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。

●「ななつ星」通販サイト、クレジットカード情報など流出か

https://www.nikkei.com/article/DGXMZO43657220S9A410C1ACX000/
https://www.asahi.com/articles/ASM4D3GMDM4DTIPE007.html

このニュースをザックリ言うと･･･

- 4月12日（日本時間）、JR九州より、豪華寝台列車「ななつ星」関連商品の通販サイトが不正アクセスを受け、最大7,996人分の個人情報が流出した（あるいはその可能性がある）と発表されました。

- 対象となるのは、2013年10月5日（サイト開設日）から2019年3月11日までに当該サイトを利用した人の住所・氏名・電話番号等、うち会員登録を行った5,964人分についてメールアドレスおよび暗号化処理がされたパスワード等、さらにクレジットカードを登録した2,816人分についてセキュリティコード（CVV）を含むカード情報（3,086件）等となっています。

- 3月11日に決済代行会社から連絡を受けてサイトを閉鎖し、調査した結果、流出が発覚したとしています。

AUS便りからの所感等

- クレジットカードにおけるデータセキュリティの国際基準「PCI DSS」では、カード情報のうちセキュリティコード等を加盟店で保持することを禁止しています。

- また、クレジット取引セキュリティ対策協議会で取りまとめられている「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」では、カード情報保護のため、「加盟店におけるカード情報の非保持化」「カード情報を保持する事業者のPCI DSS準拠」を推進しています。

- 今回のような流出事件の被害を受けた業者が決済業務をPCI DSSに準拠する決済代行業者に委託し、カード情報を自前で保持しないよう改修するケースも多くみられており、UTM等を用い、不正アクセスされない・されても情報が流出しないシステムを構成するだけでなく、流出しては困るセンシティブな情報について可能な限り保持しない仕組みにすることも流出によるダメージを抑えるための方策としては重要です。

日本経済新聞

ななつ星サイトで情報流出　JR九州、最大8千人分

九州・沖縄 社会
2019/4/12 12:03

保存 共有 印刷 その他

JR九州は12日、豪華寝台列車「ななつ星in九州」の関連商品を販売する通販サイトが外部から不正アクセスを受け、クレジットカードのセキュリティーコードなど最大約8千人分の顧客の個人情報が流出したと発表した。うち、カード情報が含まれるのは最大約2800人分で、カード番号や有効期限も流出した可能性がある。

画像の拡大

JR九州の豪華寝台列車「ななつ星in九州」（2月、大分県日田市）＝共同

カード悪用の被害が一部出ており、顧客からカード関連会社に「身に覚えのない支払いがあった」との問い合わせがあり、発覚した。件数や金額は現時点で不明という。JR九州は既に警察に届け出ており、流出した恐れがある対象客にメールや郵送で連絡して注意を呼び掛ける。

福岡市で記者会見した福永嘉之上席執行役員は「顧客に多大なる迷惑と心配をお掛けすることを深くおわびする」と述べ、謝罪した。

JR九州によると、流出した可能性があるのは、サイトが開設された2013年10月5日から、閉鎖した19年3月11日までの間に利用した顧客の情報。会員登録した顧客の氏名や住所、電話番号、メールアドレス、生年月日、職業といった情報も含まれるとしている。情報が漏れた対象には、ななつ星に乗った顧客の一部も入っている。

朝日新聞 DIGITAL

「ななつ星」通販、カード情報流出　最大２８１６人分

女屋泰之　2019年4月12日13時20分

シェア 0　ツイート list　ブックマーク 7　メール　印刷

豪華寝台列車「ななつ星」＝２０１８年１０月１６日午前１１時３分、ＪＲ博多駅、女屋泰之撮影

ＪＲ九州は１２日、豪華寝台列車「ななつ星」の関連商品を売る通販サイトに不正アクセスがあり、最大で２８１６人分のクレジットカード情報が流出したと発表した。少なくとも一人の利用者からは「身に覚えのない決済がある」とカード会社に連絡があった。住所や電話番号などを含めると、最大で７９９６人の個人情報が流出した可能性があるという。

