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。

●ICT教育アプリの開発環境に不正アクセス、国内外ユーザー12.7万件の個人情報流出

https://www.nikkei.com/article/DGXZQOUC186KP0Y3A011C2000000/
https://www.casio.co.jp/release/2023/1018-incident/
https://classpad.net/jp/news/040/

このニュースをザックリ言うと･･･

- 10月18日(日本時間)、カシオ計算機より、同社が運営する教育用アプリ「ClassPad.net」の開発環境が不正アクセスを受け、個人情報等が流出したと発表されました。

- 被害を受けたのは、国内ユーザー91,921件(個人と1,108の教育機関)・海外ユーザー35,049件(148ヶ国・地域)の氏名・メールアドレス・国と地域・学校名・学年・学級名・出席番号(学籍番号)・購買に関する情報・サービス利用履歴およびニックネームで、総アカウント数の約7割分とされています(クレジットカード情報は保持していないとのことです)。

- 10月11日に開発環境上のデータベースにおいて障害が発生していたのをきっかけに不正アクセスが発覚したとしており、攻撃を受けた原因については運用管理上の問題でネットワークセキュリティ設定の一部が解除されていたためとしています。

AUS便りからの所感等

- アカウント情報自体および個人の住所が流出したという発表はありませんが、国内外の教育機関で利用されているサービスからの情報漏洩であり、特にメールアドレスの不正利用、迷惑メール送信の被害が懸念されるところです。

- 開発環境に対する第三者からのアクセスが可能になっていたということで、本番環境と同様にセキュリティ診断を行うというわけにはいかなくとも、外部からアクセスできないことを自動的にチェックする機構やサービスの導入検討は有用でしょう。

- 開発環境上のデータベースで本番環境と同様の実際のデータを用いていた可能性があり、万が一の不正アクセス発生時のリスクを考慮し、ダミーデータやマスクされたデータを利用することも留意しましょう。

日本経済新聞

カシオ、教育アプリで不正アクセス　12万件超の情報流出

エレクトロニクス　＋フォローする
2023年10月18日 16:36

カシオは学校向けに辞書や教材などが使える教育アプリを提供している

カシオ計算機は18日、教育アプリ「ClassPad.net（クラスパッド　ドット　ネット）」で不正アクセスがあったと発表した。国内外で契約している学校名、氏名やメールアドレスなどの個人情報12万件超が流出した。総アカウント数の約7割にあたる。

11日に、カシオが管理しているアプリの開発環境データベースで外部からのサイバー攻撃を確認した。5日時点で犯行声明が出ていたという。サイバー攻撃のあった原因について同社は「システムの誤操作、不十分な運用管理によりネットワークセキュリティー設定の一部が解除状態だった」と説明した。

●国内ドメイン名の不正移管事例、JPCERT/CCが注意喚起

https://news.mynavi.jp/techplus/article/20231027-2802853/
https://blogs.jpcert.or.jp/ja/2023/10/domain-hijacking.html

このニュースをザックリ言うと･･･

- 10月25日(日本時間)、JPCERT/CCより、7月上旬に日本国内でドメイン名の不正移管事例が発生したとして注意喚起が出されています。

- 攻撃者はドメイン名レジストラーのフィッシングサイトを検索エンジンの広告に表示させ、ドメイン名管理者を誘導、入力されたアカウント情報で不正ログイン、登録メールアドレスの変更とドメイン移管ロックの解除を行い、移管手続きを行ったとしています。

- JPCERT/CCでは、フィッシングの回避策として「検索サイトで表示されたリンクが正しいものと断定せず、確認済みの公式アプリや、Webブラウザーにブックマークしていたリンクからアクセスする」、また外部から不正にログインされないよう「サイトの提供するセキュリティ機能（2段階認証など）を活用する」「簡単なパスワードや、同じパスワードの使いまわしを避ける」ことを推奨しています。

AUS便りからの所感

- 2019年4月に国内の.jpドメイン名で同様の事例が発生した際、実行者は「移管オファーを行い元所有者が移管オファーを承認しただけだった」と主張したとされており、このときはドメイン名所有者のアカウント乗っ取りもなく、一定期間以内に所有者側が移管を拒否しなかったことにより、JPRSでのルールに基づき移管が成立したとみられます(AUS便り2019/4/8号)。

- こういった不正移管への対策として既にレジストリーロック等の機構が存在するものの、今回のようにアカウントの乗っ取りに成功した場合に解除・回避される可能性があることに十分に注意し、サーバー管理者等も含め、JPCERT/CCが推奨するような防御策を確実にとることが重要です。

TECHF Powered by マイナビニュース

ドメインハイジャック攻撃に警戒を、国内のドメインが不正に移管

掲載日 2023/10/27 07:29　　著者：後藤大地

JPCERTコーディネーションセンター(JPCERT/CC: Japan Computer Emergency Response Team Coordination Center)は10月25日、「フィッシングサイト経由の認証情報窃取とドメイン名ハイジャック事件 - JPCERT/CC Eyes | JPCERTコーディネーションセンター公式ブログ」において、2023年7月上旬に日本国内で利用されていたドメインが不正に移管されるドメインハイジャックの事例を確認したとして、注意を喚起した。

●大学教員への講演依頼を騙る標的型攻撃…マルウェア感染で個人情報等4,000件以上流出か

https://mainichi.jp/articles/20231024/k00/00m/040/149000c
https://www.u-tokyo.ac.jp/focus/ja/press/z0109_00952.html
https://piyolog.hatenadiary.jp/entry/2023/10/25/164100
https://www.nisc.go.jp/pdf/press/20221130NISC_press.pdf

このニュースをザックリ言うと･･･

- 10月24日(日本時間)、東京大学より、同大学院総合文化研究科・教養学部が保有するPCがマルウェアに感染し、保存されていた個人情報等が流出した可能性があると発表されました。

- PCは同学部の教員が在宅勤務時に利用していたもので、教員宛に送られてきた標的型攻撃メールからマルウェアに感染したとされています。

- 流出の可能性がある情報は、同大学教職員・学生・卒業生2,409件、教員が在籍する学会関係1,082件、非常勤講師等で担当する授業の受講生796件の個人情報の他、過去の学生成績評価・試験情報24件、所属教員の評価等30件とされています。

AUS便りからの所感

- 攻撃メールは実在の組織からの講演依頼を騙るもので、一部報道ではやり取りの過程でメール中のURLにアクセスした、あるいはファイルを開いたことにより、マルウェアに感染したものとされています。

- セキュリティ研究者のpiyokango氏は、関係は不明ながらも、今回と類似した手口の学術関係者・シンクタンク研究員等を標的とする攻撃について、2022年11月に警察庁とNISCが注意喚起を出していたことを取り上げています。

- 在宅勤務中のPC利用時を狙われてPC上のデータが流出したという事態であり、防御が手薄になる可能性がある状況とはいえPCでは必ずアンチウイルス(Windows附属のもの含む)を有効化すること、また標的型攻撃という攻撃方法の存在をはじめ、報告されている手口の情報について収集あるいは周知されることが肝要です。

毎日新聞

東大教員パソコンにマルウエア　学生らの情報4000件以上流出か

東京大学＝東京都文京区で2021年6月15日、武市公孝撮影

東京大は24日、教員が使用していた大学のパソコンがサイバー攻撃を受けてマルウエア（悪意のあるプログラム）に感染し、学生や卒業生の名前や住所など4000件以上の情報が流出した可能性があると発表した。特定組織の情報を盗むことなどを目的とする「標的型攻撃メール」を受信したことによるものという。