— AUS（アルテミス・ユーザ・サポート）便り 2022/11/15号 —
https://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。

●「パスワード専用メモ帳」、Twitterで取り上げられ賛否両論の話題に

https://yorozoonews.jp/article/14765791
https://togetter.com/li/1969348

このニュースをザックリ言うと･･･

- 11月6日(日本時間)、Webサービス等のID・パスワードを書き留めることを目的とした手帳「ID・パスワードブック」がTwitterで取り上げられました。

- 以後、Twitterをはじめとしたネット上では、紛失時の漏洩を懸念するネガティブなものから「パスワードを使い回すぐらいなら書き留める方がまし」等とする好意的なものまで、賛否両論となっています。

- ネットメディア「よろず～」によれば、当該商品を企画した手帳メーカーでは、家族へID・パスワードや保険の緊急連絡先等を書き残す製品が好評だったことを受けて2020年に発売、人気商品となっているとしています。

- 一方でメーカーでは、(手帳を自分用だけに使うのであれば)パスワード等の情報は全て正確に書く必要はなく、伏字あるいは暗号で書くことも勧めているとのことです。

AUS便りからの所感等

- 利用するネットサービスの数がどんどん多くなっている現状、「全てのパスワードは頭の中でだけ覚えていなければならない」といった考え方は、複数のサービスで同じパスワードを使い回す傾向に陥り、たびたび当AUS便りでも取り上げている、いわゆる「リスト型攻撃」による連鎖的な不正ログインの標的となる恐れがあります。

- これを鑑み、推測されにくく、サービス毎に異なるパスワードを設定することを前提とする限り、PC上のツールないしオンラインのパスワード管理サービス(LastPass・Bitwarden等)によるパスワードの生成や保存等の管理を行うことも考慮すべきとする考え方が10年近く前から広まっています。

- 手帳へのパスワード書き留めも、アナログな手法ゆえに、例えばPCへのマルウェアや攻撃者の侵入によるアカウント情報の奪取の手が及ばないといった利点があるとされ、それぞれ得手不得手を把握した上での管理方法の採用、またいずれを用いるにせよ手帳の厳密な管理、アンチウイルスやUTM等によるPCの保護等も怠りなく行うことが肝要です。

よろず～

"パスワード専用メモ帳"にネット賛否「情報漏洩」「悪くない」　企画社は「工夫して」伏字推奨

今井 佳奈　2022.11.11(Fri)

Webサービスのログイン IDやパスワードを一覧で書きとめられる「ID・パスワードブック」がネット上で話題になっている。ツイッターでは情報漏洩を不安視する声と前向きな意見がぶつかり物議を醸した。

注目を集めたのは、「サイト名」「ID」「パスワード」「メモ」を並べて書く欄がある手のひらサイズの手帳。ログインに必要な情報を書き留めることを危険視したツイッター投稿が約1万回リツイートされた。ツイッターユーザーからは「あかん」「落としたらヤバい」「オシャレな情報漏洩」などの不安の声や、「悪くないと思う」「大切に保管する分には良い」「ヒントを書き留めておく分には有用」と活用方法を見いだすコメントが寄せられた。

ＩＤ・パスワードブックの記入欄

●大阪府の医療機関でランサムウェア感染…提携サービスからの連鎖感染か

https://www3.nhk.or.jp/news/html/20221031/k10013876181000.html
https://www.gh.opho.jp/news/
https://xtech.nikkei.com/atcl/nxt/column/18/00598/070100190/
https://www.asahi.com/articles/ASQC75HZ5QC7ULZU00N.html

このニュースをザックリ言うと・・・

- 10月31日(日本時間)、大阪急性期・総合医療センターより、同センターがサイバー攻撃を受け、電子カルテシステムが使えなくなる等の被害が発生したと発表されました。
- 「ランサムウエアと思われる攻撃」によるものとされ、緊急以外の手術および外来診療を一時停止し、通常診療ができない状況となっているとのことです。
- その後11月4日から一部手術再開、同10日には電子カルテの一部が参照可能となっているものの、新規外来の受け入れ等が依然停止しているとのことです。

