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。

●推測されやすいパスワードや使い回しは危険…JPCERT「STOP!!パスワード使い回し!!キャンペーン2017」

http://internet.watch.impress.co.jp/docs/news/1073682.html
https://www.jpcert.or.jp/pr/2017/pr170002.html

このニュースをザックリ言うと･･･

- 8月1日（日本時間）から、セキュリティ専門機関JPCERT/CCより、「STOP!!パスワード使い回し!!キャンペーン2017」と題し、パスワードの適切な使用に関する啓発キャンペーンが実施されています。

- このキャンペーンは2014年以降毎年この時期に行われており、複数のインターネットサービスで同じID・パスワードを使い回しているアカウントに対する「パスワードリスト攻撃」による不正ログインの被害が継続的に発生していることへの警告を行っています。

- 基本的な対策として、次のような対策を行うよう呼び掛けています。

●同じパスワードを使い回さない
●名前・生年月日あるいは数字等の単純なパスワードを使わず、複雑なパスワードを使う
●ワンタイムパスワード等の2段階認証を活用する
●不正なログインを早期に発見するためログイン履歴を確認する

AUS便りからの所感等

- キャンペーンが開始された2014年は、まさにリスト攻撃による不正ログインが国内大手サービスで多発して問題となった年であり、「パスワードは定期的に変更する」「紙に書き留めない」といったそれまでのやり方に「少数のパスワードパターンを使い回すユーザが発生し、逆効果だった」といったような異論も出る等、パスワード管理の考えについての転換点となった年とも言えます。

- 各サイトのアカウント情報をまとめて管理できるツールの中には、複数のサービスで同一のパスワードを使っているものがないかチェックする機能が備わっているものもあり、これを活用するのも有用でしょう。

- ただし、こういったツールでパスワードを管理する場合、パスワードデータを保護するために使用される「マスターパスワード」をくれぐれも他人に奪取されることのないよう、細心の注意を払ってください。

●IPAより夏季休暇におけるセキュリティの注意喚起

https://www.ipa.go.jp/security/measures/vacation.html

このニュースをザックリ言うと・・・

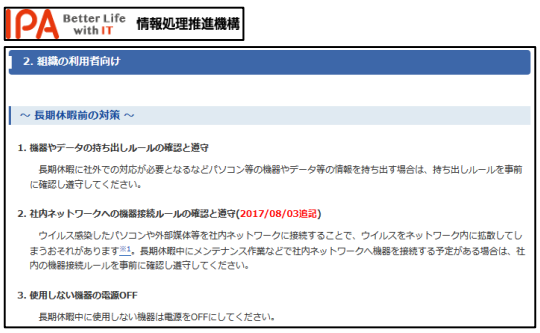
- 8月3日（日本時間）、多くの企業が長期休暇となるお盆の時期を迎えるにあたり、IPAが以前から発表している「長期休暇における情報セキュリティ対策」が更新されました。

- 同情報は、システム管理者が長期間不在になることにより、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまう可能性や、従業員等が友人や家族と旅行に出かけた際のSNSへの書き込み内容から思わぬ被害が発生する可能性等を指摘し、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれの対象者に対して実施すべき対策をまとめているものです。

- 今回、組織の利用者に対する休暇前の対策として「社内ネットワークへの機器接続ルールの確認と遵守」が追加されており、休暇中にメンテナンス等の理由でPCや外部媒体を社内ネットワークに接続する際、それらがマルウェアに感染していた場合に社内ネットワークにマルウェアが侵入される恐れがあることから、社内の機器接続ルールを事前に確認し遵守するよう呼び掛けられています。

AUS便りからの所感等

- IPAでは、長期休暇以外の日常においても各自が行うべきセキュリティ対策に関する情報も公開しており（https://www.ipa.go.jp/security/measures/everyday.html）、これらの情報は、情報システムとインターネットを組織内外で利用する者として、「普段から」セキュリティを意識した慎重な行動をとることと、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応すること、それぞれへの注意を促すものとなっています。


