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。

●IPA「情報セキュリティ10大脅威 2021」一般利用者向け資料公開

https://internet.watch.impress.co.jp/docs/news/1346519.html
https://www.ipa.go.jp/security/vuln/10threats2021.html

このニュースをザックリ言うと･･･

- 8月23日(日本時間)、IPAより、「情報セキュリティ10大脅威 2021」の一般利用者向け簡易説明資料が公開されました。

- IPAの「情報セキュリティ10大脅威 2021」は1月に概要が発表されて(AUS便り 2021/02/01号参照)以降、2月に詳細の解説書が、3月に「組織編」「個人編」と題した簡易説明資料が順次公開されています。

- 今回公開の資料は、前述の「個人編」からポイントとなる箇所をよりわかりやすく解説し、主に個人のパソコンやスマートフォンでインターネットを利用する人の視点で、インターネットトラブルを避けるための対策に着目したものとなっているとのことです。

- なお、個人向けの10大脅威ランキングは1位「スマホ決済の不正利用」、2位「フィッシングによる個人情報等の詐取」が昨年同様、3位に「ネット上の誹謗・中傷・デマ」が昨年7位からランクアップ等となっています。

AUS便りからの所感等

- 個人向け10大脅威の1位「スマホ決済の不正利用」は昨年1月発表の「情報セキュリティ10大脅威 2020」で1位に初登場した脅威であり、当時急激に普及が進んだQRコードベースの決済を含め、不正な残高引き出しや商品購入等の事件がニュースになっていたもので、資料では対策として「パスワードは使い回しをせず、長く複雑なものとする」「二要素認証・3Dセキュアが利用できるサービスであれば利用する」を挙げています。

- 一方の組織向けランキングも、3位に「テレワーク等のニューノーマルな働き方を狙った攻撃」が初めてランクインする等、2020年の企業におけるITの利用を取り巻く急激な環境の変化、そしてそれを好機とみる攻撃の傾向を色濃く反映したものとなっています。

- 来年1月末には、IPAより今年の傾向を基にした新たなランキングと資料が発表されるとみられますが、まずは今年出ている各種資料に目を通し、注意・対策が必要ながら疎かになっている事項がないか点検することが大事でしょう。

Impress Watch

IPA、「情報セキュリティ10大脅威2021」の一般利用者向け資料を公開

個人における脅威として「ネット上の誹謗・中傷・デマ」のランクが上昇

山田 貞幸　2021年8月27日 15:00

独立行政法人情報処理推進機構（IPA）は、2月に発表していた「情報セキュリティ10大脅威 2021」の一般利用者向け簡易説明資料を、同機構のウェブサイトで公開した。

2020年に発生した情報セキュリティにおける事案から、IPAが脅威候補を選出。約160人のメンバーからなる「10大脅威選考会」が審議・投票を行って決定したもの。個人と組織のそれぞれを対象に、1～10位を発表している。

同機構のウェブサイトでは、全体の詳細な内容や対策をまとめた資料のほか、特定の対象向けにまとめた簡易資料をPDFファイルで公開している。今回公開されたのは「個人編（一般利用者向け）」で、日常的にスマートフォンやPCを利用するにあたって注意すべきポイントが、個人における10大脅威に沿って解説されている。

● Emotet無力化後に別のマルウェア、SMTPを狙う不正アクセス等…IPA、2021年上半期届出事例発表

https://www.ipa.go.jp/security/outline/todokede-j.html
https://www.ipa.go.jp/files/000093083.pdf

このニュースをザックリ言うと・・・

- 8月23日(日本時間)、IPAより、2021年上半期(1月～6月)における「コンピュータウイルス・不正アクセスの届出事例」についての資料が公開されました。

- 資料では、同期間に届出のあったうち主な事例127件を「コンピュータウイルスの検知・感染被害(14件)」「身代金を要求するサイバー攻撃の被害(30件)」「IDとパスワードによる認証を突破された不正アクセス(31件)」「脆弱性や設定不備を悪用された不正アクセス(24件)」「サプライチェーンに関するインシデント(23件)」「その他(6件)」の6種に分類して取り上げています。