AUS便りからの所感

- 同センター等と提携して食事の配達を行っている医療法人の給食提供システムが同時期にランサムウェアに感染しており、同センターにはその約40分後にネットワークを経由して連鎖感染した可能性があると一部で報じられています。
- 病院の電子カルテシステムがランサムウェア感染で利用できなくなる事案は昨年10月に徳島県つるぎ町立半田病院で、また10月27日にも静岡県沼津市の病院で発生しています。
- 半田病院の事例では詳細な報告書が公表されており(AUS便り 2022/06/21号参照)、ランサムウェアにおいては、感染の防止以上にデータを暗号化された場合に速やかに復旧できるよう、バックアップの実行とバックアップデータの保全を確実に行うといった体制を整えることを、当該報告書を参考にする等して実施して頂ければ幸いです。

NHK

大阪急性期・総合医療センターでシステム障害 サイバー攻撃か

2022年10月31日 22時35分

大阪 住吉区の大阪急性期・総合医療センターは「ランサムウエア」と呼ばれる身代金要求型のウイルスによるサイバー攻撃を受け、電子カルテのシステムに障害が発生して緊急以外の手術や外来診療などを停止していると発表しました。復旧のめどは立っておらず、11月1日以降もこの状況が続くとしています。

これは31日、大阪急性期・総合医療センターが記者会見を開いて明らかにしました。

病院によりますと31日午前7時ごろ、電子カルテのシステムに障害が発生し閲覧などができなくなりました。

● 2022年7～9月に最も狙われたのは5年前に修正されたOfficeの脆弱性

https://japan.zdnet.com/article/35195417/
https://www.digitalshadows.com/blog-and-research/q3-2022-vulnerability-roundup/
https://www.ipa.go.jp/security/ciadr/vul/20171129_ms.html

このニュースをザックリ言うと・・・

- 10月26日(現地時間)、英Digital Shadows社より、2022年第3四半期(7～9月)における脆弱性の悪用状況の分析記事が発表されました。
- 同期間において攻撃者が最も話題にしていた脆弱性は、2017年11月に修正パッチがリリースされたOfficeの脆弱性「CVE-2017-11882」だったとしています。
- 当該脆弱性は、「Formbook」「Redline」といった、PC上の情報を奪取するマルウェアの感染に悪用されているとのことです。
- またこれに次いで多かった脆弱性として、2022年5月に修正されたWindowsの診断ツールの脆弱性「Follina(CVE-2022-30190)」が挙げられています。

AUS便りからの所感

- CVE-2017-11882はOfficeの数式エディタの脆弱性で、細工されたOfficeファイルを開くことによってマルウェア感染等の被害を受ける恐れがあり、(当時サポート対象となっていた)Office 2007～2016についてパッチがリリースされていました。
- 修正から数年たった脆弱性が悪用されるケースは決して珍しくなく、例えばVPN装置の脆弱性を悪用して組織内ネットワークに侵入する攻撃等も注意喚起が出されています。
- Office 2007・2010は既にサポートが終了、Office 2013は2023年に終了予定、以後も買い切り版のOfficeはサポート期間が短くなる傾向が進んでおり、組織によっては「更新されない状態のOfficeが多く存在する」という状況が発生する可能性があります。
- マルウェア感染のターゲットとなる可能性が高いOfficeにおけるセキュリティ確保の観点からも、例えば自動的なバージョンアップが提供されるMicrosoft 365の導入等は十分に検討に値するでしょう。

ZDNet Japan

「Microsoft Office」に潜む脆弱性、3Qにサイバー犯罪者が最も悪用

Danny Palmer (ZDNet.com) 翻訳校正: 編集部　2022-11-01 12:42

サイバー犯罪者らが過去数カ月間で最も悪用していたセキュリティ脆弱性の1つは、「Microsoft Office」に潜んでいる脆弱性だという。この脆弱性は約5年前に発見され、すぐにセキュリティアップデートが利用可能になったにもかかわらず、アップデートを適用しない企業の多さから、依然として悪用が続いている。

Digital Shadowsのサイバーセキュリティリサーチャーたちの分析によると、2022年第3四半期の3カ月間でサイバー犯罪者らが最も話題にしていた脆弱性は、「CVE-2017-11882」だったという。このMicrosoft Officeの脆弱性が最初に開示されたのは2017年のことだった。

この脆弱性の悪用によって、サイバー犯罪者らは遠隔地から、脆弱性を抱えた「Windows」システム上で任意のコードを実行できるようになるため、標的としたシステム上にひそかにマルウェアをデプロイすることが可能になる。