— AUS（アルテミス・ユーザ・サポート）便り 2016/06/06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。

●「増加するインターネット接続機器の不適切な情報公開とその対策」IPAが改めて啓発、新たな検索サイト登場も登場

http://internet.watch.impress.co.jp/docs/news/759958.html
https://www.ipa.go.jp/about/press/20160531.html

このニュースをザックリ言うと･･･

- 5月31日（日本時間）、独立行政法人情報処理推進機構（IPA）は、2014年に公開していたテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」を改訂し、改めて注意を呼び掛けています。

- 発表で引用されている2015年11月の民間調査では、「IoT(物のインターネット)」(※1)ブームにより、インターネット接続機器が2016年には64億台に増加、今後もさらに増え続けるとされています。

- 改訂の理由の一つとして、問題のある機器を検索する新たなサイト「Censys(センシス)」が登場したことを挙げており、それ以前に登場していた「SHODAN(ショダン)」(※2)共々、自組織の機器が登録されていないかの安全確認のために利用する方法を掲載しています。

AUS便りからの所感等

- CensysやSHODANの利用は、ネットワーク機器を狙う攻撃者にとっても、そしてそれ以上にネットワークの防御を固めたい管理者にとっても有用なものとなるでしょう。

- Censysに登録されている、日本国内のものとされる機器は350万台に上り、特に多いオープンポートとして、HTTP・SMTP・FTP等が挙がっています。

- 内部LAN上のWebサーバ等を意図的に公開しているものも含まれていると思われますが、意図しない公開を行っていないか、自社以外の不特定多数のネットワークからアクセス可能でないかについても調査は重要です。

INTERNET Watch

IPA、IoT機器の情報漏えい対策をまとめた文書を公開

（2016/5/31 13:47）

独立行政法人情報処理推進機構（IPA）は31日、従来から公開していたテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」のレポートPDFの改訂版を公開した。

今回の改訂では、IoT機器などのインターネット接続機器を無償で検索できる検索エンジン「Censys（センシス）」の利用方法を新たに掲載した。

IPAでは、複合機で読み取った情報がインターネット越しに外部から閲覧できる状態にあった2013年11月の事例を受け、設定不備などで意図しない情報が開示されないように対策を解説したテクニカルウォッチを公表していた。その後のIoTの進展もあり、2015年11月に発表の調査によれば、IoT機器などのインターネット接続機器は、2016年には64億台に増加、今後もさらに増え続けるという。

IPA Better Life with IT 情報処理推進機構

プレス発表　改訂版「増加するインターネット接続機器の不適切な情報公開とその対策」を公開

～ネットに接続された機器の点検に、新たに登場した検索エンジンの活用も～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、"Censys(※1)"（センシス）が2015年10月に新たに登場したことを受け、2014年に公開したテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」を更新し、その使い方、機能などを追加し、2016年5月31日より改訂版として公表しました。

URL：https://www.ipa.go.jp/security/technicalwatch

IPAテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」

最終更新日：2016年5月31日
独立行政法人情報処理推進機構

IPA（独立行政法人情報処理推進機構）セキュリティセンターは、無償で利用できる検索エンジン"Censys"（センシス）が2015年10月に新たに登場したことを受け、2014年に公開したテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」を更新し、その使い方、機能などを追加し、2016年5月31日より改訂版として公表しました。

下記より改訂版「増加するインターネット接続機器の不適切な情報公開とその対策」についてのレポートPDF版をダウンロードしてご利用いただけます。

本レポートの目次

1. オフィス機器とサーバー機能
2. インターネット接続機器検索サービスSHODAN
3. SHODANを使用した目組織の検査
4. インターネット接続機器検索サービスCensys
5. 実施すべき対策
6. おわりに

※1 IT用語辞典 e-Words

IoT 【 Internet of Things 】 モノのインターネット / インターネットオブシングス
IoTとは、コンピュータなどの情報・通信機器だけでなく、世の中に存在する様々な物体（モノ）に通信機能を持たせ、インターネットに接続したり相互に通信することにより、自動認識や自動制御、遠隔計測などを行うこと。
自動車の位置情報をリアルタイムに集約して渋滞情報を配信するシステムや、人間の検針員に代わって電力メーターが電力会社と通信して電力使用量を申告するスマートメーター、大型の機械などにセンサーと通信機能を内蔵して稼働状況や故障箇所、交換が必要な部品などを製造元がリアルタイムに把握できるシステムなどが考案されている。

※2 コトバンク

ショダン（SHODAN）
米国のコンピュータープログラマー、ジョン＝マザリーが開発したサーチエンジン。
名称はロールプレーイングゲームに登場する架空の人工知能の名称に由来する。
一般的なサーチエンジンと異なり、インターネットに接続されたサーバー、ルーター、IP電話などの機器を検索できる。ほかにウェブカメラ、プリンター複合機、IP電話、発電所の制御システムなども検索できるため、セキュリティー上の問題がある端末の検索などに悪用される可能性が指摘されている。

●複数メーカー製PCのプリインストールアプリに脆弱性

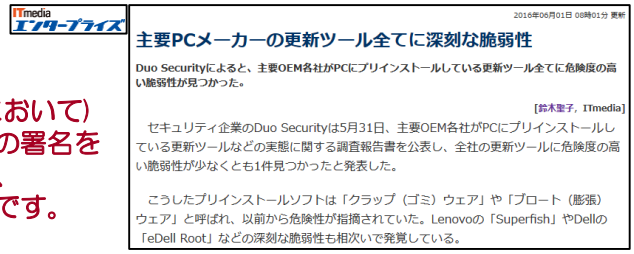
http://www.itmedia.co.jp/enterprise/articles/1606/01/news090.html

