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。

●オムニ7アプリのソースコードに漏洩の疑い…「GitHub」上で閲覧可能な状態に

https://www.businessinsider.jp/post-195187

このニュースをザックリ言うと・・・

- 7月24日（日本時間）、一部ネットメディアより、セブン&アイグループが提供するモバイルアプリ「オムニ7アプリ」のソースコードがコード管理サイト「GitHub」において閲覧可能な状態だった、とする記事が発表されました。

- 記事によれば、今月上旬に発生した「7pay」における不正購入等の問題に関連して、同グループのオムニ7アプリの解析を行っていた外部のエンジニアが解析中に表示されたアプリのアクセス先サーバの名前をGitHub上で検索したことがきっかけとのことです。

- ソースコードは2015年5月～7月頃時点のものとされ、7月10日には削除されている他、GitHub上でフォーク（他のユーザによる複製）されたものも同18日に開発に関わったとみられる業者からの削除申し立てがされたとのことです。

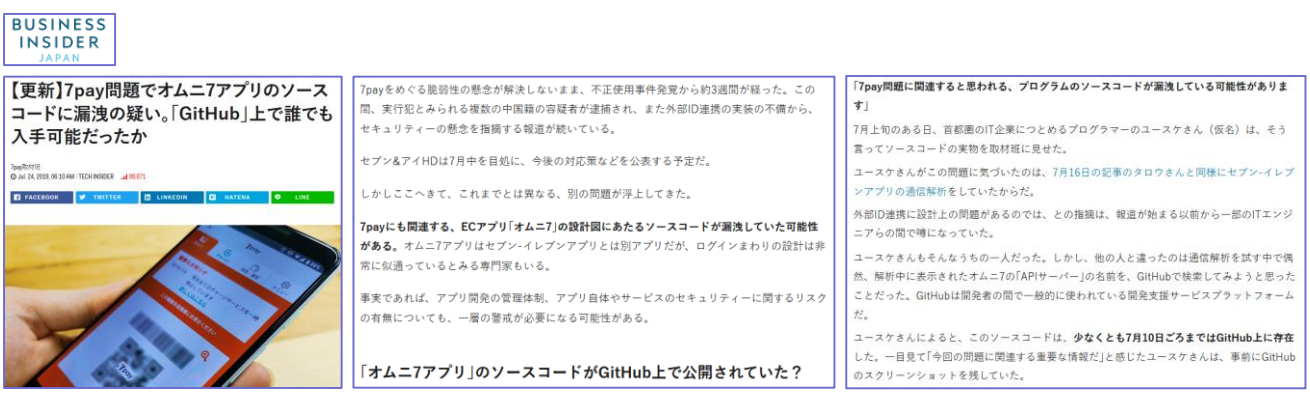
AUS便りからの所感等

- GitHubはソースコードやドキュメント等を管理（複数名による分散管理）ないし不特定多数と共有するためのサイトとして特に開発者に絶大な人気を持っていますが、2019年1月まではリポジトリ（ソースコードの保管庫）を非公開にする設定が有料ユーザのみに制限されていた経緯があります。

- ソースコードのバージョンが古い等の状況から、「アプリの開発チームが正式にGitHubを使用していた訳ではなく開発者の一人が個人的にアップロードしていた」こと、第三者に開示することを意図していなかったであろうソースコードを「当時有料ユーザ契約をしなかったことにより公開状態で管理していた」こと、そして「GitHubを使わなくなり削除することを怠っていた」こと、等が推測されます。

- 全てのデータを社内等のサーバに保存する「オンプレミス」での開発に慣れ、それしか知らない状態でチームや個人が安易に「クラウド」を採用することは危険であり、「基本的に非公開とし誤って公開されていないか確認する」「公開状態のリポジトリにセンシティブなデータ(パスワードやセキュリティトークン等)を含んだ状態でアップロードしない」「管理対象を把握し不要となったものは可及的速やかに削除する」等、利用にあたって注意すべきことを事前に啓発し、適切に利用させることがクラウドの利用にあたっては最低限必要となります。

- 一方のオンプレミスにおいても「サーバが外部にないから安全」という認識でいるのではなく、クライアントPCに感染したマルウェア等を経由して不正アクセス等が行われる可能性に注意し、UTMの設置やネットワークセグメントの分割等といった防御策をとることが重要です。


BUSINESS INSIDER JAPAN

【更新】7pay問題でオムニ7アプリのソースコードに漏洩の疑い。「GitHub」上で誰でも入手可能だったか

Jul. 24, 2019, 09:10 AM | TECH INSIDER

FACEBOOK TWITTER LINKEDIN HATENA LINE

7payをめぐる脆弱性の懸念が解決しないまま、不正使用事件発覚から約3週間が経った。この間、実行犯とみられる複数の中国籍の容疑者が逮捕され、また外部ID連携の実装の不備から、セキュリティーの懸念を指摘する報道が続いている。

セブン&アイHDは7月中を目処に、今後の対応策などを公表する予定だ。

しかしここへきて、これまでとは異なる、別の問題が浮上してきた。

7payにも関連する、ECアプリ「オムニ7」の設計図にあたるソースコードが漏洩していた可能性がある。オムニ7アプリはセブン-イレブンアプリとは別アプリだが、ログインまわりの設計は非常に似通っているとみる専門家もいる。

