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。

●バイク用品通販サイトからクレジットカード情報流出か…3Dセキュアパスワードも奪取

https://www.tanax.co.jp/motorcycle/topics/900.html

このニュースをザックリ言うと・・・

- 10月27日(日本時間)、バイク用品等を取り扱うタナックス社より、同社通販サイト「TANAXオンラインショップ」が不正アクセスを受け、クレジットカード情報含む個人情報が流出した可能性があると発表されました。

- 被害を受けたとされるのは、2020年12月7日～2021年1月7日に同サイトでクレジットカード決済を行った26名分の氏名・住所・電話番号・メールアドレスおよびカード情報で、カード情報についてはカード番号・名義人・有効期限・セキュリティコードの他、3Dセキュアのパスワードも流出し、一部不正利用も確認されているとのことです。

- 1月7日に流出の懸念について連絡を受け、同15日に決済を停止しており、第三者機関による調査の結果、不正アクセスによるペイメントアプリケーションの改ざんが行われたことが原因とされています。

AUS便りからの所感等

- 今日におけるECサイトからのカード情報流出の事例は「カード情報の入力フォームを改ざんし、入力されたカード情報を奪取する」ものが主流となっており、例えば不正なJavaScriptの挿入により、入力内容が外部に送信される等の手口がとられます。

- 本来の決済手順(カード情報の入力をECサイト上のフォームで行うか・外部サイトに遷移するか等)やカード情報の保存方法(どこでどう保存するか、等)に拘わらず、不正アクセスによる改ざんが発生してしまえば、攻撃者が用意した任意の手順に基づいてカード情報等を入力するよう仕向けられることになるため、脆弱性を突かれることのないよう、ECサイト構築で使用しているものを含めサーバー上の各種ソフトウェアは常に最新のバージョンに保ち、WebアプリケーションにSQLインジェクション等の脆弱性があれば確実に対策し、かつ不正なリクエストを検知・遮断するWAFやIDS・IPS等のソリューションの導入も含めたサイトの防御を行うことが重要となります。

- 今回は偽の3Dセキュア入力画面へ誘導するよう改ざんを行ったとみられますが、現状本物の3Dセキュア入力画面であってもドメイン名から信頼のおけるサイトか推測しにくいケースが多くみられており、クレジットカード業界側においても、3Dセキュア入力画面等をクレジットカード会社のドメイン下で用意することを必須とするといった、これまで着手していない取り組みに踏み込むべきと考えます。

TANAX MOTORCYCLE

2021年10月27日

お客様各位

タナックス株式会社
代表取締役社長　田中　浩二
千葉県流山市後平井107-3

弊社が運営する「TANAXオンラインショップ」への不正アクセスによる
個人情報漏えいに関するお詫びとお知らせ

このたび、弊社が運営する「TANAXオンラインショップ」におきまして、第三者による不正アクセスを受け、お客様のクレジットカード情報（26件）が漏洩した可能性があることが判明いたしました。
お客様をはじめ、関係者の皆様に多大なるご迷惑及びご心配をおかけする事態となりましたこと、深くお詫び申し上げます。
尚、個人情報が漏洩した可能性のあるお客様には、本日より電子メールおよび電話にてお詫びとお知らせを個別にご連絡申し上げております。

●10月度フィッシング報告数は48,740件…12か月連続での3万件超え

https://www.antiphishing.jp/report/monthly/202110.html

このニュースをザックリ言うと・・・

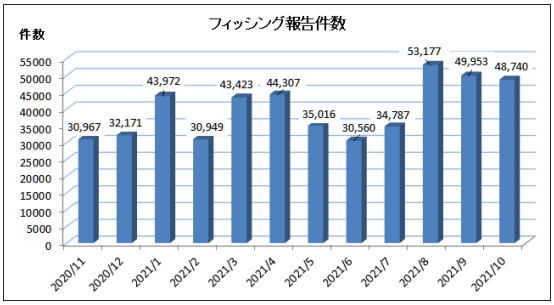
－11月4日、フィッシング対策協議会より、10月に寄せられたフィッシング報告状況が発表されました。

－10月度の報告件数は48,740件で、8月度(https://www.antiphishing.jp/report/monthly/202109.html)の49,953件からは1,213件減少となっている一方、フィッシングサイトのURL件数は7,418件(9月度6,636件)と増加、また悪用されたブランド件数は77件(9月度76件)となっています。

