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。

●自治体ポイントのサーバー不正アクセス…アカウント情報8,075人分等流出か

https://www.advertimes.com/20211013/article365237/
https://chibapo.pointpack.jp/file/20211012_info.pdf

このニュースをザックリ言うと・・・

- 10月12日(日本時間)、千葉市より、同市が実証実験を行っている地域ポイント「ちばシティポイント」および「ちばしウオーキングポイント」のデータベースサーバーが不正アクセスを受け、参加者に関する一部情報が流出した可能性があると発表されました。

- 被害を受けたとされるのは、ちばシティポイントのWebサイトへのログインID(WAONカード番号)とハッシュ化されたパスワードおよび生年月日8,075人分、ちばウオーキングポイント用アプリ登録用のメールアドレス2,646人分、ポイント付与・利用履歴18,188人分、郵便番号6,635人分およびアンケート結果(居住エリア・性別・年代)とされています(氏名・住所・電話番号等は別のサーバー上にあり、影響を受けていないとのことです)。

- 市では、9月29日にサーバーを管理する委託業者から不正アクセスについて、次いで10月7日に流出の可能性がある旨の連絡を受けたとのことで、10月11日にパスワードのリセットを行ったとのことです。

AUS便りからの所感等

- パスワードは前述の通りハッシュ化された状態で、理論上は即座に不正なログインが可能となるものではないものの、ハッシュ化に用いたアルゴリズムあるいは手順次第で元のパスワードが復元されるケースが、計算機の性能向上もあって現実的なものとなっていることから、今回のようなケースでパスワードのリセットを行うことは最低限必要な処置と言えるでしょう。

- メールアドレスとパスワードの組み合わせが丸ごと流出したという確証は得られていませんが、もし当該サービスで使用していたパスワードを他のサービスでも使い回していた場合には、いわゆる「リスト型攻撃」による不正ログインが発生するものと心得、必ずパスワードの変更を行うべきでしょう。

- 流出した各種情報は断片的ではあるものの、メールアドレスだけでも迷惑メール、それこそ千葉市やポイント運営事務局を騙るフィッシングメールが送られる等の可能性は容易に想像できますので、公式サイトにて正しい情報を入手し、あるいはトップページの案内に従ってパスワードの再設定を行う等の慎重な行動をとることが重要です。

AdverTimes.(アドタイ)

千葉市の地域ポイントで不正アクセス メールアドレスなど流出か

AdverTimes.
2021年10月13日 掲載

千葉市は10月12日、地域ポイント制度「ちばシティポイント」「ちばしウオーキングポイント」のサーバーに不正アクセスがあり、利用者のマイページログイン用のIDやパスワード、メールアドレスの一部が外部に流出した恐れがあることを発表した。委託先事業者はフェリカポケットマーケティング。

不正アクセスを受けたデータベースに記録されていたのは、利用者の「マイページ」にログインするためのIDやパスワード、生年月日が8075人分、「ちばウオーキングポイント」用アプリのユーザー登録のためのメールアドレス2646人分、ポイントの付与・利用履歴1万8188人分、郵便番号6635人分、居住エリア、性別、世代などのアンケート結果。パスワードは10月11日に一斉リセットした。

●JALマイレージバンクの「数字6桁限定」パスワード、10/20より変更

https://internet.watch.impress.co.jp/docs/yajiuma/1358671.html
https://www.jal.co.jp/jp/ja/jmb/jmb-login/info/

このニュースをザックリ言うと・・・

- 10月20日(日本時間)、日本航空(JAL)が提供する「JALマイレージバンク」のログインパスワードの仕組みが変更される予定となっています。

- 当該サービスはこれまで、パスワードとして「数字6桁」のみが使用可能となっており、ユーザーID(JMBお得意様番号)も数字7桁あるいは9桁で、この組み合わせでログインを行うことになっていました。

