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。

●EC-CUBEを使ったWebサイトで情報漏洩被害が増加…経産省・IPAが注意喚起

https://news.mynavi.jp/article/20191227-946428/
https://www.meti.go.jp/press/2019/12/20191220013/20191220013.html
https://www.ipa.go.jp/security/announce/alert20191225.html

このニュースをザックリ言うと･･･

- 12月20日(日本時間)に経済産業省より、同25日には情報処理推進機構(IPA)より、ECサイト構築用ソフトウェア「EC-CUBE」の脆弱性を突いた攻撃が増加しているとして注意喚起が出されています。

- 攻撃により、ECサイトの改ざんが行われ、クレジットカード番号等が窃取されるといった被害が多発しており、2019年の時点で約14万件のカード情報が漏洩しているとのことです。

- IPAでは、自身のサイトでEC-CUBEが使われているかとそのバージョンを確認すること、最新でない場合は速やかにアップデートすること、開発元のイーシーキューブ社が提供する情報に基づいてセキュリティ対策を実施することを推奨しています。

AUS便りからの所感等

- ECサイトのサーバー側においてクレジットカード情報を保存・処理あるいは通過させない、いわゆる「非保持化」が進んでいる状況ですが、サイトの脆弱性を突かれ改ざんが行われた場合、この「非保持化」が維持されながらも、入力したカード情報を決済業者ではなく攻撃者へ送信するよう密かに細工することも可能であり、実際に攻撃者の手口もそれを狙うケースが増えています。

- サービスを信頼してサイトにアクセスし、かつ重要な情報を入力してくれるユーザーを危険に晒すことのないよう、使用するソフトウェアを最新のバージョンに保ち、また脆弱性を悪用しようとする不正なリクエストをWAF等で検知・遮断するといった対策も併せて行うことを推奨致します。

経済産業省
Ministry of Economy, Trade and Industry

本件概要

- 株式会社イーシーキューブが開発・提供するインターネットサイト構築パッケージ「EC-CUBE」の脆弱性等を突いたインターネットショップのサイトの改ざん等により、クレジットカード番号等が窃取されるといった被害が多発しております。
- 2019年現在までにインターネットショップが公表した漏えい事案において、約14万件のクレジットカード番号等が漏えいしていることが確認されております。
- このような甚大な被害が発生している状況に鑑み、インターネットショップの皆様におかれましては、「EC-CUBE」のご利用状況について再度検証を行い、ご利用を継続する場合には、的確な安全対策を行ってください。
- ご対応についてご不明な点がありましたら、下記の問い合わせ窓口までご連絡ください。

【本件に関するお問い合わせ窓口】

株式会社イーシーキューブ

電話：06-4795-7506

受付時間：10時～12時、13時～17時 土曜日、日曜日・祝日及び年末年始を除く

イーシーキューブ ホームページ

※本件に関する詳細は以下をご覧ください

イーシーキューブ：サイト改ざんによるクレジットカード流出被害が増加しています

● Facebookユーザー2億6,700万件以上の個人情報、ネットに流出

https://www.afpbb.com/articles/-/3260477
https://gigazine.net/news/20191220-facebook-users-data-exposed-online/

このニュースをザックリ言うと･･･

- 12月19日(現地時間)、米Facebookより、同ユーザー2億6,714万436件の個人情報(ID・電話番号・名前)を含んだデータベースがオンライン上に公開されていたと報告を受けていたことが発表されました。

- データベースは12月4日頃から作成され、同12日にハッカーのフォーラムで公開されたとみられ、これを発見したセキュリティ研究者が14日にISPに通報した後、19日に削除されたとのことです。

- Facebookでは近年ユーザー情報の大規模な流出がたびたび発覚しており、2019年4月に5億件以上(AUS便り2019/4/15号参照)、同9月にも4億件以上(同2019/9/17号参照)の情報が公開状態にあったと発表されています。

AUS便りからの所感

- 前述のうち2019年4月の件では、サードパーティー(外部企業)が情報を保存していたデータベースが設定ミスで公開状態にあったことが原因でしたが、今回のケースはそういった偶然に起こったものではなく、悪意のある人物が意図的に流出させた可能性が高いとみられています。

- また、情報の取得については、何らかのセキュリティホールを突いた可能性の一方で、単にFacebook上で公開されているプロフィールページから取得した可能性も指摘されています。

- SNS上等で公開状態の電話番号を収集されることにより、攻撃者がSMSでスパムを送信する可能性等が指摘されています(メールアドレスでも同じことが言えますが)ので、各種情報について、特に登録する必要がある場面以外ではむやみに登録せず、また適宜公開範囲を限定するよう設定しているか確認することを推奨致します。

●Wi-Fiルーターを安全に使うための注意点、業界団体が提言

https://securityinsight.jp/news/13-inbrief/4034-191223-1
https://dlpa.jp/pdf/dlpa_pr_20191218.pdf
https://www.jpcert.or.jp/newsflash/2019121801.html

このニュースをザックリ言うと･･･

- 12月18日(日本時間)、家庭用ルーター・NASのメーカー等が参加する一般社団法人デジタルライフ推進協会(DLPA)より、「ご家庭でWi-Fiルーターをより安全にお使い頂くために」と題しての提言が発表され、同日JPCERT/CCでも取り上げられました。

- 提言は大きく「最新のファームウェアの適用」「デフォルトの設定からの見直し(パスワードの変更等)」の二つからなり、前者では、アップデート手順をマニュアル等で確認するのみならず、使用している機種について型式番号等の詳細を把握すること、またサポート期間が終了しアップデートが提供されない機種について使用を停止することを挙げています。

- 後者では、第三者に機器を悪用されないよう、パスワードにデフォルトのものや安易な文字列を設定しないことの他、UPnPといった機能が利用していないのに有効になっていないか確認すること等を挙げています。

AUS便りからの所感等

- この提言を取り上げたJPCERT/CCでは、デフォルトのIDやパスワードを悪用されて侵入され、マルウェア感染などの被害に繋がったとの報告を複数受けているとしています。

- DLPAでは、ファームウェアを自動で更新する機能がついているものや、管理画面にログインするためのID・パスワードについて機器毎に別々のものを登録している機種を推奨ルーターとし、DLPAに加盟するメーカー4社もこれに適応する機種の一覧を挙げており、購入の際には十分参考にするのが良いでしょう。

- 提言は主に家庭用機器を対象としていますが、企業・組織においても、内部で利用している全ての機器について機種情報等を把握し、適切な設定が行われているか等を管理しておくことは当然重要です。