IPA Better Life with IT 情報処理推進機構

2. 組織の利用者向け

～ 長期休暇前の対策 ～

1. 機器やデータの持ち出しルールの確認と遵守

長期休暇に社外での対応が必要となるなどパソコン等の機器やデータ等の情報を持ち出す場合は、持ち出しルールを事前に確認し遵守してください。

2. 社内ネットワークへの機器接続ルールの確認と遵守(2017/08/03追記)

ウイルス感染したパソコンや外部媒体等を社内ネットワークに接続することで、ウイルスをネットワーク内に拡散してしまうおそれがあります[注]。長期休暇中にメンテナンス作業などで社内ネットワークへ機器を接続する予定がある場合は、社内の機器接続ルールを事前に確認し遵守してください。

3. 使用しない機器の電源OFF

長期休暇中に使用しない機器は電源をOFFにしてください。

- もしこの「AUS便り」を連休明けにご覧になったとしても、その時点で点検すべきことは多くあり、年末年始やゴールデンウィークといった長期休暇に備えて、準備・点検を行うよう意識して頂ければ幸いです。

●SMBの新たな脆弱性、研究者がハッキングイベントで発表

http://www.itmedia.co.jp/enterprise/articles/1708/01/news049.html

このニュースをザックリ言うと・・・

- 7月29日（現地時間）、米国で開催されたハッキングカンファレンス「DEF CON 25」において、Windowsの共有フォルダ等に関連するプロトコルであるSMBに未修正の脆弱性が存在することがセキュリティ研究者より発表されました。

- 「SMBLoris」と名付けられたこの脆弱性はSMBの古いバージョン（SMBv1）に存在し、PCのメモリとCPUリソースを使い尽くされる、いわゆるDoS（サービス拒否）攻撃に悪用される可能性があるとされ、実際に8GBのメモリを積んだPCが数秒で応答しなくなる攻撃デモも行われたようです。

- セキュリティ研究機関である米SANS Internet Storm Centerより、脆弱性の緩和策として「SMBで使用される445番ポートへの同じアクセス元からの接続数をファイアウォール等で制限すること」が挙げられており、またMicrosoftも、さほど重大な影響はないと判断しセキュリティパッチの提供予定はないとしつつも、「インターネットからSMBv1へのアクセス遮断を検討することを推奨する」としています。

AUS便りからの所感等

- SMBv1については3月にも脆弱性が発表されてセキュリティパッチがリリースされましたが、今回パッチリリース予定がないのは、PCに侵入される類のものではないためとみられます。

- Windows Vista以降ではSMBのより新しいバージョンであるSMBv2等が用いられており、Windows XP以前を利用していない限り、サーバにてSMBv1を無効化することにより、今後SMBv1固有の脆弱性が新たに確認された場合も理論上は回避可能とみられます。


ITmedia エンタープライズ

SMBの新たな脆弱性、研究者がDEF CONで発表
Microsoftは対処予定なし

悪用された場合、標的とするマシンにDoS攻撃を仕掛けてメモリとCPUリソースを枯渇させ、サービスを妨害することが可能とされる。

[鈴木聖子，ITmedia]

MicrosoftのServer Message Block（SMB）プロトコルに新たなサービス妨害（DoS）の脆弱（ぜいじゃく）性が見つかったとして、米国ラスベガスで開かれたハッキングカンファレンス「DEF CON 25」でセキュリティ研究者が詳細を発表した。この問題に対処するMicrosoftのセキュリティ更新プログラムは公開されない見通しだと伝えられている。

米セキュリティ機関のSANS Internet Storm Centerによると、今回の問題は、ショーン・ディロン、ザック・ハーディングの両氏が7月29日にDEF CONで発表した。悪用された場合、標的とするマシンにDoS攻撃を仕掛けてメモリとCPUリソースを枯渇させ、サービスを妨害することが可能とされる。

- UTMにおいては、前述したSMBサービスポートへの不正なアクセスを遮断する機能は既に備わっており、今後はSMBv1による接続をも遮断する機能が追加されることも考えられ、万が一クライアントPCにマルウェアが侵入し、そこから直接攻撃を受けたりすることのないよう、Windowsサーバの前面にUTMを設置する構成とするのが良いでしょう。