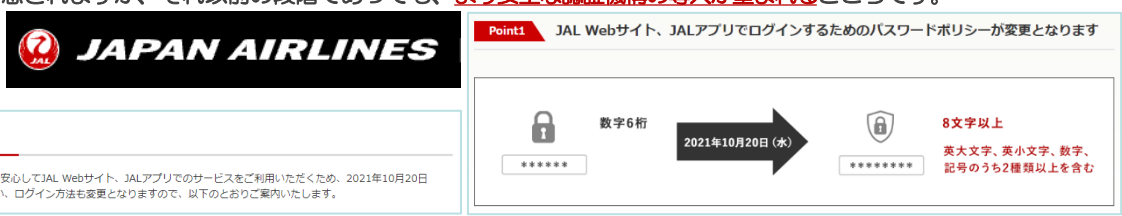
- 10月20日以降、パスワードとして「英字の大文字・英字の小文字・数字・記号から2種類以上を組み合わせて8文字以上」が設定可能となり、また、会員情報・個人情報を取り扱う一部のサービスにおいて、登録メールアドレスにワンタイムパスワードを送信することによる2段階認証を導入するとしています。

AUS便りからの所感

- JALマイレージバンクでは、2014年2月にユーザー約60人が不正アクセスを受け、マイルが不正にAmazonギフト券に交換される事案が発生していました(https://internet.watch.impress.co.jp/docs/news/633807.html)が、以後もパスワードの仕組みは変わらず、同年8月に一部サービス利用時に2段階認証を導入していたものの、「生年月日」の入力を要求するというもの(https://www.itmedia.co.jp/news/articles/1408/04/news060.html)で、安全性には疑問が呈されていました。

- JALの発表によれば、2022年秋頃には数字6桁のパスワードは使用できなくなるとのことですので、利用者においては速やかに、推測されにくくかつ他のサービスと異なるパスワードを設定することを強く推奨致します。

- 今回導入される新たな2段階認証についても、ワンタイムパスワードをスマートフォンアプリ等で生成する仕組みではないことや、SMSで送信する形ではないことに対しやはり疑問を呈する声があり、これまでのパスワードが使用できなくなるタイミングで新たな施策が導入されることも予想されますが、それ以前の段階であっても、より安全な認証機構の導入が望まれるところです。



● MSより10月月例パッチリリース…ゼロデイ1件含む脆弱性修正

https://news.mynavi.jp/article/20211013-2135999/
https://msrc.microsoft.com/update-guide/releaseNote/2021-Oct
https://jprs.jp/tech/security/2021-10-15-windowsdns.html

このニュースをザックリ言うと・・・

- 10月13日(日本時間)、マイクロソフト(以下・MS)より、月例のセキュリティパッチ(Windows 10向けパッチKB5006670他)がリリースされ、多数の脆弱性が修正されています。

- 修正された脆弱性のうち、Windowsカーネルドライバー(Win32k)の脆弱性「CVE-2021-40449」について、その時点で攻撃が確認されていた、いわゆる「ゼロデイ脆弱性」であったとされています。

- この他、WindowsサーバーのDNS機能に存在する脆弱性「CVE-2021-40469」については、リモートからサーバーを乗っ取る等の攻撃が可能となる恐れがあり、JPドメインを管理するJPRS社からも注意喚起が出されています。

AUS便りからの所感

- パッチにはWindowsの印刷スプーラー(Print Spooler)に関する脆弱性の修正も含まれていましたが、適用後、ネットワークプリントサーバを利用しての印刷に失敗する問題が一部環境で報告されており、回避策が提示されている模様です(https://news.mynavi.jp/article/20211019-2163125/)。

- これを含めた他に何らかの不具合が発生していたとしても、安易にパッチをアンインストールすることは、他の脆弱性への対策も無効になる恐れがあり危険なため、基本的にはアップデートを行うようにし、またシステム管理者等においても組織内で問題が発生していないか調査するとともに、回避策があるか情報収集と提供を行うこと、またパッチ未適用状態のPC等が攻撃を受ける可能性を抑止するため、アンチウイルスやUTMによる防御を確実に行う体制を整えることが肝要です。