— AUS（アルテミス・ユーザ・サポート）便り 2016/08/01号 —
http://www.artemis-jp.com

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。

●7月も個人情報流出相次ぐ、エフエム愛知から約11万件、印刷会社から約9000件他

http://www.security-next.com/072110
http://www.itmedia.co.jp/news/articles/1607/19/news091.html
http://www.news24.jp/articles/2016/07/26/07336355.html

このニュースをザックリ言うと・・・

- 7月についても、国内における個人情報の流出が相次いで発表されました。

- 7月6日（日本時間、以下同）、転職支援サイトを運営するアイコニックジャパン社より、同社の3つのWebサイトから登録者計1105件の個人情報（氏名・生年月日・メールアドレス・住所・履歴書・職務経歴書・他）が流出したことが発表され、その発表によると、6月29日未明にサーバへの不正アクセスが確認されている他、流出したメールアドレス宛に同社を装いPaypalへのログインを促す不審なメールが送信されていたとのことです。

- 7月19日、総合印刷業のグラフィック社より、顧客計8,985件の個人情報等（法人名・担当者名・住所・電話番号・メールアドレス・アカウント情報・他）が流出したことが発表され、その発表によると、顧客情報データベースに不正アクセスがあり、同1日に決済代行会社からの連絡を受けたことにより、流出が発覚したとのことです。

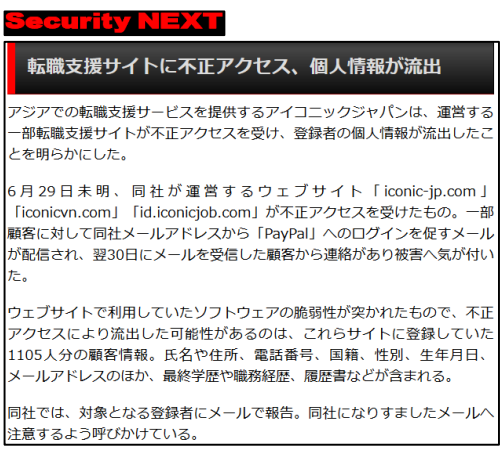
- 7月25日には、ラジオ局のエフエム愛知より、メール会員の一部となる約11万件の個人情報の流出したことが発表され、その発表によると、同24日午前0時頃から不正アクセスがあったとしており、現在個人情報は外部接続できない場所に移されているとのことで、同社になりすましてクレジットカード情報やマイナンバーなどを聞き出す等の不正なメールに注意を呼び掛けています。

AUS便りからの所感等

- 各々で起こったことおよび各社の対応は、いずれも個人情報流出の防御のみならず、万が一の時の事後対応において行うべきことの参考となることでしょう。

- 今回の事例では数日から一週間程度で事件の詳細が発表されており、速やかな調査を行う体制が整っていたことが窺え、攻撃の全容を早く把握するための、ネットワークに対する投資は重要です。

- また、一般に不正アクセスと言っても、外部からの直接の攻撃のみならず、内部でのマルウェア感染による攻撃にも注意を払う必要があり、そういった意味でもアンチウイルスによる感染防御、UTMによる不正な出入りの遮断・アクセスログ収集等の機能を有効活用することも大切でしょう。


Security NEXT

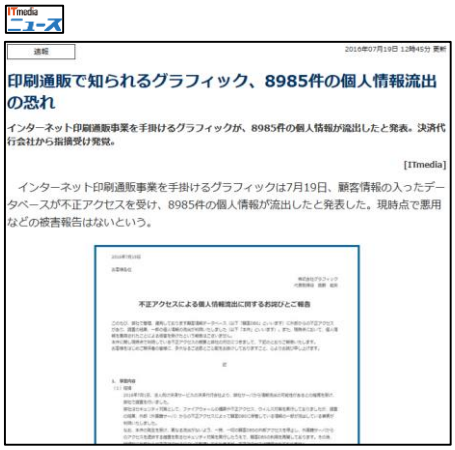
転職支援サイトに不正アクセス、個人情報が流出

アジアでの転職支援サービスを提供するアイコニックジャパンは、運営する一部転職支援サイトが不正アクセスを受け、登録者の個人情報が流出したことを明らかにした。

6月29日未明、同社が運営するウェブサイト「iconic-jp.com」「iconicvn.com」「id.iconicjob.com」が不正アクセスを受けたもの。一部顧客に対して同社メールアドレスから「PayPal」へのログインを促すメールが配信され、翌30日にメールを受信した顧客から連絡があり被害へ気が付いた。

ウェブサイトで利用していたソフトウェアの脆弱性が突かれたもので、不正アクセスにより流出した可能性があるのは、これらサイトに登録していた1105人分の顧客情報。氏名や住所、電話番号、国籍、性別、生年月日、メールアドレスのほか、最終学歴や職務経歴、履歴書などが含まれる。

同社では、対象となる登録者にメールで報告。同社になりすましたメールへ注意するよう呼びかけている。


ITmedia ニュース

印刷通販で知られるグラフィック、8985件の個人情報流出の恐れ

インターネット印刷通販事業を手掛けるグラフィックが、8985件の個人情報が流出したと発表。決済代行会社から指摘受け覚覚。

[ITmedia]

インターネット印刷通販事業を手掛けるグラフィックは7月19日、顧客情報の入ったデータベースが不正アクセスを受け、8985件の個人情報が流出したと発表した。現時点で悪用などの被害報告はないという。


