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。

●カタログギフト会社のECサイトに不正アクセス…個人情報150,236件・カード情報28,700件流出か

https://www.itmedia.co.jp/news/articles/2207/13/news153.html
https://www.harmonick.co.jp/announcement

このニュースをザックリ言うと･･･

- 7月13日(日本時間)、カタログギフトを取り扱うハーモニック社より、同社ECサイトが不正アクセスを受け、個人情報およびクレジットカード情報が流出した可能性があると発表されました。

- 被害を受けたのは、2020年11月14日までに同サイトで商品購入または会員登録を行った最大150,236名分の個人情報(氏名・住所・電話番号・メールアドレス・性別・生年月日)および2020年11月14日～2021年11月11日に同サイトでカード決済を行った最大28,700名分のクレジットカード情報(名義・番号・有効期限・セキュリティコード)とされています。

- 2月8日に一部カード会社から流出の懸念について連絡を受け、カード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

- ECサイトからのカード情報漏洩は、Webサイトの注文ページ周り等を改ざんし、偽の決済ページへの誘導や、フォームに入力された内容の攻撃者への送信を行うよう改変する等により、セキュリティコードも含めたカード情報の奪取を行う手口が主流となっており、AUS便りでも度々取り上げています。

- 同社では、できる限りのセキュリティ対策を施していたものの、システムの比較的手薄な部分を狙われ、不正アクセスを許すこととなったとしていますが、サイトやシステム全体のセキュリティ強度は「最もセキュリティの弱い部分」次第であり、「蟻の一穴」の破れが致命的な損害をもたらすものと心得なければなりません。

- 独自にECサイトを立ち上げる場合には、Webアプリケーションやサーバーの脆弱性について確実に修正・対策を行い、攻撃者による侵入や改ざんの余地をなくすよう努めることが肝要であり、加えて攻撃の形跡・兆候を検知・遮断するためのIDS・IPSおよびWAFの設置、および情報の流出を食い止める出口対策についても検討することを強く推奨致します。

ITmedia NEWS

カタログギフト販売サイトに不正アクセス　最大2万8700件のクレカ情報、最大15万236件の個人情報が漏えいか

2022年07月13日 16時03分 公開　　[松浦立樹，ITmedia]

カタログギフト販売ECサイト「カタログギフトのハーモニック」（以下、ECサイト）を運営するハーモニック（新潟県三条市）は7月13日、第三者による不正アクセスを受け、利用者のクレジットカード情報と個人情報が漏えいした可能性があると発表した。カード情報は最大2万8700件、個人情報は最大15万236件漏えいした可能性があるという。

漏えいした可能性があるカード情報は、2020年11月14日～2021年11月11日にECサイトでカード決済をした人（最大2万8700人）のカード名義人名とカード番号、有効期限、セキュリティコード。

漏えいした可能性のある個人情報は、2020年11月14日までにECサイトで商品を購入、または会員登録した利用者全て（最大15万236人）の氏名と住所、電話番号、メールアドレス、性別、生年月日。また、名入れ商品の購入者（最大5445人）は、子どもの氏名と性別、生年月日、出産時の体重と身長も漏えいした可能性がある。

●バンダイナムコHD、海外グループ会社がランサムウェア攻撃受ける

https://www3.nhk.or.jp/news/html/20220713/k10013716411000.html
https://www.itmedia.co.jp/news/articles/2207/14/news102.html
https://www.bandainamco.co.jp/files/202207E4B88DE6ADA3E382A2E382AFE382BBE382B9E382B3E3_2.pdf

このニュースをザックリ言うと･･･

- 7月13日(日本時間)、バンダイナムコホールディングス社より、日本を除くアジア地域の複数のグループ会社が不正アクセスを受けたと発表されました。

- 発表によれば、不正アクセスは同3日に発生し、被害を受けたサーバー・PCには、日本を除くアジア地域のトイホビー事業に関わる顧客情報が含まれていた可能性があるとしています。

- また、NHK等の報道によれば、「ALPHV」と名乗るハッカー集団からのランサムウェア攻撃によるものとみられ、グループ会社から奪取した情報を公開すると主張しているとのことです。