AUS便りからの所感

- このうち、例えば「コンピュータウイルスの検知・感染被害」については、猛威を振るったマルウェア「Emotet」が1月27日に無力化(AUS便り 2021/02/01号参照)されて以降、検知や感染およびメールによる拡散を確認していないとする一方で、Emotetに類似した手口をとる「IcedID」、あるいはやはり2020年から被害が拡大していた「Qakbot(Qbot)」といったマルウェアに感染した、あるいはそれらへの感染を狙う返信メールを装った不審なメールの送受信を検知したとする事例が挙げられています。

- また、最も事例が多い分類「IDとパスワードによる認証を突破された不正アクセス」では、31件中19件がメールシステムへの不正アクセス事案で、メール送信用プロトコルのSMTPが「多要素認証などの認証方式には対応していない」ために、そこから不正アクセスを受けた事例も多く含んでいる模様です。

- システム管理者においては、ここで紹介されている各々の事例をもとに、自社で使用しているシステムで防御すべき箇所の洗い出しを行い、必要に応じセキュリティ機構の追加やUTMの採用等で防御を固めることを検討するよう推奨致します。

返信を装った攻撃メールで感染を狙うウイルス被害の事例		
7	2021/3/8	届出者（企業）のメールアカウントが海外から不正アクセスを受け、過去にやり取りしたメールの件名や本文が引用されたウイルス付きメールが複数の宛先に対して送信された。IcedID への感染を狙った攻撃メールと見られ、メールサービスからのウイルス検知の通知により事象を認知した。従来メールシステムへのアクセスは社内ネットワークからのみに制限していたが、テレワーク対応のために社外からの接続を許可していたときに、強度の弱いパスワードを設定していたアカウントが不正アクセスされたことが原因と考えられる状況であった。社外からアクセスする場合はデジタル証明書を利用したデバイス認証を必須とし、またパスワード厳格化のポリシーを適用して再発防止を図った。

メールシステムへの不正アクセスの事例		
45	2021/1/6	届出者（企業）が使用するシステムにおいて、一部のアカウント情報が窃取され、過去にメールを送った届出者の顧客に対して、届出者からの返信を装った不審メールが 1500 通以上送信された。パスワードをさらに強固なものに変更することで対策を行い、さらに本件の調査完了後には不審メールの送信に使われたアカウントを削除する予定である。

● 8月度のフィッシング報告数は53,177件に…過去最多の5万件超え

https://www.antiphishing.jp/report/monthly/202108.html

このニュースをザックリ言うと・・・

- 9月3日、フィッシング対策協議会より、8月に寄せられたフィッシング報告状況が発表されました。

- 8月度の報告件数は53,177件で、7月度(https://www.antiphishing.jp/report/monthly/202107.html)の34,787件から18,390件増加し、過去最多となっています。

- フィッシングサイトのURL件数が9,024件(7月度8,108件)、悪用されたブランド件数が89件(7月度74件)と、こちらも過去最多を記録しています。

- また、当月度におけるフィッシング報告のトピックとして、「ねんきんネット(日本年金機構)」「特別定額給付金申請サイト(総務省)」「コロナワクチンナビ(厚生労働省)」の偽サイトへ誘導するものが挙げられています(AUS便り 2021/08/03号・08/31号参照)。

AUS便りからの所感

- 一時は4万件台を記録した月もみられながら、ここ3ヶ月において3万件台を推移していた報告件数が一気に5万件台を突破、フィッシングサイト件数も徐々に右肩上がりが続いていたものが7月度に急増した勢いを引き続き維持しています。

- 報告全体に対するブランドの割合において、最も多いAmazonで24.8%(7月度33.1%)と分散傾向が続き(これに三井住友カード・エポスカード・イオンカード・PayPay銀行を合わせた5ブランドで約65.8%(7月度 67.8%))、一方でより多くのブランドで大量のフィッシングの報告がされているとのことです。

- 同協議会では、有名ブランドのフィッシングメールの殆どで差出人メールアドレスを正規のドメイン名としていることを挙げ、本物の企業・組織から送信されたメールかどうかを検証可能にするSPFやDMARCといった仕組みを導入することを推奨しており、受信側としてはもちろん、送信側としても取引相手が被害を受けないよう可能な限り取り組んでいくべきでしょう。