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。

●三越伊勢丹ECサイト等に不正ログイン…会員情報15,000件が閲覧された可能性

https://www.itmedia.co.jp/news/articles/2008/07/news089.html
https://mitsukoshi.mistore.jp/store/news/200806.html

このニュースをザックリ言うと･･･

- 8月6日(日本時間)、三越伊勢丹ホールディングスより、同社グループ運営のECサイト「三越伊勢丹オンラインストア」およびクレジットカード「エムアイカード」のWebサイトにおいて、不正ログインにより会員情報を閲覧された可能性があると発表されました。

- 被害を受けたのは、三越伊勢丹オンラインストア会員情報15,336件(氏名・住所・電話番号・メールアドレス・生年月日およびクレジットカード番号の下4桁等)と、エムアイカード会員情報3,583件(氏名・請求予定額および保有ポイント等)とされています。

- 不正ログインは7月6日～8月3日に海外のIPアドレスから行われ、会員からの「身に覚えのないログイン通知メールが届いた」という連絡で発覚したとのことで、他のWebサイトで流出したアカウント情報を悪用した、いわゆる「リスト型攻撃」によるものとされています。

AUS便りからの所感等

- 同社では個々の対象ユーザーに対しメール連絡を行いパスワードの変更を依頼している他、不正ログインを行ったアクセス元を遮断する等、セキュリティ対策を強化しているとのことです。

- 様々なWebサービスにおいて、リスト型攻撃による大規模な不正ログインの事案が何年もの間続いており、例えばクレジットカード加盟店において安全なカード情報の取り扱いに関する具体的な対策のガイドラインが定められたのと同様、将来ECサイトに対し二段階認証等の対策を義務付けるといったガイドラインの策定が行われることが十分に考えられます。

- ECサイト側での対策が確立することを待つまでもなく、ユーザー側においても「複数のサービス間で全く同じパスワードを使い回さない」「推測されやすい簡単なパスワードを設定しない」こと等に注意し、今後も不正ログイン発生時に備え、各サービスに登録しているアカウント全てについて漏れなく管理を行うことが肝要です。

MITSUKOSHI

三越伊勢丹WEB会員・Webエムアイカード会員への不正ログインについて
「リスト型アカウントハッキング（リスト型攻撃）」による不正ログインの発生とパスワード変更のお願い

この度、弊社が運営するオンラインサイト「三越伊勢丹オンラインストア」および、グループ会社である㈱エムアイカードのホームページにおきまして、海外のIPアドレスからの不正アクセスを受け、不正にログイン、一部会員については会員情報が閲覧された可能性があることが発覚いたしました。今回の不正ログインの手法は、他社サービスから流出した可能性のある ユーザＩＤ・パスワードを利用した「リスト型アカウントハッキング（リスト型攻撃）」の手法で行われていると推測されます。詳細は、以下の通りです。

【不正ログインの状況】※8月5日（水）時点の数字で今後変更になる可能性がございます。
① サイト名称：「三越伊勢丹オンラインストア」
・件数：15,336件
・期間：7月6日（月）～8月3日（月）
・閲覧された可能性がある会員情報：氏名・住所・電話番号・メールアドレス・生年月日など
※クレジットカード情報は、有効期限とカード番号下4桁のみ

② サイト名称：エムアイカード ホームページ
・件数：3,583件
・期間：7月6日（月）～8月3日（月）
・閲覧された可能性がある会員情報： 会員氏名・ご請求予定額・現在の保有ポイントなど

● 7月のフィッシング報告件数、先月より微減も依然高水準…対策協議会発表

https://www.antiphishing.jp/report/monthly/202007.html

このニュースをザックリ言うと・・・

- 8月5日(日本時間)、フィッシング対策協議会より、7月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 7月度の報告件数は16,767件で、6月度の16,811件より44件の減少、一方フィッシングサイトのURL件数は5,536件で、6月度の5,481件から55件の増加となっています。

- Amazon・LINE・楽天およびAppleを騙るフィッシングメールについての報告が全体の約90%、特にAmazonについては全体の約62%を占めているとのことです。