AUS便りからの所感

- 同社グループでは既に被害の拡大を防ぐためのサーバーへのアクセス遮断等の対応を行っているとのことで、原因究明と調査結果の適宜公表、および再発防止の施策に取り組む等としています。

- 発表・報道による限り、日本国内の拠点には被害は及ばなかった模様ですが、例えば全ての拠点でVPN接続が行われ、拠点間の通信がフィルタリングなしで行われているような設定の場合、一つの拠点でランサムウェア感染や攻撃者の侵入の発生からたちどころに他の拠点をターゲットとした攻撃に発展することに注意が必要です。

- 全ての拠点において「攻撃者が侵入しない」「マルウェアに感染しない」よう防御を固めることはもちろん、万一これを破られて侵入等を受けた場合をも想定したさらなる防御にも十分な備えを行うことが肝要です。

NHK

バンダイナムコHDのグループ会社にサイバー攻撃

2022年7月13日 20時21分　IT・ネット

ゲームやおもちゃなどの大手メーカー「バンダイナムコホールディングス」の、アジアにあるグループ会社が、身代金要求型のコンピューターウイルス「ランサムウエア」によるサイバー攻撃を受けたことがわかりました。会社は「現時点で事業に大きな影響はないが、顧客の情報などが漏えいした可能性があり調査中だ」としています。

●農研機構サイトが一時改ざんされる…個人情報流出なし

https://ibarakinews.jp/news/newsdetail.php?f_jun=16578812256623
https://www.naro.go.jp/publicity_report/press/laboratory/naro/154067.html

このニュースをザックリ言うと･･･

- 7月15日(日本時間)、国立研究開発法人 農業・食品産業技術総合研究機構(農研機構)より、同機構が運営するWebサイトの一つが不正アクセスを受け、コンテンツが改ざんされる被害を受けていたと発表されました。

- 被害を受けたのは「イネ QTL 遺伝子情報データベース」Webサイトで、同14日13:07～17:49の間、漫画調のスロットマシンが表示される状態になっていたとされています。

- 同14日夕方に研究者が改ざんを発見してサイトへのアクセスが遮断されており、個人情報の流出等は確認されていないとのことですが、同機構ではこの間にサイトにアクセスしたユーザーに対し、念の為マルウェアチェックを行うよう呼び掛けています。

AUS便りからの所感

- Webサイトの改ざんは、単なる愉快犯的な行為から、前述したようなサイト閲覧者に対しマルウェア感染を狙うケース(一時はFlash Playerの脆弱性を突くものが多くありましたが、今日では不正な実行ファイルのダウンロードが主流とみられます)や、密かにフィッシングサイトが設置されたり、場合によってはWebサーバーからの不審なメールを大量発信するような仕掛けがなされたりするケースがあり、改ざんに至る経路も、Webサーバーに直接侵入するもの、CMS(コンテンツ管理システム)の脆弱性(SQLインジェクション等)を突くもの等様々です。

- 報道によればサーバーはクラウド上に設置されており、それ自身に個人情報は保存されておらず、また他のサーバーへ連鎖的に不正アクセスを行うようなこともできなかったと推察され、例えば組織のネットワーク上に設置したサーバーを公開する形(オンプレミス)であったとしても、サーバーをDMZに設置したり、サーバーから内部のネットワークへアクセスできないよう制限する設定を行ったりすることは、いわゆる「出口対策」の一環として有効でしょう。

茨城新聞 クロスアイ

農研機構サイトが一時改ざんされる　個人情報流出なし

0件

2022年7月16日(土)

【AD】

農業・食品産業技術総合研究機構(茨城県つくば市)は15日、ウェブサイトが一時改ざんされたと発表した。14日午後に漫画調のスロットマシンが表示されるようになっていた。サイトから個人情報の流出は確認されていないという。

農研機構によると、14日午後4時ごろ、「イネ　QTL　遺伝子情報データベース」が改ざんされているのを管理していた研究者が気付いた。同5時49分、サイトへのアクセスを遮断した。この間、200～300件のアクセスがあったという。