— AUS（アルテミス・ユーザ・サポート）便り 2021/03/08号 —
https://www.artemis-jp.com

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。

●JAL・ANA、のべ192万件の会員情報流出…海外企業における不正アクセス被害が原因

https://www.nikkei.com/article/DGXZQODZ05ABI0V00C21A3000000/
https://www.nikkei.com/article/DGXZQODZ060K00W1A300C2000000/
https://www.jal.co.jp/jp/ja/info/2021/other/210305/
https://www.ana.co.jp/ja/jp/amc/news/info/2021/210306_memberinfo.html

このニュースをザックリ言うと･･･

- 3月5日から6日(日本時間)にかけて、日本航空(JAL)マイレージバンク会員情報約92万件、および全日空(ANA)マイレージクラブ会員情報約100万件が、外部で発生した不正アクセスにより流出したことが、両社より相次いで発表されました。

- 両社とも影響を受けたのは全マイレージ会員の3%にあたり、名前(アルファベット表記)・会員番号および会員ステータスが流出したとされる一方、生年月日・住所・クレジットカード番号・パスポート番号・メールアドレス・パスワード・予約情報等は影響を受けていないとのことです。

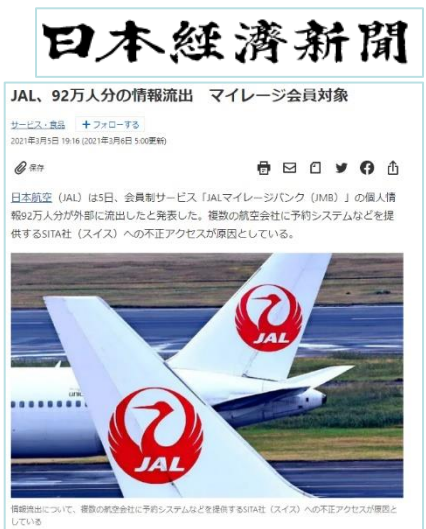
- 世界の航空業界各社にネットワークや業務アプリケーション等を提供するSITA社の米国子会社が不正アクセスを受け、管理する顧客データの一部が流出したことが発表されており、JAL・ANA両社もSITAに顧客データを共有していたことにより、流出の影響を受けた模様です。

AUS便りからの所感等

- JALはワンワールド、ANAはスターアライアンスとそれぞれが航空連合に加盟し、加盟社間で共有していた情報が流出しており、両社とも全会員の情報あるいは会員のマイルが不正利用され得る範囲の情報までは影響を受けなかった一方、共通のシステム提供者が不正アクセスを受けたことにより、複数の航空連合にまたがる多数の航空会社に被害が及ぶ結果となっている模様です。

- 前述の通り、現時点でメールアドレス・パスワードの流出は確認されておらず(ただし両社とも、念の為パスワード変更を希望する利用者に対して変更方法の案内を行っています)、今回については当てはまらないとは思われますが、システムへの不正アクセスによるアカウント情報(IDやメールアドレスとパスワードの組合せ)の大量流出が発生した場合、程なくして他のサービスにも、そのアカウント情報による不正ログイン試行が行われることが往々にして起こり得ます。

- 自分が登録した何らかのサービスにおいて万が一そういった不正アクセスや情報流出が発生した場合には流出した情報の種類を確認し、特にアカウント情報が含まれていることが確定的になった場合には速やかにパスワードの変更を行うこと、かつ連鎖的な不正ログインの被害を受けないためにも、同じパスワードを複数のサービス間で使い回していないか点検することを心掛けるようにしてください。


日本経済新聞

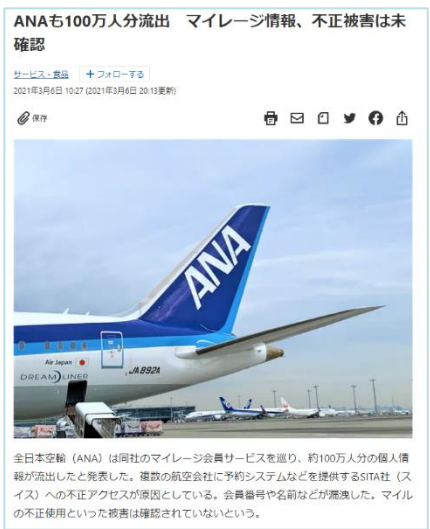
JAL、92万人分の情報流出　マイレージ会員対象

サービス・食品　＋フォローする
2021年3月5日 19:16 (2021年3月6日 5:00更新)

保存

日本航空（JAL）は5日、会員制サービス「JALマイレージバンク（JMB）」の個人情報92万人分が外部に流出したと発表した。複数の航空会社に予約システムなどを提供するSITA社（スイス）への不正アクセスが原因としている。

情報流出について、複数の航空会社に予約システムなどを提供するSITA社（スイス）への不正アクセスが原因としている


ANAも100万人分流出　マイレージ情報、不正被害は未確認

サービス・食品　＋フォローする
2021年3月6日 10:27 (2021年3月6日 20:13更新)

保存

全日本空輸（ANA）は同社のマイレージ会員サービスを巡り、約100万人分の個人情報が流出したと発表した。複数の航空会社に予約システムなどを提供するSITA社（スイス）への不正アクセスが原因としている。会員番号や名前などが漏洩した。マイルの不正使用といった被害は確認されていないという。

● Exchange Serverに脆弱性、緊急リリースのパッチ適用を

https://www.jpcert.or.jp/at/2021/at210012.html
https://www.ipa.go.jp/security/ciadr/vul/20210303-ms.html
https://msrc-blog.microsoft.com/2021/03/02/20210303_exchangeoob/
https://msrc-blog.microsoft.com/2021/03/07/20210306_exchangeoob_mitigations/