事実であれば、アプリ開発の管理体制、アプリ自体やサービスのセキュリティーに関するリスクの有無についても、一層の警戒が必要になる可能性がある。

「オムニ7アプリ」のソースコードがGitHub上で公開されていた？

「7pay問題に関連すると思われる、プログラムのソースコードが漏洩している可能性があります」

7月上旬のある日、首都圏のIT企業につとめるプログラマーのユースケさん（仮名）は、そう言ってソースコードの実物を取材班に見せた。

ユースケさんがこの問題に気づいたのは、7月16日の記事のタロウさんと同様にセブン-イレブンアプリの通信解析をしていたからだ。

外部ID連携に設計上の問題があるのでは、との指摘は、報道が始まる以前から一部のITエンジニアらの間で噂になっていた。

ユースケさんもそんなうちの一人だった。しかし、他の人と違ったのは通信解析を試す中で偶然、解析中に表示されたオムニ7の「APIサーバー」の名前を、GitHubで検索してみようと思ったことだった。GitHubは開発者の間で一般的に使われている開発支援サービスプラットフォームだ。

ユースケさんによると、このソースコードは、**少なくとも7月10日ごろまではGitHub上に存在**した。一目見て「今回の問題に関連する重要な情報だ」と感じたユースケさんは、事前にGitHubのスクリーンショットを残していた。

●年金機構、個人情報含む記録媒体紛失…データは暗号化、漏洩は確認されず

https://news.tv-asahi.co.jp/news_society/articles/000160311.html

このニュースをザックリ言うと・・・

- 7月21日（日本時間）、日本年金機構の東京・有明の事務センターにおいて、個人情報を含む年金関連データを記録した媒体が紛失していたと報じられました。

- 媒体は、国民年金未納者に対する電話催促や訪問の業務を年金機構から委託された業者が業務報告のために同センターに送付していたもので、未納者約23,000人分の個人情報（氏名・住所・電話番号等）が含まれている可能性があるとされていました。

- データは同センター内のPCでしか閲覧できないよう暗号化されており、漏洩は確認されていないとのことで、同センターではデータ自体を閲覧できなくする対応を行ったとしています。

AUS便りからの所感等

- かつて同機構から大規模な個人情報流出が発生したこともあり、紛失そのものを批判する報道が見られましたが、報道内容を見る限りでは、漏洩対策や事後対応は適切に機能していたように見受けられます。

- データの暗号化にあたっては、それを第三者に解読されてしまう可能性を意識し、今回とられていたとされる「政府推奨の高度な暗号化措置」、例えば「AES」のような強力な暗号等を用いているかはもちろん、暗号化に用いている鍵やパスワードが脆弱でないか等、あらゆるポイントにおいて十分に注意を払うことが肝要です。


テレ朝▶news

約2万3000人分の個人情報入りDVD紛失　日本年金機構 [2019/07/23 18:50]

日本年金機構が国民年金の未納者約2万3000人分の個人情報が入ったDVDを紛失していたことが分かりました。

日本年金機構によりますと、機構は国民年金の未納者への支払いの催促を外部の業者に委託していて、この業者から3日に納付の状況などを記録したDVD8枚を受け取りました。9日になって、機構の職員が紛失に気付いたということです。紛失したDVDには、国民年金の未納者約2万3000人分の基礎年金番号や生年月日、電話番号などが記録されていました。DVDは元々、機構の事務センターなどの限られたパソコンでしか内容を見られないように暗号化されていて、紛失後にこうしたパソコンでも見られないようにする措置を取りました。これまでに情報の流出は確認されていないということです。機構は「再発防止に努めて参ります」とコメントしています。

●Slack、ユーザの約1%のパスワードをリセット…再設定をメールで呼び掛け

https://www.itmedia.co.jp/news/articles/1907/19/news051.html

このニュースをザックリ言うと・・・

- 7月18日（現地時間）、米Slack Technologiesより、同社が運営するグループチャットツール「Slack」の一部ユーザが不正ログインを受けていた可能性があるとし、パスワードのリセットを行ったと発表されました。

- 対象となるのは「2015年3月以前に作成」かつ「それ以降にパスワードを変更したことがない」等の条件を持つ全ユーザの1%にあたり、その中には実際に不正ログインされていないユーザも予防措置として対象に含まれているとのことです。

- 同社では対象となったユーザにメールで連絡しており、強制的なログアウトは行われていないものの、パスワードは無効化されているため、ヘルプページをもとに新しいパスワードを設定するよう呼び掛けています。

AUS便りからの所感等

- Slackでは2015年にも不正ログインが発生し、実際に被害を受けたユーザのパスワードをリセットする等の処置を行っていましたが、その時期にログインしていたものとみられる他のアカウントのパスワードの情報が今回Slack社に報告されたことにより、さらに広い範囲のアカウントについて同様の処置をとったとしています。

- 現代においてパスワードを変更すべき、あるいはそれを促すべき最も重要なタイミングは「アカウント情報流出や不正ログインが発覚した時」または「設定されているパスワードが他で設定されているものと同じであることが判明した時」であり、同様のタイミングでパスワードのリセットなどの処置を行った大手サービスは他にも存在します。


CLOUD USER

Slack、ユーザーの約1%のパスワードをリセット　再設定をメールで呼び掛け

[ITmedia]

企業向けコラボレーションツール「Slack」を運営する米Slack Technologiesは7月18日（現地時間）、約1%のSlackアカウントのパスワードをリセットすると発表した。対象となるユーザーにはメールでも連絡した。

【重要】Slackパスワードのリセットのご連絡

- Slackでは他にもSMSやスマホアプリを用いた「二要素認証」の設定を行うよう呼び掛けていますが、今や「リスト型攻撃」等から自サービスのアカウントを保護する意味でもこれを導入・提供することの検討は重要と言えます。