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。

●ネット証券に委託SEが不正アクセス…顧客15口座から約2億円着服

https://www.itmedia.co.jp/news/articles/2103/24/news108.html
https://www.scsk.jp/news/2021/pdf/20210324.pdf
https://www.matsui.co.jp/company/ir/press/pdf/pr210324.pdf

このニュースをザックリ言うと･･･

- 3月24日(日本時間)、SCSK社より、松井証券のシステム開発・運用を委託されていた同社元社員が同証券の顧客口座から不正出金を行っていた容疑で逮捕されたと発表されました(同日、松井証券からも同様の発表がありました)。

- 両社の発表によれば、元社員は、2017年6月～2019年11月に業務上付与された権限を悪用して同証券ユーザーのID・パスワードおよび取引暗証番号を取得、有価証券の売却代金や預けられていた現金を不正に取得する等の行為を行ったとしています(ターゲットとなった顧客の本人確認書類を偽造し、同姓同名の銀行口座を外部に作成する等の手口もとっていたとのことです)。

- 2020年1月に顧客から同証券に対し身に覚えのない取引があったとの通報を受けて発覚しており、被害は顧客15名の口座から約2億円に上るとされています。

AUS便りからの所感等

- 内部関係者の犯行による事案としては(今回と多少異なり個人情報等が流出したものですが)、2014年のベネッセの事例、また2018年には日経新聞社社員がPCを分解しHDDを抜き取って持ち出した事例がありますが、うち後者の例のような、物理的な保存媒体の奪取がそのまま情報の流出に繋がる恐れに対しては、ディスクの暗号化を行うことが有効な対策の一つとなります。

- (これも今回のケースと必ずしも合致しない一般的な推奨事項ではありますが)サービスにおけるなりすましを防ぐため、顧客本人であることを証明する認証時の情報等を保存するにあたっては、本人以外はたとえシステム管理者であっても元の情報を読み取ることができないよう、基本的にはハッシュ化等の実施が前提とされるべきです。

- 本人確認書類を偽造して銀行口座を用意する手口は、同業のSBI証券が2020年9月に外部から不正アクセスを受け資金流出の被害を受けた際にもとられており、今回の件に限らず、あるサービスで発生した不正行為について他社が荷担させられることなく阻止するという観点からも、サービス登録時に(ないし登録済みの顧客についても)「eKYC」の導入等による本人確認のさらなる徹底が行われることが今後予想されます。

ITmedia NEWS

松井証券のシステム開発委託先SE、顧客口座から2億円着服か　パスワードなど不正使用して出金

2021年03月24日 17時06分 公開　[ITmedia]

印刷　見る　Share　B! 222

大手SIerのSCSKは3月24日、松井証券のシステム開発を担当していた同社の元社員が、松井証券顧客15人のIDやパスワードなどを不正に取得し、顧客になりすまして、口座に預けられていた現金など総額2億円を不正出金していたと発表した。

元社員は、電子計算機使用詐欺・不正アクセス禁止法違反などの容疑で同日、警視庁に逮捕された。

1. 経緯

2020 年 1 月に身に覚えのない取引があったとのお客様からの通報を受けて調査を開始した松井証券様より、当社に対して照会があり、当社においても直ちに調査を開始いたしました。松井証券様と協力しながら調査した結果、松井証券様のシステム開発等に専任で従事していた当該元社員が松井証券様の複数のお客様の顧客 ID、パスワード、取引暗証番号等を不正に取得した上で、松井証券様のお客様になりすまして、松井証券様のお客様の有価証券を売却し、その売却代金を含め証券口座に預けられていた現金を不正に出金していた疑いがあることが判明いたしましたため、松井証券様とともに直ちに警察への相談を開始し、以降、警察による捜査に全面的に協力をしてまいりました。

なお、当社は、かかる不正行為の疑いがあることが判明したのち、証拠隠滅を避けるために、当該元社員に本件調査ならびに警察の捜査等を察知されないよう可能な限り配慮しつつ、松井証券様とともに更なる不正行為に

1

●スキー滑走情報等共有アプリ、不正アクセスでユーザーの全画像ファイル・滑走ログが消失

https://nlab.itmedia.co.jp/nl/articles/2103/27/news035.html
https://www.yuki-yama.com/news/1824/

このニュースをザックリ言うと・・・

- 3月26日(日本時間)、スキー滑走情報や画像等の記録・共有が可能なスマホアプリ「yukiyama」を運営するユキヤマ社より、社外にあるストレージサーバーが不正アクセスを受け、画像データ等を格納するフォルダーが削除されたと発表されました。