このニュースをザックリ言うと・・・

- 3月3日(日本時間)、マイクロソフト(以下・MS)より、Exchange Serverに複数の脆弱性が確認されたとして、定例外のセキュリティアップデートがリリースされています。

- 脆弱性の悪用により、Exchange Serverが稼働しているサーバーのシステム権限を外部から乗っ取ることも可能とされている上、既に一部の脆弱性を悪用した攻撃も確認されているとのことで、IPA・JPCERT/CC等からも相次いで注意喚起が出されています。

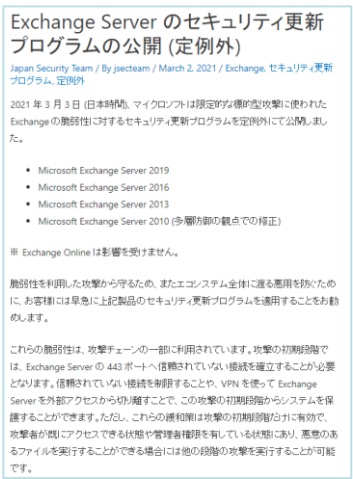
- Exchange Server 2019, 2016, 2013(および既にサポートが終了している2010)についてアップデートが提供されており、Microsoft 365のExchange Onlineは影響を受けないとのことです。

AUS便りからの所感

- MSの発表によれば、攻撃の初期段階として「Exchange Serverの443ポートへ信頼されていない接続を確立することが必要」としており、外部ネットワークに接続しているExchange Server(特にOutlook Web Appに外部からアクセス可能な状態である等のケース)について、優先的にアップデート等対策の実施を推奨しています。

- また、アップデートをすぐさま適用できないケースについての緩和策も提示されていますが、完全な保護策ではなく、また既にサーバーを侵害された場合の復旧策でもないとしている点には注意が必要です(この他、侵入の痕跡を調査するツール等も提供されています)。

- いずれにせよ、組織内部で使用するサーバーについて(あるいは外部への公開を意図しているサーバーでも)外部から全てのポートに制限なしでアクセス可能な状態となっていることは一般に危険であり、サーバー自身やUTM等によるフィルタリングを用いて特定のポートへのアクセス以外を遮断することがまずは必要ですし、可能であれば外部からのアクセスはVPNを介して行わせることにより、不特定多数からのアクセスを制限することも検討に値するでしょう。


Exchange Server のセキュリティ更新プログラムの公開 (定例外)

Japan Security Team / By jsecteam / March 2, 2021 / Exchange, セキュリティ更新プログラム, 定例外

2021 年 3 月 3 日 (日本時間)、マイクロソフトは限定的な標的型攻撃に使われた Exchange の脆弱性に対するセキュリティ更新プログラムを定例外にて公開しました。

- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2010 (多層防御の観点での修正)

※ Exchange Online は影響を受けません。

脆弱性を利用した攻撃から守るため、またエコシステム全体に渡る悪用を防ぐために、お客様には早急に上記製品のセキュリティ更新プログラムを適用することをお勧めします。

これらの脆弱性は、攻撃チェーンの一部に利用されています。攻撃の初期段階では、Exchange Server の 443 ポートへ信頼されていない接続を確立することが必要となります。信頼されていない接続を制限することや、VPN を使って Exchange Server を外部アクセスから切り離すことで、この攻撃の初期段階からシステムを保護することができます。ただし、これらの緩和策は攻撃の初期段階だけに有効で、攻撃者が既にアクセスできる状態や管理者権限を有している状態にあり、悪意のあるファイルを実行することができる場合には他の段階の攻撃を実行することが可能です。

● 2月度フィッシング報告件数、1月度より一転して減少

https://www.antiphishing.jp/report/monthly/202102.html

このニュースをザックリ言うと・・・

- 3月3日(日本時間)、フィッシング対策協議会より、2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。

- 2月度の報告件数は30,949件で、1月度(https://www.antiphishing.jp/report/monthly/202101.html)の43,972件から13,023件の減少となり、2020年9～12月度における3万件前後の水準に一旦立ち戻っている模様です。

- フィッシングメールに悪用されたブランドとしてはAmazonが全体の60.4%と最も多く、これに三井住友カード・楽天・三菱UFJニコス・MyJCBを合わせた5ブランドが報告全体の約90.8%を占めていたとのことです(また、フィッシングに悪用されたブランド件数59件のうち、クレジット・信販系が16、金融機関系が7となっています)。

AUS便りからの所感

- 4万件台を一気に突破した先月度から一転しての減少となったものの、前述のように中長期的には3万件台前後の状態が続いており、以後も少なくともその水準を割る可能性は低いと予想致します。

- 2月中旬は主にクレジットカードを騙るフィッシングメールや宅配便の不在通知を装うSMSの報告は減少したことにより、報告件数がそれまでの約半数になったとしているものの、2月下旬は再び多くの報告があったとのことで、引き続き油断することなくフィッシングに警戒すべきでしょう。

- 同協議会からは2月17日に三菱UFJニコス、また3月に入ってもアプラスや楽天を騙るフィッシングへの注意喚起が出されており、今後も利用しているサービスや企業・組織の公式サイトあるいはSNS等から随時情報を収集する、またサービスの公式サイトへブックマークからアクセスする、等の防御策をとり、不審なメールやショートメッセージの受信時に慎重に行動できるよう備えることが肝要です。