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。

●個人情報等の不正持ち出し事案相次いで報告…フィッシングによる流出も

https://www.itmedia.co.jp/news/articles/2108/05/news146.html
https://www.okayama-u.ac.jp/user/hospital/news/detail284.html
https://www.itmedia.co.jp/news/articles/2108/06/news098.html
https://corporate.murata.com/ja-jp/newsroom/news/company/general/2021/0805

このニュースをザックリ言うと･･･

- 8月4日(日本時間)、岡山大学病院より、同院患者のべ269人分の個人情報がフィッシング詐欺によって流出したと発表されました。

- 個人情報は、同院医師によって(大学の規定に反して)持ち出され、個人利用のクラウドサーバーに保存されていましたが、医師がフィッシング詐欺によってアカウント情報を奪取され、個人情報が攻撃者から閲覧可能な状態になったとのことです(発表時点で情報の悪用および病院内システムへの不正アクセスは確認されていないとのことです)。

- 8月5日には、村田製作所より、会計システムの更新業務を日本IBMから再委託されていたIBM中国法人の社員が、業務用パソコンにダウンロードした個人情報等72,460件を個人利用のクラウドサービスに保存していたことが発表されています。

- 持ち出されていた情報は取引先情報30,555件(会社名・住所・氏名・電話番号・メールアドレス・銀行口座)および従業員の関連情報41,905件(従業員番号・会社名・氏名・メールアドレス・銀行口座)を含むプロジェクト管理データで、後日クラウド上のデータは削除され、こちらは第三者からの不正アクセスは確認されていないとのことです。

AUS便りからの所感等

- 前者の事案は、別の大学病院でも「個人利用のクラウドにデータを同期」「フィッシング詐欺による流出」と似通ったケースで発生しており(AUS便り 2021/05/17号参照)、また今回もデータの匿名化を行っていなかったとみられ、それが被害の深刻化につながっている一面もあると推察されます。

- 後者の事案では、村田製作所は前述の通り「第三者がコピー・ダウンロードした事実のないことが確認されたと報告を受け」たものの、データ対象範囲の広さと、取引先情報および個人情報が含まれていることから、発表に至ったとしています。

- また、再委託先において社内監視システムのセキュリティアラートが検知されたことから発覚したことが明らかになっており、クラウド上にデータのアップロードを行った際にアラートが発動したとみられますが、このような外部へ機密データを持ち出そうとする動きを検知さらには遮断するソリューションの採用は、内部関係者のみならず、PCに感染したマルウェアの行動を阻止、もしくはそれが叶わなかったとしても流出の可能性を早期に把握する一助となり、社員への教育・啓発との両輪で実施することを念頭に置くべきでしょう。

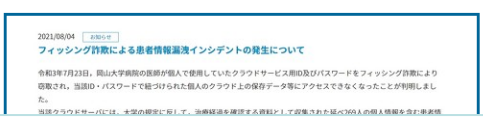
ITmedia NEWS

岡山大病院の医師がフィッシング被害に　私用クラウド奪われ患者269人分の個人情報が流出か

2021年08月05日 18時32分 公開　[松浦立樹，ITmedia]

印刷　209　Share　B!　4

岡山大学病院は8月4日、同病院の医師一人がフィッシング被害に遭い、医師の個人用クラウドに保存していた患者269人分の個人情報が攻撃者から閲覧できる状態になったと発表した。4日時点で情報の悪用や、病院内システムへの不正アクセスは確認されていないという。


2021/08/04
フィッシング詐欺による患者情報漏洩インシデントの発生について
令和3年7月23日、岡山大学病院の医師が個人で使用していたクラウドサービス用ID及びパスワードをフィッシング詐欺により

村田製作所、再委託先が7.2万件の情報を不正持ち出し　IBM中国法人の社員が個人用クラウドにアップロード

2021年08月06日 13時16分 公開　[ITmedia]

印刷　3869　Share　B!　51

村田製作所は8月5日、会計システムの更新を委託していた日本アイ・ビー・エムの再委託先であるIBM中国法人の社員が、約7万2000件の情報を不正に取得していたと発表した。社員は業務用PCから無断でデータを取得し、中国国内のクラウドサービスを使って個人アカウントにアップロードしていたという。既にデータは削除されており「情報の悪用は確認されていない」としている。

●7月度フィッシング報告件数は34,787件、サイトURL数は過去最多更新…対策協議会発表

https://www.antiphishing.jp/report/monthly/202107.html

このニュースをザックリ言うと・・・

－8月4日(日本時間)、フィッシング対策協議会より、7月に同協議会に寄せられたフィッシング報告状況が発表されました。

－7月度の報告件数は34,787件で、6月度(https://www.antiphishing.jp/report/monthly/202106.html)の30,560件から4,227件の増加となりました。

