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。

●ネットユーザの8割近くがソフトウェアアップデートの重要性を理解していない･･･カスペルスキー調べ

http://internet.watch.impress.co.jp/docs/news/1034874.html
http://www.kaspersky.co.jp/about/news/virus/2016/vir13122016

このニュースをザックリ言うと･･･

- 12月13日（日本時間）、セキュリティベンダーのカスペルスキー社より、同社が9月1・2日に国内インターネット利用者623人に対し実施したセキュリティ意識に関するインターネット調査の結果が発表されました。

- 調査結果によれば、OSやソフトウェア、アプリケーションのアップデートを怠ることにより、ウイルスに感染する可能性が高まることについて、全体の実に76%が「知らない」「詳しくはわからない」と回答しています。

- ソフトウェアアップデートを行っているかどうかについては、60%が「必要なことなのですぐに行っている」と回答した一方、30%が「通信速度や機器のパフォーマンスに影響するので行っていない」と回答しています。

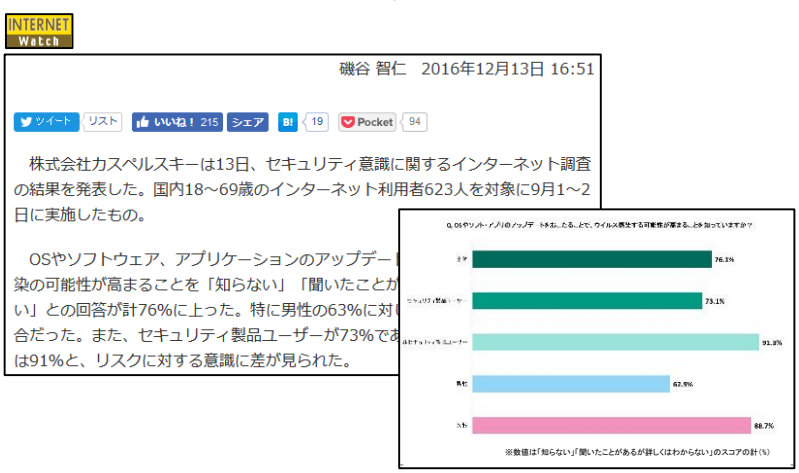
- 同社では、長期間使用していない、あるいはアップデートせず放置していたりするOSやソフトウェアはそれ自体が脆弱性となりマルウェア感染を引き起こすとして、アップデートの重要性を説くとともに、OSや各アプリが自動的にアップデートされるよう設定することを推奨しています。

AUS便りからの所感等

- 調査では、この他にも、自分のデバイスに意図しないソフトウェアがインストールされようとするときに「必ず気付くと思う」と回答したのは全体の19%に留まる等の結果が出ており、全てのユーザが十分なリテラシーを持っていることに依存するのはまだ危険と言えます。

- 基本的にあらゆるソフトウェアについて自動更新機能があるならば、それに任せるに越したことはありませんし、特にFlash Playerについては必ず自動更新機能を有効にし、意識していなくても最新のバージョンに保たれる状態にしておきましょう。

- 昨今ではWindows10へのアップグレードあるいはセキュリティアップデートにより、業務が中断してしまう等の批判を見ることがありますが、こういうケースでOSのセキュリティアップデートを保留させる判断をせざるを得ない場合に、システムのセキュリティレベルを少しでも維持するためにも、周辺のソフトウェアを最新に保つことや、アンチウイルス・UTM等による多重防御の実施は欠かすことができないものです。


INTERNET Watch

磯谷 智仁　2016年12月13日 16:51

ツイート　リスト　いいね！ 215　シェア　B!　19　Pocket　94

株式会社カスペルスキーは13日、セキュリティ意識に関するインターネット調査の結果を発表した。国内18～69歳のインターネット利用者623人を対象に9月1～2日に実施したもの。

OSやソフトウェア、アプリケーションのアップデー
染の可能性が高まることを「知らない」「聞いたことが
い」との回答が計76%に上った。特に男性の63%に対
合だった。また、セキュリティ製品ユーザーが73%で
は91%と、リスクに対する意識に差が見られた。