流出したクレジットカードの情報はカード番号、有効期限、セキュリティーコード。カードの不正利用についての被害状況は調査中で、不正利用された分はＪＲ九州が補償する。

不正アクセスがあったサイトは「ななつ星Ｇａｌｌｅｒｙ」。決済代行会社から３月１１日に、情報流出の可能性があると指摘があり、同日、サイトを閉鎖した。その後、外部から情報を閲覧した形跡が確認されたという。

●企業を最も悩ませるサイバー攻撃はフィッシング…英政府の報告書より

https://japan.zdnet.com/article/35135387/

このニュースをザックリ言うと・・・

- 4月3日（現地時間）、イギリス政府より、セキュリティレポート「2019 Cyber Security Breaches Survey」が公開されました。

- レポートでは、企業にとって最大のセキュリティ問題はフィッシングや偽の電子メールだとしており、サイバー攻撃のうち最も多いのは、詐欺の電子メールあるいは偽のWebサイトに誘導するフィッシングだと報告しており、フィッシングによる情報漏洩等、サイバー攻撃により企業が被る平均コストは4,180ポンド（60万円強）で、2018年当時に比べ1,000ポンド以上増加しているとのことです。

- また、セキュリティ侵害の報告件数が前年より増加している一方、報告した企業は減少している傾向について、企業のセキュリティが向上していることの他に、攻撃者がより狭い範囲の企業に集中して攻撃を行うようになった可能性があると推測しています。

AUS便りからの所感等

- この記事では、フィッシングメールを「信頼できる同僚などのコンタクト先を攻撃者が装うことでターゲットになった人が油断してパスワードやその他の詳細情報を渡すように仕向けるもの」と定義しており、「標的型攻撃」「ビジネスメール詐欺」の側面も持ったフィッシングを取り上げているようです。

- こういった攻撃の準備段階として、ターゲット企業（あるいはその商談相手）のメールサーバに不正アクセスしたり、PCをマルウェアに感染させたりすることにより、やりとりされるメールの内容を盗み見するケースがあります。

- 不正アクセスやマルウェア感染をアンチウイルス・UTMで防御することは重要ですが、それだけでは防げないフィッシング・標的型攻撃等もあり、利用者や管理者が不審な行動に確実に気付けるようなシステムの構築、および社員等に対しどういった攻撃手法があるのかを教育することもまた欠かせないものとなるでしょう。

●IEにゼロデイの脆弱性、不正な.mhtファイルによりPC上のファイルを盗まれる可能性

https://gigazine.net/news/20190415-internet-explorer-zero-day-vulnerability/

このニュースをザックリ言うと・・・

- 4月10日（現地時間）、セキュリティ研究者のJohn Page氏より、Internet Explorer（IE）に未修正の脆弱性が存在することが発表されました。

- 発表によれば、脆弱性はMHTML（.mht）ファイルの処理に存在し、ローカルに保存した不正な.mhtファイルを開くことにより、PC上のファイルを読み取られ、外部に送信すること等が可能になるとされています。

- Page氏は3月27日にMicrosoftに脆弱性を報告したものの、Microsoft側の返信によれば緊急でパッチがリリースされる等の予定はないと推測しており、過去に.mhtファイルを利用してマルウェアが拡散したケース等があることから、注意を呼び掛けています。

AUS便りからの所感等

- 今回の脆弱性には、XMLファイルを処理する際に、XMLファイルと同じマシン上のファイルが埋め込まれるという「XML外部実体攻撃(XXE)」が根本にありますが、この攻撃が注目されるようになってわずか1年近くしか経っておらず、今後これが原因となる脆弱性は他にも確認される可能性があります。

- Windows 10の場合、Edge自体は.mhtファイルを処理しないものの、通常.mhtファイルを開くアプリがIEに関連付けられているため、メールに添付された等による.mhtを開くことにより、脆弱性の影響を受けるとされます。

- 今後アンチウイルスのパターンファイルにおいて不正な.mhtファイルへの対応が期待されますが、肝心のIEについて修正の望みが薄い現状では、場合によっては「.mhtファイルとIEとの関連付けを解除する」ないし「IE自体を使用しない」といった回避策をとらざるを得なくなることも考えられるでしょう。