－この他、フィッシングサイトのURL件数は8,108件(6月度 6,394件)と急増、報告全体に対するブランドの割合は引き続き最も多いAmazonが33.1%(6月度 35.8%)、これに三井住友カード・楽天・イオンカード・VISAを合わせた5ブランドで約67.8%(6月度 71.4%)とそれぞれ微減、また悪用されたブランドの件数も74件(6月度 82件)と減少しています。

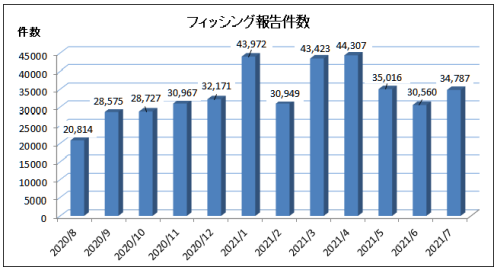
AUS便りからの所感

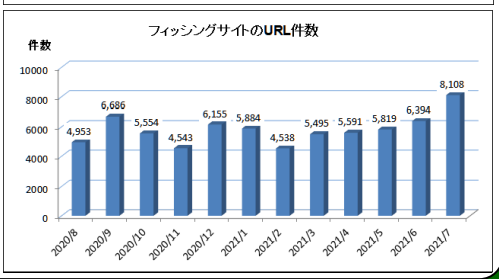
フィッシング対策協議会 Council of Anti-Phishing Japan

－今年に入ってからのフィッシング報告件数は常に3万件を超える水準での乱高下が続いている一方、サイトのURL件数は過去最多だった2020年9月度の6,686件を一気に更新しています。

－同協議会からは8月上旬において、2日に日本年金機構の架空のサービスを名乗るもの(AUS便り 2021/08/03号参照)およびニッセン・クレジットサービス、以後3日～5日にかけて大丸松坂屋カード、アメックス、ジャックスのフィッシングについての注意喚起が出されています(https://www.antiphishing.jp/news/alert/)。

－クレジットカードを中心として、仮想通貨(暗号資産)・ISP・ホスティング事業者・宅配業者(不在通知を騙るもの)およびビットコインを要求する脅迫メールと、フィッシングのトレンドは前月度までの傾向が続いており、これまで同様、各種セキュリティ関連企業・団体の情報、利用しているサービス等からの公式発表、Twitter等での報告に注視する、信頼できないメール・SMSのリンクはクリックせず、サービスの公式サイトにはブックマークからアクセスするといった、慎重な行動を努めていくことを強く推奨致します。





●Kindleに脆弱性、悪意のある電子書籍によりアカウント情報奪取の恐れ…ファームウェア更新の確認を

https://news.mynavi.jp/article/20210810-1943244/
https://blog.checkpoint.com/2021/08/06/amazon-kindle-vulnerabilities

このニュースをザックリ言うと・・・

－8月6日(現地時間)、セキュリティベンダーの米CheckPoint社より、電子書籍リーダー「Kindle」にデバイスの乗っ取りが可能な脆弱性が存在するとして注意喚起が出されています。

－脆弱性は悪意のある電子書籍のインストールで可能になるとされ、デバイス上に保存されているAmazonアカウント情報等の機密情報が奪取される恐れがあるとのことです。

－同社ではAmazon社に脆弱性を報告済みで、4月に脆弱性を修正したファームウェアバージョン5.13.5がリリース済みとのことです。

AUS便りからの所感

TECH+ Powered by マイナビニュース

－注意喚起では、攻撃者が悪意のある電子書籍を特定の言語・世代向けに無料で発行する等により、その言語圏や世代のユーザーに対する効果的な標的型攻撃が行われる可能性が指摘されています。

－脆弱性を突く電子書籍の形式がKindle独自のものである必要があるか否か、逆にPDFやMOBI形式等からも攻撃可能なのかは明言されていないこともあり、とにかくファームウェアのバージョンを最新に保つことが必須と言えます。

－例えばスマートフォンアプリについては「不審なサイトからではなく公式のアプリストアからダウンロードする」といった防御策が有効ですが、Amazon社がKindleストアにおいて同様に電子書籍ファイルのチェックを行うようになるかについても注目されるところと思われます。

Kindleに脆弱性でAmazonアカウント窃取の危険性、バージョンの確認を

2021/08/10 14:05　　著者：後藤大地

世界で最も人気のある電子ブックリーダー「Kindle」は、比較的安全なデバイスと考えられている。しかし、サイバー犯罪者は常にどんなデバイスでも攻撃する隙を探している。この度、その「隙」が明らかになった。1冊の電子書籍をインストールすることで、あなたのAmazonアカウントが窃取されるかもしれないのだ。

Check Point Software Technologiesは8月6日(米国時間)、「Amazon Kindle Vulnerabilities could have led Threat Actors to Device Control and Information Theft - Check Point Software」において、Amazon Kindleに脆弱性が存在すると伝えた。この脆弱性を悪用されると、Kindleの制御権は完全に乗っ取られ、Kindleデバイスに保存されているAmazonアカウントなどの機密情報が窃取される危険性があるという。ユーザーに必要な操作は一冊の電子書籍をインストールするだけだ。