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。

●消費税増税に便乗、三井住友銀行騙るフィッシングに注意

https://internet.watch.impress.co.jp/docs/news/1209504.html
https://www.antiphishing.jp/news/alert/smbc_20190926.html
https://www.smbc.co.jp/security/attention/index23.html

このニュースをザックリ言うと・・・

- 9月26日(日本時間)、フィッシング対策協議会より、三井住友銀行を騙るフィッシングメールおよびSMSが確認されたとして注意喚起が出されています。

- フィッシングメールは、件名が「[重要]：お客様の【三井住友銀行の口座】セキュリティ強化、カード・通帳一時利用停止、再開のお手続きの設定してください。」等、また文面にて「消費税率引き上げに伴うSMBCダイレクトの各種手数料改定」を名目としたもの等が例に挙げられており、同銀行のネットバンキングサービス「SMBCダイレクト」のログイン画面に巧妙に似せた偽サイトにリンクしています。

- 協議会では、このようなフィッシングサイトにて、店番号、口座番号、契約者番号、第一暗証、電話番号などの情報を絶対に入力しないよう呼び掛けています。

AUS便りからの所感等

- 大きなイベントにはそれに便乗したフィッシング等のサイバー犯罪がつきものですが、それはオリンピックやラグビーワールドカップといったスポーツイベントに限らず、国民の多くが興味を持つ政治・経済的な出来事でも同様と言えます。

- SMBCダイレクトでは実際に税率引き上げによる手数料改定を行う予定ですが、そういった情報の確認時に偽のサイトにアクセスしないよう、通常使用するサービスのサイトはブラウザーのブックマークに予め登録しておくこと、また不審なメール・SMSについてネット上の報告がないか確認する習性をつけ、かつブラウザー・アンチウイルスおよびUTMのセキュリティ機能による防御を確実に行うことが肝要です。

- なお、本物のSMBCダイレクトのログインページではEV-SSL証明書を使用しているものの、Chromeは現バージョン77でアドレスバーに直接組織名を表示しないよう変更されており、Firefoxも次期バージョン70で同様の変更を行う予定となっている(https://gigazine.net/news/20190813-extended-validation-certificate/ ※鍵アイコンをクリックすれば組織名は表示されます)ため、これによるサイトの確認には依存しないよう注意が必要です。

●Windows 7の有償延長サポート、中小企業にも提供へ

https://japan.zdnet.com/article/35143400/
https://gigazine.net/news/20191003-microsoft-windows-7-extended-update-support/
https://www.microsoft.com/microsoft-365/partners/news/article/announcing-paid-windows-7-extended-security-updates

このニュースをザックリ言うと・・・

- 10月1日(現地時間)、マイクロソフト(以下、MS)より、Windows 7(ProfessionalおよびEnterprise)に対し2020年1月の一般サポート終了後に提供する有償の延長サポート「Windows 7 Extended Security Updates(ESU)」について、提供範囲を中小企業にも拡大することが発表されました。

- 昨年9月にESUが発表された当初は、ボリュームライセンス契約に対してのみ提供される予定でした(AUS便り2018/9/18号参照)が、今回その制限が解除され、Windows 7 ProfessionalないしEnterpriseであれば企業の規模に拘らずMSのクラウドソリューションパートナーを通じてESUの購入が可能になるとのことです。

- ESUは2023年1月まで提供され、課金はデバイス単位、かつ料金は毎年引き上げられることになります(例えばProにおける提供料金は1年目が50ドル、2年目が100ドル、3年目が200ドルとなる模様です)。

AUS便りからの所感等

- MSは1月に「2020年の一般サポート終了時点で、Windows 7が稼働するPCが約1,750万台残存する」と予測しており(https://japan.zdnet.com/article/35131276/)、今回のESUに関する方針転換はこういった状況を鑑みてのものとみられます。

- それでも、特に2023年まで利用した場合にかかる料金を鑑みて、単純に「お金を払えば2020年以降もWindows 7を使い続けられる」とすべきなのかという問題はあり、やはり基本的にはWindows 10へ移行することを前提とし、早急な移行計画をとるべきでしょう。

- もちろん、ESUを購入せず、パッチが提供されない状態のWindows 7あるいはそれ以前のOSを無計画にネットワークに接続するのはもってのほかであり、マルウェアへの感染の可能性、あるいは社内外へマルウェアの拡散や不正アクセスを発生させてしまう可能性を考慮し、適切な隔離等を行うことが重要です。

●個人情報の事故、「メール誤送信」「ノートPCの盗難」などに注意…JIPDEC調べ

- https://webtan.impress.co.jp/n/2019/09/25/34033
- https://privacymark.jp/news/other/2019/0918.html

このニュースをザックリ言うと・・・

- 9月18日(日本時間)、日本情報経済社会推進協会(JIPDEC)より、「個人情報の取扱いにおける事故報告集計結果」(2018年度)が発表されました。

- 同協会が運営するプライバシーマークが付与されている16,275事業者のうち912事業者から、2,323件の個人情報の取扱いにおける事故が報告されており、原因別では「誤送付」が1,345件(57.9%)、次いで「紛失」478件(20.6%)、「その他漏えい」330件(14.2%)、となっています。

- また「誤送付」のより詳しい原因で最も多いのが「メール誤送信」586件(25.2%)とされた他、「紛失」および「盗難」にあった媒体別では「書類」274件(51.5%)が過半数を占める一方で「ノートPC・モバイル機器」が2017年度の32件から2018年度には76件と増加しているとのことです。

AUS便りからの所感等

- 「メール誤送信」および「ノートPC紛失」についてAUS便りで取り上げた例としては、「大学病院、メール誤送信により患者情報3,275人分流出の可能性」(2019/8/19号)、「顧客情報67,000件超を記録したノートパソコンを紛失」(2019/9/17号)等が挙げられます。

- うち後者については、遠隔でPCを使用できなくするソリューションが導入されており、こういった「インシデント発生時にも可能な限り流出の可能性を抑制する」防御策をシステム側で導入することを検討することにより、単に利用する人間に対し「ルールを守らせる」「注意してもらう」ことに依存しない情報流出対策をとって頂ければ幸いです。