KASPERSKY

<カスペルスキーレポート：セキュリティ意識調査>インターネット利用者の約8割がソフトウェアのアップデートの必要性を詳しく理解していないと回答

2016年12月13日
ウイルスニュース

～断捨離とアップデートでデバイス内を大掃除、新年は脆弱性のない環境でスタート～

情報セキュリティソリューションを提供する株式会社カスペルスキー（本社：東京都千代田区、代表取締役社長：川合林太郎）が、日本国内で行ったセキュリティ意識に関するインターネット調査[※1]によると、インターネット利用者の約8割がデバイスのOSやソフトウェア、アプリケーションのアップデートを行わないとウイルス感染の可能性が高まることを「知らない」「詳しくわからない」と回答しました。また、自分のデバイスに意図せずソフトウェアがインストールされようとする時に、「必ず気づくと思う」と回答した人は2割未満に留まりました。

インターネットに接続しているデバイスに、長期間使用していない、あるいはアップデートせず放置していたりするOSやソフトウェアがあるとそれらが脆弱性となり、マルウェアに感染する可能性が高まります。年の瀬の大掃除の機会に、デバイス内のOSやソフトウェア、アプリケーションも整理しましょう。不要なソフトウェアは削除し、引き続き利用するものはアップデートを行って、脆弱性のない最新の環境で新しい年を迎えることをお薦めします。

1.インターネット利用者の約8割がソフトウェアの必要性を詳しく理解していないと回答

本調査では、インターネット利用者の76%がOSやソフトウェア、アプリケーションのアップデートを行わないとウイルス感染の可能性が高まることを「知らない」「詳しくはわからない」と回答しました。特に女性の間でその割合が高く、男性63%に対して女性は89%でした。また、セキュリティ製品のユーザーでは73%だったのに対し非ユーザーでは91%と、セキュリティ製品を使っている人といない人の間でリスクに対する意識に差があることも明らかになりました。さらに、ソフトウェア・アップデートについて60%の人が「必要なことなのですぐに行っている」という回答した半面、「ネット通信速度やデバイスのパフォーマンスに影響するのでアップデートしたくない」という回答が30%に上りました。

●地下鉄が一時運賃無料に、システムのランサムウェア感染が原因か？

http://www.itmedia.co.jp/enterprise/articles/1611/29/news076.html

このニュースをザックリ言うと・・・

- 11月26日（現地時間）、米サンフランシスコ市のネットメディア「SFGate」等により、同市交通局（SFMTA）が運営するサンフランシスコ市営鉄道（Muni）がクラッキングを受け、一時運賃を無料にする事態になったと報じられました。

- SFMTAの発表やSNSでの報告によれば、11月25日にSFMTA職員のPCや地下鉄の駅にあるPCのディスプレイに「You hacked, ALL Data Encrypted, Contact For Key」と表示されていたとのことで、Muniのコンピュータ2,112台がランサムウェアに感染し、起動しなくなった模様です。

- 感染したランサムウェアは暗号化解除の身代金として100ビットコイン（約$73,000相当）を要求していましたが、電車の運行自体が危機にさらされることはなかった模様です。

- なお、SFMTAではランサムウェアの要求に応じない一方で、「利用者への影響を最小限に抑えるため」25日～26日に運賃を一時無料とする処置をとり、その後27日までには一部システムを復旧させたとしています。

AUS便りからの所感等


ITmedia エンタープライズ

米サンフランシスコ市交通局、ランサムウェア感染で一部システムに被害

約900台のオフィスのコンピュータが影響を受け、券売機にも攻撃者のメッセージが表示されていたという。

[ITmedia]

米国サンフランシスコ市の交通当局（SFMTA）は11月28日、局内のコンピュータがランサムウェアに感染して金銭関連システムに支障が出ていることを明らかにした。市営鉄道などの安全運行には影響がないとしているが、一部報道によれば券売機などで攻撃者のメッセージが表示されるなどのトラブルに見舞われたという。

- 11月28日の時点でも（Muniの一部システム復旧後も）、バックアップからのシステムの復旧作業を行っていたとしており、事前に各PCのバックアップをとっておくこと、またバックアップデータ自体が暗号化されないよう隔離しておくことは、感染後の対応のために重要なことです。