このニュースをザックリ言うと・・・

- 5月31日（現地時間）、二段階認証サービスを提供するDuo Security社は、Acer・ASUS・DELL・HPおよびLenovo製のPCに、セキュリティ上問題のあるソフトウェアがプリインストールされているとするレポートを発表し、警告しています。

- 問題が指摘されているソフトウェアの一例として、サードパーティー製のアプリケーション更新ツールが挙げられており、Duo社が調査したPC全てに搭載されていたとのことです。

- また、Lenovo社は、同社製PCにプリインストールされている「Lenovo Accelerator Application」に「中間者攻撃」を受ける問題があり、最悪の場合攻撃者にリモートからPCを乗っ取られる可能性があるとし、アンインストールを呼び掛けています。


ITmedia エンタープライズ

2016年06月01日 08時01分 更新

主要PCメーカーの更新ツール全てに深刻な脆弱性

Duo Securityによると、主要OEM各社がPCにプリインストールしている更新ツール全てに危険度の高い脆弱性が見つかった。

[鈴木聖子，ITmedia]

セキュリティ企業のDuo Securityは5月31日、主要OEM各社がPCにプリインストールしている更新ツールなどの実態に関する調査報告書を公表し、全社の更新ツールに危険度の高い脆弱性が少なくとも1件見つかったと発表した。

こうしたプリインストールソフトは「クラップ（ゴミ）ウェア」や「ブロート（膨張）ウェア」と呼ばれ、以前から危険性が指摘されていた。Lenovoの「Superfish」やDellの「eDell Root」などの深刻な脆弱性も相次いで発覚している。

AUS便りからの所感等

- Duo社のレポートでは「(アップデートファイルの取得等において)暗号化通信を行っていなかった」「アップデートファイル等の署名をチェックしていなかった」といった問題点が挙げられており、これらが原因で中間者攻撃を回避できない状態にあった模様です。

- Lenovo社およびDell社製PCにおいては以前にも、「プリインストールされている独自のルート証明書を攻撃者のなりすましに悪用される可能性」といった問題が取り上げられていましたが、他の主要メーカーでも対岸の火事ではなかったと言えます。

- 問題のあるアプリケーションやルート証明書が関係する通信については、ブラウザやUTMのアンチフィッシング機能において、既に(もしくは今後新たに)、ある程度の対応が行われることが期待されますが、ともあれメーカーからの情報等を確認の上でアンインストールを行うこと、および可能な限り、新たなPCの購入・配備の際のマニュアルにもそれを含めること、などが安全性を高めることの一助になることでしょう。

●Microsoft、安易なパスワードを使用禁止　攻撃にも対抗措置

http://www.itmedia.co.jp/enterprise/articles/1605/27/news063.html

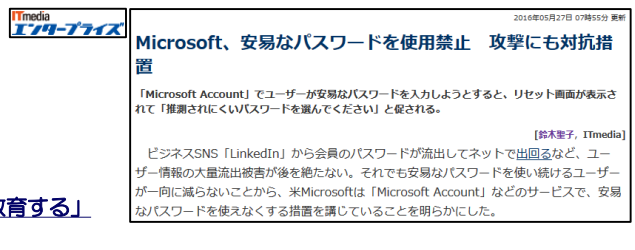
このニュースをザックリ言うと・・・

- 5月24日（米国時間）、Microsoft社（以下MS）は、同社の「Microsoft Account」等のサービスにおいて、簡単すぎる等の問題があるパスワードを使えないようにする措置をとっていることを発表しました。

- MSでは、ビジネス特化型SNS「LinkedIn」で1億1700万人分のアカウント情報が流出した事件について、「123456」といった安易なパスワードが使用されている実態が伝えられていたこと、また、MSのサービスにおいても1日1000万件以上のアカウントがブルートフォースアタック（パスワードの総当たり攻撃）等の攻撃を受けていることを挙げています。

- 使用が禁止されるパスワードは、攻撃の際に特に対象になっているとされるパスワードからなり、リストは随時更新されるとのことで、この他、IT管理者向けの「パスワードに関するガイダンス」も公開されています。

AUS便りからの所感等


ITmedia エンタープライズ

2016年05月27日 07時55分 更新

Microsoft、安易なパスワードを使用禁止　攻撃にも対抗措置

「Microsoft Account」でユーザーが安易なパスワードを入力しようとすると、リセット画面が表示されて「推測されにくいパスワードを選んでください」と促される。

[鈴木聖子，ITmedia]

ビジネスSNS「LinkedIn」から会員のパスワードが流出してネットで出回るなど、ユーザー情報の大量流出被害が後を絶たない。それでも安易なパスワードを使い続けるユーザーが一向に減らないことから、米Microsoftは「Microsoft Account」などのサービスで、安易なパスワードを使えなくする措置を講じていることを明らかにした。

- ガイダンスでは、IT管理者に対して推奨する事項として、
「1. パスワード長は最低でも8文字とする」
「2. 文字の組み合わせ(複雑さ)に関する要件を廃止する」
「3. 定期的な変更は強制しない」
「4. わかりやすい一般的なパスワードを禁止する」
「5. 業務用アカウントのパスワードを社外サービス等で使い回さないよう教育する」
「6. (二段階認証等の)多要素認証を必ず利用する」
「7. リスクベース多要素認証を検討する」
を挙げています。2と3については賛否両論がありますが、ユーザが攻撃者に推測されやすいパスワードを設定してしまう等のデメリットの方が大きいことをMSは理由に挙げています。

- この他、マルウェアへの感染や、感染による内部からのアカウント情報流出の恐れに対し、アンチウイルスやUTMによる防御を忘れずに行うこと、そういった事態においてパスワードを確実に更新できる体制を整えておくことも重要でしょう。