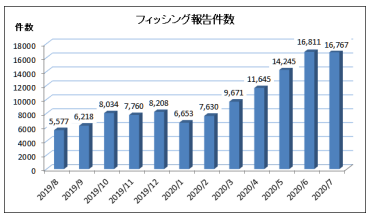
AUS便りからの所感

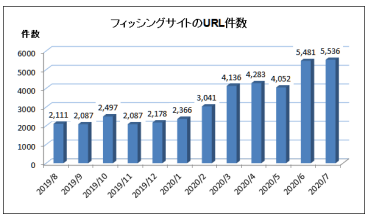
- 今年1月以降急増の一途をたどっていた報告件数が7月度では一段落したという見方もできますが、割合的には微々たる減少であり、フィッシングサイトURL件数と同様、依然非常に高い水準を保っています。

- 挙げられている手口の傾向は6月度と同様で、不正なアプリのインストール誘導、SNSの短縮URL機能等の悪用によるURLフィルタリングの回避、あるいは大量に取得したランダムな文字列の独自ドメインに正規サイトのドメイン名を追加したURLによる、スマートフォン等での閲覧時の誤認を誘導するもの、等があります。

- フィッシングか否かに拘らないSPAMメールの受信量が7月に激増している模様ですので、引き続き普段からのフィッシング回避策として、不審なメールについてネット上の情報を調査して確認する、利用しているサービスのサイトにはブックマークからアクセスする、等を心がけてください。

フィッシング対策協議会
Council of Anti-Phishing Japan





●夏季休暇における情報セキュリティに関する注意喚起、IPA呼びかけ

https://www.ipa.go.jp/security/topics/alert20200803.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となるお盆の時期を迎えるにあたり、8月3日(日本時間)にIPAより、情報セキュリティに関する注意喚起が出されています。

- 組織内に常駐(あるいはテレワークでネットワークに接続)する人が少なくなる、システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性、および従業員等が友人や家族と旅行に出かけた際の、SNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- 休暇前にシステムのセキュリティ対策が十分か確認すること、休暇期間中のインシデント対応体制や関係者への連絡方法を調整すること、および休暇明けには不正アクセス・侵入等の痕跡をサーバ等のログから確認することを呼びかけており、実施すべき項目をまとめています。

AUS便りからの所感

- IPAでは、毎回の長期休暇の前に、通常時には生じにくい様々な問題が発生し得ることを鑑み、そういった問題にも早く確実に対応することへの注意を促しており、JPCERT/CCも4月と12月に同様の注意喚起を行っています。

- 各組織による注意喚起の骨子は毎回大きく変わるものではない一方、4月の注意喚起(同 2020/04/27号参照)で新設された「テレワークを行う際のセキュリティ上の注意事項」では参照すべき情報源へのリンクが追加されており、そういった追加された情報にも随時目を通すことを推奨致します。

- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有がそういった攻撃による被害を最小限に抑えられるために大切なことと言え、また休暇に入るまでに十分な対応が間に合わなかったとしても、明けてから点検すべきことは多く存在しますし、以後も年末年始等に備えて、準備・点検を行うよう意識して頂ければ幸いです。

IPA


夏休みにおける情報セキュリティに関する注意喚起

最終更新日：2020年8月3日
独立行政法人 情報処理推進機構
セキュリティセンター

多くの人がお盆休みや夏休みなどの長期休暇を取得する時期を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりがちです。このような場合、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

最近では外出自粛の影響により、逆に家でパソコンなどを利用する時間が長くなり、ウイルス感染やネット詐欺被害のリスクが高まることも考えられます。

これらのような事態とならないよう、(1)組織のシステム管理者、(2)組織の利用者、(3)家庭の利用者、のそれぞれの対象者に対して取るべき対策をまとめています。

■長期休暇における情報セキュリティ対策
また、長期休暇に限らず、日常的に行うべき情報セキュリティ対策も公開しています。
■日常的に実施すべき情報セキュリティ対策
被害に遭わないためにもこれらの対策の実施をお願いします。