- フォルダーの削除により、yukiyama全ユーザーのアイコン画像・投稿画像および滑走記録データが消失したとのことで、消失したデータの復旧は不可能であるとのことです。

- 個人情報およびユーザーデータを管理しているサーバーへの不正アクセスはなく、外部連携サービスへの影響もないとしており、消失したデータ以外のサービス自体は同27日に復旧しています。

AUS便りからの所感

ねとらぼ

- 同社では再発防止策として、認証等セキュリティ強化の実施、第三者機関による対策のチェック、および全ての情報の定期的バックアップを行うとしています。

- オンプレミスの物理サーバーであればわずかながら復旧の可能性があるかもしれません(RAIDは論理的な削除に対する防止策にはなりませんし、SSDを利用していた場合はHDDよりもさらに困難となります)が、クラウド等のサーバーでは、サービスが提供するデータを保護するオプション等を利用したり、自前でデータのバックアップを行ったりしていない限り、このような事態への対応はやはり不可能でしょう。

- 今回のような不正アクセスやランサムウェア等マルウェアの感染といった各種攻撃さらには利用者側あるいはサーバーを提供する側のオペレーションミス等の可能性を鑑みても、あらゆる事態を想定してのバックアップの実施およびバックアップから確実に復旧できる体制の確立は、セキュリティ対策として、データの可用性・完全性の確保のために重要な要素です。


ゲレンデの位置情報アプリ「yukiyama」不正アクセスでユーザーの全画像ファイル・滑走ログが消失

個人情報の流出はないとのこと。

[ねとらぼ]

ゲレンデでの滑走データを保存できるポータルアプリ「yukiyama」で3月26日に不正アクセスが発生し、サーバ上のユーザーの全画像データ、滑走ログファイルなどが消失しました。なお、個人情報の流出は一切ないとのこと。

●コンビニATMの公式Twitterアカウント乗っ取り、不正な投稿

https://www.itmedia.co.jp/news/articles/2103/24/news073.html
https://www.enetcom.co.jp/news/emergency/emergency00045_20210325/
https://web.archive.org/web/20210325083651/https://www.enetcom.co.jp/news/emergency/emergency00012_20210323/

このニュースをザックリ言うと・・・

- 3月23日(日本時間)、コンビニATMを運営するイーネット社より、同社の公式Twitterアカウントが乗っ取りの被害にあったと発表されました。

- 同23日16:50頃より、当該アカウントにおいてプロフィールの書き換えおよび不審な投稿が行われたことから乗っ取りが発覚したとしており、Twitter社に連絡をとった上で、同25日にはアカウントを回復させたことが改めて発表されています(ただし3月29日現在、アカウントは非公開状態となっています)。

- コンビニATMの稼働や、同社が管理する他のソーシャルメディアアカウント(Facebook・YouTube)については、影響がないことを確認済みである一方、同社を騙るTwitterのDMその他による不審な連絡に返信したり、そこに記載されているURLにアクセスしないよう呼び掛けています。

AUS便りからの所感

ITmedia NEWS

- Twitterでは推測されやすいパスワードを設定したアカウントの乗っ取りが長らく発生しており、例えば著名なブランドのサングラスを宣伝するスパム投稿等が多くのユーザーに知られています。

- 当該アカウントからは「経営不振により全口座を閉鎖させていただきます」「二段階認証もせずにハッキングされたと騒ぐな」という内容が投稿されていたとのことですが、前者については同社が事実ではないとする一方、後者については今回乗っ取りの一因となった可能性があり、アカウント回復後の発表では「強固なパスワードへの変更、2要素認証の設定」を行ったとしています。

- 第三者に推測されない複雑なパスワードを設定すること(かつ複数サービスで同一パスワードの使い回しをしないこと)が長年啓発され、一方で二段階認証(ないし多要素認証)を必須としているサービスも珍しくなくなってきている状況においては、それぞれの対応をいずれも行っていないアカウントが常に乗っ取りの被害を受ける恐れがあると心得た上で、設定されているパスワードを確認し、二段階認証等を任意であっても設定することを強く推奨致します。


コンビニATMのイーネット、公式Twitterが乗っ取り被害に　「全口座を閉鎖」「騒ぐな」などツイートされる

2021年03月24日 12時30分 公開

[谷井将人，ITmedia]

印刷　見る　Share　B! 27

コンビニATMを展開するイーネットは3月23日、同社の公式Twitterアカウントが何者かに乗っ取られ「全口座を閉鎖する」「ハッキングされたと騒ぐな」など、意図しないツイートが投稿されたとして謝罪した。ATMの運営やユーザーへの影響はないという。