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。

●JPCERT/CCが今年も実施、「STOP! パスワード使い回し!キャンペーン」

http://www.jpcert.or.jp/pr/2018/stop-password2018.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2018」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、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おり、リスト攻撃が問題となった2014年以降、毎年この時期に行われています。

- パスワードを使い回さずに不正ログイン等を防止するための対策として、次の事項が挙げられています。
（1）「文字列は長めにする(12文字以上推奨)」「様々な文字種(大小英字、数字、記号)を組み合わせる」「推測されやすい単語、生年月日、数字、キーボードの配列順などの単純な文字の並びやログインIDは避ける」といった条件を満たす安全なパスワードを設定すること
（2）「紙にメモして、人目に触れない場所で保管する」「パスワード付きの電子ファイルで保管する」「パスワード管理ツールを使用する」といった方法での適切な管理
（3）「ワンタイムパスワードなどの2段階認証機能」「ログイン履歴機能、ログインアラート機能」「ID・パスワードを忘れた場合の再設定機能」といったセキュリティ機能を事前に確認し、活用すること

AUS便りからの所感等

- これまでパスワード管理において今まで常識ともされてきた「定期的に変更する」について、これをシステム上で要求してきたことにより、逆に安全でない推測されやすいパスワードが設定されていたという実験結果がキャンペーンのページでは挙げられており、今年は、やはりこれを推奨していた総務省も撤回し、方針転換するという出来事がありました（「AUS便り 2018/04/09号」参照）。

- 一見して安全だと思われるパスワードであっても、「一つの単語の一部文字を記号に変えた」程度のものは、今では攻撃者が使用するブルートフォース（総当たり）攻撃用のツールで対応しているケースが多く、不正ログインされるのは時間の問題とされており、設定可能であれば、一単語ではなく、他人が推測しにくい複数の単語～一つの文章をパスワード（パスフレーズ）とすることにより、パスワードの安全性を高めることが期待できます。

- 残念ながら今でも「英数字のみ」や「8文字以下」といったパスワードの制限を行っているサービスは珍しくありませんが、自組織内でのアカウントを発行する場合やユーザが登録するサービスを提供する場合において、こういった制限を設けないようにすることはユーザを保護するという観点では重要な事項と言えるでしょう。

JPCERT CC

●HTTPサイトは「保護されていません」と表示…Google Chrome 68正式公開

https://forest.watch.impress.co.jp/docs/news/1134616.html

このニュースをザックリ言うと･･･

- 7月24日（米国時間）、GoogleよりWebブラウザ「Google Chrome」バージョン68の正式版が公開されました。

- このバージョンの主なトピックとして、暗号化されてないHTTPを用いているWebサイト（以下HTTPサイト）へのアクセスは全てアドレスバーの左側に「保護されていません」と警告が表示されるようになっています。

- 10月リリース予定のバージョン70では、HTTPサイト上でパスワードを送信しようとした場合、この警告部分が赤く表示されるようになるとのことです。

AUS便りからの所感等

- 近年、Wi-Fi通信に関して公衆アクセスポイントの利用において通信が暗号化されない場合があることや、不正なアクセスポイントに誘導されたりする可能性が指摘され、あるいは多くのモバイル機器でWPA2暗号化通信を解読される脆弱性が発表されたりするといった事情を鑑み、「上位のレイヤー」における安全性確保の手段として、HTTPS通信を用いることの重要性が高まっている模様です。

- Webサイト全体で一切HTTPを使わず全てHTTPSにする「常時SSL化」の流れも、HTTPSサイトを提供するために必要なSSL証明書を無料で発行するサービスが登場したことにより、さらに加速しています。

- 今回の変更は、ある意味では「証明書による確認ができないから、正当なWebサイトとの接続かどうかは保証できないことを示している」に過ぎず、フィッシングサイトへの接続やWebサイトからのマルウェアのダウンロードを遮断する機能は、依然ブラウザの別の機能やUTM等が担っていることを理解し、表示に惑わされない行動をとって頂ければ幸いです。

●夏季休暇における情報セキュリティに関する注意喚起、IPA呼びかけ

https://www.ipa.go.jp/security/topics/alert300802.html

このニュースをザックリ言うと･･･

- 8月2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より情報セキュリティに関する注意喚起が出されています。

- 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インシデント発生に気付きにくく対処が遅れてしまう可能性、および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、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- 休暇前にシステムのセキュリティ対策が十分か確認すること、休暇期間中のインシデント対応体制や関係者への連絡方法を調整すること、および休暇明けには不正アクセス・侵入等の痕跡をサーバ等のログから確認することを呼びかけており、実施すべき項目をまとめています。

AUS便りからの所感等

- IPAおよびJPCERT/CCでは、毎回の長期休暇の前に、組織内に常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、そういった問題にも早く確実に対応することへの注意を促しています。

- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有がそういった攻撃による被害を最小限に抑えられるために大切なことと言えます。

- 万一休暇に入るまでに十分な対応が間に合わなかったとしても、明けてから点検すべきことは多く存在しますし、以後も年末年始等に備えて、準備・点検を行うよう意識して頂ければ幸いです。