－報告全体に対するブランドの割合については、最も多いAmazonは28.2%と9月度(30.6%)より減少、これにメルカリ・三井住友カード・ETC利用照会サービス・楽天を合わせた5ブランドで約66.6%(9月度 64.0%)、また1,000件以上の報告があったブランドが11あり、これらで全体の約83.2%を占めたとしています。

AUS便りからの所感

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



－2020年4月に初めて1万件を超え(AUS便り 2020/05/11号参照)て以降、報告件数はほぼ右肩上がりの傾向を続け、同年11月に3万件を突破(同2020/12/07号参照)してからは、ここまで12ヶ月連続で3万件を切ることなく高水準が続いています。

－同協議会では、調査用メールアドレス宛に10月に届いたフィッシングメールのうち約89.6%が正規のメールアドレスを用いた「なりすまし」であったとしている一方、報告の多くはDMARCによる送信元メールアドレス検証を行っていないISPやモバイルのメールサービス利用者から寄せられていたとしており、DMARC検証および迷惑メールフィルターによってこういった「なりすまし」メールの多くが排除されているものと推測しています。

－自社で独自にメールサーバーを立てているケースにおいては、従来から使われている迷惑メールフィルターの他、送信元IPアドレスのSPFによる検証、そして前述のDMARCによる検証といった機構を導入することにより、メール文面に違和感のない見破ることが困難なフィッシングメールであっても効果的に検出・遮断を行い、自社ユーザーや取引先ユーザーに対するフィッシングからの保護も行うことを推奨致します。

●病院システムがランサムウェア感染、予約外患者受け入れできず

https://www.topics.or.jp/articles/-/612733
https://www.topics.or.jp/articles/-/614361
https://www.topics.or.jp/articles/-/615382
http://www.handa-hospital.jp/

このニュースをザックリ言うと・・・

－10月31日(日本時間)、徳島県つるぎ町立半田病院より、同病院の電子カルテシステムがランサムウェアに感染したと発表されました。

－同日未明に英語の文書がプリンターから印刷されていることが発見されて感染が発覚したもので、カルテシステムのメインサーバーの他、バックアップサーバーにもランサムウェアが侵入している可能性があり、連係している検査システム・画像システム・診療報酬システムも使用不可状態になっているため、外来患者について予約済みのもの以外は受け入れられない等の状態となっているとしています。

－サーバーに保存されていた患者約85,000人分の個人記録に関して流出の有無は不明とされている一方、患者情報等の共有のため当該システムとVPN経由で接続していた県内の他の施設には影響は出ていないとのことです。

AUS便りからの所感

徳島新聞 電子版
The Tokushima Shimbun


半田病院の電子カルテがランサムウエアに感染　新規診療などの受け入れを当面停止

10/31 21:10

シェア 431　ツイート　LINEで送る

記者会見で謝罪する病院幹部＝つるぎ町の半田病院

拡大する

つるぎ町立半田病院は31日、電子カルテシステムが身代金要求型ウイルス「ランサムウエア」に感染したと発表した。感染したのはシステムのメインサーバーで、患者約8万5千人分の個人記録が保存されている。個人記録の流出の有無は不明。サーバーへのアクセスができないため、11月1日から新規診療などの受け入れを当面停止する。

半田病院によると、感染によって、電子カルテのメインサーバーへのアクセスが不能となった。バックアップサーバーにもウイルスが侵入している可能性があるため、安易にアクセスできない状態という。電子カルテシステムと連係した検査システムや画像システム、診療報酬システムなども使用不能となった。

－11月7日の時点でもシステム復旧の目途は立っておらず、カルテについては一時手書きで対応、のち古いPCによるオフラインでの入力・印刷等の体制を整えているとのことです。

－オフラインでの入力データを外部PCとUSBメモリー等の媒体で共有しようとする場面では、媒体の紛失の事例や、接続したPCから媒体にマルウェアが感染し、別のPCにも接続することにより、オフラインであっても感染が拡大する事例がこれまでにも報告されていることには注意が必要です。

－特にランサムウェアが話題になった頃から、万が一の感染時に復旧を行うことへの備え、またバックアップシステムやデータも感染や暗号化・破壊で使えなくなる恐れについても考慮することが叫ばれており、「バックアップは複数箇所にとり、うち1つをオフラインに保管する」あるいは「データの書き換えが不可能な場所にバックアップを取る」等も念頭に置いたシステム構築が、中小企業であっても必要となるでしょう。