日テレNEWS24

エフエム愛知　個人情報約１１万件流出か

2016年7月26日 21:00

ツイートする　シェアする

全文

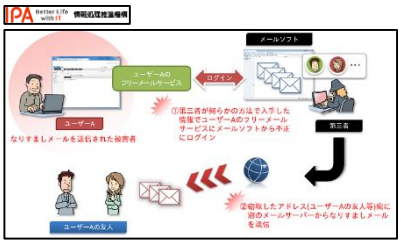
愛知県に本社があるラジオ放送局、「エフエム愛知」は、メール会員の個人情報が流出した可能性があると発表した。流出は約１１万件に上る恐れがあるという。

「エフエム愛知」によると、２５日午後、サーバーを管理する会社が、サーバーへのアクセス状況を調べたところ、外部から不正にアクセスされた可能性があることが明らかになった。不正アクセスにより、番組情報の配信などに使うメール会員の氏名や住所など約１１万件が外部に流出した恐れがある。

●メールサーバへ不正ログイン？パスワード使い回しが原因のなりすましメール送信にIPA警告

http://www.ipa.go.jp/security/anshin/mgdayori20160726.html

このニュースをザックリ言うと・・・



- 7月26日（日本時間）、情報処理推進機構（IPA）は、同組織の安心相談窓口に「自分が使っているフリーメールのアドレスが悪用され、友人・知人になりすましメールが送られている」といった相談が寄せられているとして警告しています。

- なりすましメール送信における事象としては、「利用しているフリーメールのアドレスを送信元に詐称」「友人・知人など(受信トレイにあるメールの送信元アドレスなど)宛てに送信されている」「フリーメールサービスのログイン履歴に不審な記録は見られない」「ログインパスワードを変更してもなりすましメールの送信は止まらない」などが挙げられています。

- IPAではこれらの事象から、フリーメールサービスのアカウントを奪取した攻撃者が（Webメールからではなく）メールソフトを用いて不正ログインしていたものと推測しており、「POPやIMAPによる不正ログインで受信トレイ上のメールから宛先情報を奪取する」「さらに別のメールサーバから、最初に不正ログインしたアカウントのアドレスで、奪取した宛先にメールを送信する」というシナリオを想定している模様です。

AUS便りからの所感等

- IPAは悪用されたサービスの具体名を示していませんが、別の情報では「Yahoo!メール」で同様の事件が発生しているとの指摘があり、同サービスの各種セキュリティ機能を活用すること、それでもPOPやIMAPのアクセスに関しては防御し切れない場面があることに注意することを呼び掛けています。

- ともあれ、「他のサービスで不正ログインに成功したID・パスワードのリストをWebサービスだけでなくメールサーバに対しても試行している」のであれば、当然「推測されにくいパスワードを用いる」という鉄則をそういったアカウントについても適用することが重要です。

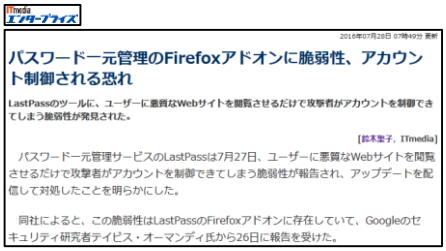
●パスワード管理ツール「LastPass」のFirefoxアドオンに脆弱性、アカウント制御される恐れ

http://www.itmedia.co.jp/enterprise/articles/1607/28/news063.html

このニュースをザックリ言うと・・・

- 7月27日（現地時間）、オンラインでのパスワード管理サービス「LastPass」がブラウザ向けに提供するアドオンの一部に脆弱性が報告され、修正されたことが発表されました。

- 脆弱性はFirefox向けアドオンのバージョン4.0以降に存在し、攻撃者が用意した悪意のあるWebページを閲覧することにより、ユーザが気付かないままにLastPassの操作を実行し、登録したパスワード情報を削除される、あるいは最悪の場合全て抜き取られる等の恐れがあった模様です。


ITmedia エンタープライズ
2016年07月28日 07時49分 更新
パスワード一元管理のFirefoxアドオンに脆弱性、アカウント制御される恐れ
LastPassのツールに、ユーザーに悪質なWebサイトを閲覧させるだけで攻撃者がアカウントを制御できてしまう脆弱性が発見された。
[鈴木聖子，ITmedia]
パスワード一元管理サービスのLastPassは7月27日、ユーザーに悪質なWebサイトを閲覧させるだけで攻撃者がアカウントを制御できてしまう脆弱性が報告され、アップデートを配信して対処したことを明らかにした。
同社によると、この脆弱性はLastPassのFirefoxアドオンに存在していて、Googleのセキュリティ研究者テイビス・オーマンディ氏から26日に報告を受けた。

- LastPassでは修正バージョン4.1.21aを配信して対応していますが、Firefox向けアドオンのバージョン3.0や、他のブラウザ向けアドオンには脆弱性は存在しないとしています。

AUS便りからの所感等

- LastPassは、そのサービスの特性上非常に攻撃者から狙われやすいものと目され、2015年には運営者のネットワークに不正アクセスされる事件がありましたが、ユーザに対し即座にマスターパスワード（LastPassのデータを暗号化・復号するためのパスワード）を変更するよう呼び掛け、また二段階認証等強力なセキュリティ機能によるアカウント保護を提供する等、サービスの安全性を高く保つための振る舞いにおいても支持されています。

- 一方で、必ずしもそれを強く推奨するわけではありませんが、LastPass以外のローカルでパスワードを管理するツールを検討することも、選択肢の一つとしては尊重されるべきものでしょう。

- それとは別に、攻撃者の不正なページへの誘導、あるいは他のパスワード管理ツールであってもPCや端末上でパスワードを奪取しようとするマルウェアの侵入は脅威であり、これらを食い止めるためのアンチウイルスやUTMの導入は不可欠です。