- 2,000台近く（一部報道では8,000台以上ともされる）大規模な感染被害が発生した背景には、Muniのネットワーク内で感染したPCからネットワーク上の他のPCあるいはサーバにアクセスされないよう隔離する機構がなかったものと推測され、マルウェア感染あるいは侵入されたPCを踏み台としたネットワーク内での攻撃が拡散しないよう、UTM等を用いた各ネットワークの分離ないし出口対策が重要となるでしょう。

●流出した電子メールパスワードの半数近くがユーザの名前を含むという調査結果

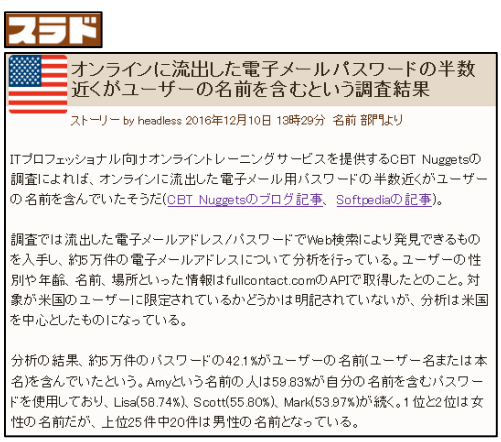
http://www.itmedia.co.jp/enterprise/articles/1612/02/news106.html

このニュースをザックリ言うと・・・

- 12月6日（現地時間）、セキュリティ等IT関連のオンライントレーニングを手がける米CBT Nuggets社より、オンラインに流出したメールアドレスとパスワードに関する調査結果が発表されました。

- 調査では、約5万件の流出したメールアドレス・パスワードをWeb上から入手し、メールアドレスをもとにユーザが公開しているプロフィールと照合、分析する形で行われていた模様です。

- 調査により、42%のパスワードがユーザアカウント名あるいはユーザの本名を含んでいた他、英単語の中でパスワードに含まれる頻度が高かったものとして「love」「star」「girl」「angel」「rock」「miss」「hell」「Mike」「John」等があったとされています。


スラド

オンラインに流出した電子メールパスワードの半数近くがユーザーの名前を含むという調査結果

ストーリー by headless 2016年12月10日 13時29分 名前 部門より

ITプロフェッショナル向けオンライントレーニングサービスを提供するCBT Nuggetsの調査によれば、オンラインに流出した電子メール用パスワードの 半数近くがユーザーの 名前を含んでいたそうだ(CBT Nuggetsのブログ記事、Softpediaの記事)。

調査では流出した電子メールアドレス/パスワードでWeb検索により発見できるものを入手し、約5万件の電子メールアドレスについて分析を行っている。ユーザーの性別や年齢、名前、場所といった情報はfullcontact.comのAPIで取得したとのこと。対象が米国のユーザーに限定されているかどうかは明記されていないが、分析は米国を中心としたものになっている。

分析の結果、約5万件のパスワードの42.1%がユーザーの名前(ユーザー名または本名)を含んでいたという。Amyという名前の 人は59.83%が 自分の 名前を含むパスワードを使用しており、Lisa(58.74%)、Scott(55.80%)、Mark(53.97%)が続く。1位と2位は女性の 名前だが、上位25件中20件は男性の 名前となっている。

AUS便りからの所感等

- ユーザ本人の名前にまつわる単語、あるいは辞書に載っている単純な単語、そしてそれらを組み合わせただけのパスワードは、攻撃者の長時間の試行により破られてしまう可能性が高くなります。

- そして、一旦破られたパスワードを別のサービスで使い回しているようなケースでは、連鎖的に不正アクセスの犠牲となり得ることもここ数年何度も取り上げられていることです。

- 自分に関連する事柄等、推測されやすい要素を含むパスワードではなく、完全にランダムなパスワード、ないし自分だけが記憶できる語呂合わせ等による、数字・記号も含んだパスワード、しかもサービス毎に別々のパスワードを設定することが重要です（記号を含んでいるからと言って、メールアドレスそのものをパスワードとするのも決してやってはいけないことです）。