うと･･･

- 7月2日（日本時間）、新日本プロレスリングの公式Webサイトが不正アクセスを受け、チケット購入者等のクレジットカード番号を含む個人情報が流出した可能性があると発表されました。

- 発表によれば、4月28日に決済代行会社からの連絡によってクレジットカード情報流出の可能性が発覚し、以後6月までログの解析を行った結果、公式サイト上でチケット購入およびオフィシャルファンクラブ入会・更新を行った最大18,000件分の氏名・住所・電話番号・メールアドレス（クレジットカード決済11,155件含む）が流出した模様です。

- 不正アクセスはWebアプリケーションの脆弱性を突いて行われたとしており、Webサーバ内のディレクトリファイルのクレジットカード情報を削除し、脆弱性の修正、管理体制の不備の改修、決済システムの変更等の対策をとったとしています。

AUS便りからの所感等

- 今回の事件では、Webサーバのドキュメントルート（DocumentRoot）以下に個人情報を含むファイルが保存されていた可能性がありますが、こういった形でWebサーバ上に保存されたCSV形式等の個人情報にアクセス可能な状態になっていたという問題は、Webサーバの設定ミスやデータ配置の不備によって発生するものであり、90年代から2000年代にかけて多く報告されていたものです。

- Webサイトの運用にあたって重要なのは、不必要な情報を表示しないようあらゆる設定を確認すること、本来アクセスされるべきではない機密情報やソースコードないしそれらの古いファイル等をDocumentRoot以下に残さないこと、また、Webアプリケーションの脆弱性次第では、最悪の場合サーバ上の任意の場所にあるファイルにアクセスされる可能性もあることにも注意が必要です。

- Webアプリケーションに対する攻撃やWebサーバ上のデータを不正に取得しようとするリクエストについては、Webサーバの前面にWebアプリケーションファイアウォール（WAF）やそれを提供するUTMの設置によって防ぐことが可能な場合もあり、可能な限り活用を検討すべきでしょう。


ITmedia エンタープライズ

2015年07月02日 17時20分 更新

新日本プロレスに不正アクセス、顧客情報の漏えいも

Webサイトへの不正アクセスが原因で、最大1万8000件の個人情報やクレジットカード情報が流出した。

[ITmedia]

印刷／PDF ツイート 144 いいね！ 62 チェック g+1 0 Pocket 12 通知

PR モバイル推進の業務部門 vs.リスク管理の経営層 解決策は？
PR ユニークなアプリを開発して、NYのWatson研究所へ行こう！

新日本プロレスリングは7月2日、最大1万8000件の個人情報やクレジットカード情報が外部に漏えいしたと発表した。公式サイトのWebサーバの脆弱性を突いた不正アクセスが原因だとしている。

同社によると、漏えいした情報は公式サイトで2014年8月28日から2015年4月28日までの間に、「チケット購入」や「オフィシャルファンクラブ入会・更新」をした顧客のクレジットカード情報と氏名、住所、電話番号、メールアドレス。1万8000件のうちクレジットカード決済は1万1155件。


News 最新情報

NEW JAPAN PRO-WRESTLING OFFICIAL WEBSITE

Home » News » All » 不正アクセスによるお客様情報流出に関するお知らせとお詫び

All 全ての情報 | Topics トピックス | Media メディア | Event イベント | Other その他 | Shop 開明ショップ

2015-07-02

不正アクセスによるお客様情報流出に関するお知らせとお詫び

お客様および関係者様各位

ツイート 435 いいね！ 966 g+1 9 B! チェック いいね！

不正アクセスによるお客様情報流出に関するお知らせとお詫び

このたび弊社公式サイトにおいて、第三者による不正アクセスがあり、一部のお客様のクレジットカード情報を含むご購入情報流出が判明いたしました。

不正アクセスによるお客様情報流出の概要と対応につきまして、下記の通りご報告いたしますとともに、お客様をはじめとする関係各位の皆様に対し、多大なるご迷惑およびご心配をおかけする事態に至りましたことを、ここに深くお詫び申し上げます。

●米人事管理局に不正アクセス、2,210万人分の個人情報が流出

http://itpro.nikkeibp.co.jp/atcl/news/15/071002307/
http://www.afpbb.com/articles/-/3054124

このニュースをザックリ言うと・・・

- 米連邦人事管理局（OPM）が不正アクセスを受け、連邦政府職員らの個人情報が流出していたことが明らかにされ、その件数は7月9日（現地時間）に発表された段階で2,210万人分に上るとされています。

- OPMへの不正アクセスは昨年5月から今年4月に発生していたとされ、6月初頭に発表された時点での被害件数は現・元職員および採用候補者420万人分とされていましたが、その後身辺調査対象者1,970万人および主に採用候補者の配偶者や同居人など180万人分の個人情報も被害を受けていたことが明らかになり、これらの重複を除いた合計が2,210万人分となる模様です。

- 流出したとされる個人情報は、氏名・住所・生年月日・社会保障番号(SSN)・指紋および身元調査申告書に記載されたアカウント情報とされています。

AUS便りからの所感等

- 米国政府機関からの個人情報流出事件は、5月にも米内国歳入庁（IRS）から約10万人の納税情報が流出した事件がありましたが、これとは比較にならない件数であり、被害は現時点で全アメリカ国民の6～7%分に上っています。

- 社会保障番号が日本において今年10月導入予定の社会保障・税番号（マイナンバー）に相当するものであることを考えれば、やはり6月に発生した日本年金機構の事件と同様、番号を発行する側およびそれを託されて管理する側（企業等）にとって、セキュリティインシデント発生時の被害をいかに最小限に抑えるよう対策するかが問われる題材となるでしょう。

- 不正アクセスが如何にして発生したかの詳細は不明ですが、マルウェア感染等を伴う標的型攻撃であれ、直接的な不正アクセスであれ、様々な攻撃を想定し、アンチウイルスやUTM等を有効に活用することにより、機密情報にユーザ以外が容易にアクセスできないようなシステム構成を行うことが望まれます。

●Flash Player等の脆弱点、監視ツール開発業者への不正アクセスで発覚

http://blog.trendmicro.co.jp/archives/11884

このニュースをザックリ言うと・・・

- 市民のPCやスマートフォンなどを監視するツールを捜査機関向けに提供しているとされるイタリアのHacking Team社が外部から不正アクセスを受け、7月5日（現地時間）、盗み出された顧客リストやメール等の機密情報を含んだ約400Gバイトのデータがインターネット上にアップロードされました。

- 流出した機密情報には、監視ツールで用いられているとみられる、WindowsやFlash Playerに存在する未修正の脆弱点を攻撃するコードが含まれており、Flash Playerを提供する米Adobe社が8日に急遽パッチを提供する事態となりました。

- トレンドマイクロによれば、Flash Playerの脆弱点は、修正される前の6月下旬に日本および韓国のユーザに対する攻撃に悪用された模様です。

AUS便りからの所感等

- 修正されたFlash Playerのバージョンは18.0.0.203（Windows版）となっており、通常は自動更新によって最新版へアップデートされますが、念の為Adobeのサイトにアクセスしてバージョンを確認することを推奨します。

- 同様に、Windowsの脆弱点についても15日の定例のアップデートによって対応されるとみられますが、パッチが間に合わない可能性あるいはそれまでにやはり攻撃に悪用される可能性がありますので、被害を最低限に抑えるためにもアンチウイルスとUTMによる防御が重要でしょう。


TREND MICRO トレンドマイクロ セキュリティブログ
POWERED BY TrendLabs セキュリティ専門家による脅威情報・ニュースをお届けします。

「Hacking Team」の情報漏えい事例：Flashゼロデイ脆弱性、発覚前に韓国と日本で被害発生か

投稿日：2015年7月9日
脅威カテゴリ：不正プログラム，脆弱性，TrendLabs Report
執筆：Threats Analyst - Weimin Wu

2015年7月、イタリア企業「Hacking Team」から漏えいした情報からエクスプロイトコードが複数確認されました。その後、トレンドマイクロは、このエクスプロイトコードがさまざまなエクスプロイトキットに利用されていることに言及しています。しかし、弊社のクラウド型セキュリティ基盤「Trend Micro Smart Protection Network」のフィードバックによると、このエクスプロイトコードは韓国と日本に限定した攻撃で利用されていました。最も重要な点は、この攻撃が「Hacking Team」の漏えい事件前に実行されていたことです。弊社は、この攻撃を2015年7月1日に初めて確認しました。