— AUS（アルテミス・ユーザ・サポート）便り 2017/11/27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。

●犯人は1ヶ月以上メールを監視…ビジネスメール詐欺対策は3つ

http://itpro.nikkeibp.co.jp/atcl/column/17/110700496/110800002/

このニュースをザックリ言うと・・・

- 11月17日（日本時間）、nikkei BPnetにおいて、企業版振り込め詐欺「ビジネスメール詐欺」に関する記事が掲載されており、日本企業が被害に遭いやすいケースとして「犯罪者が海外の取引先になりすます手口」が取り上げられています。

- 記事で挙げられている一例では、攻撃者は準備段階として、商談を行っている2社のうち片方のメールシステムに不正アクセスし、やり取りを少なくとも1ヶ月以上は観察するとしており、その後、両社に対し相手側の担当者になりすましてメールを送信し、「監査中なので通常とは違う口座になる」「トラブルのためメーン銀行で入金を受けられない」といった理由をつけて攻撃者自身の口座に振り込ませようとするとのことです。

- 記事ではこういったビジネスメール詐欺対策のため、以下の3つの策を挙げています。

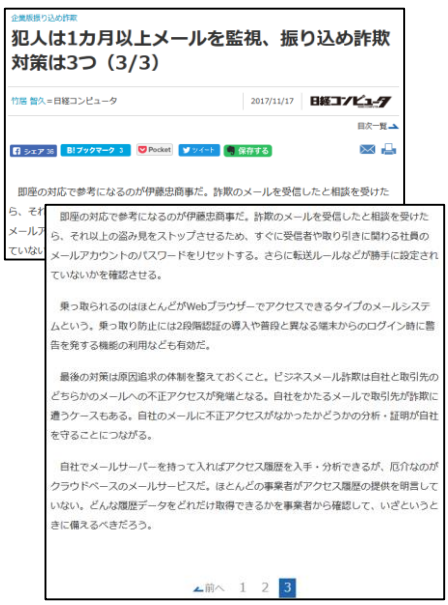
1) 周知を徹底する：詐欺の存在や手口を、海外含め全社員に知らしめる。
2) 即座に対応する：詐欺に気付いたらすぐ銀行に連絡、メールのパスワードもリセットする。
3) 原因追求に備える：メールシステムの不正アクセスを調べられるようにしておく。

AUS便りからの所感等

- 記事によれば、詐欺の実行において、例えば請求書のPDFも偽装し、口座情報のみを巧妙に書き換えるケースもあるとしており、商談の流れに絶妙なタイミングで入り込んでくるため、特に気付くのが難しいとされています。

- 準備段階における「メールへの不正アクセス」のための手段としては、やはりマルウェアへ感染させるものが有力と考えられ、普段からアンチウイルス等による防御を行うことは当然不可欠です。

- 記事では、Webメールが狙われやすいとされる一方、2段階認証の導入や異なる端末からログインがあった場合の警告を活用する等の対策が挙げられており、単に侵入を防ぐだけではなく、利用者や管理者が確実に異変に気付けるようなシステム作りもまた重要です。



●ゆうちょ銀行・みずほ銀行等をかたるフィッシングメールに注意

https://internet.watch.impress.co.jp/docs/news/1092493.html
https://www.jc3.or.jp/topics/virusmail.html

このニュースをザックリ言うと・・・

- 11月20日（日本時間）、ゆうちょ銀行をかたるフィッシングメールが拡散中として、警視庁サイバー犯罪対策課のTwitterアカウントおよび日本サイバー犯罪対策センター（JC3）より警告が出されています。

- 警告によれば、◆メールは件名が「ゆうちょ銀行　入金のご連絡　(N71019788477G)」、◆本文が「いつもゆうちょダイレクトをご利用いただき、誠にありがとうございます。 お客さまの口座へ入金がございましたので、お知らせいたします。」で始まり、メール中のリンクにアクセスすると「URSNIF(gozi)」と呼ばれるマルウェア等がダウンロードされる可能性があるとされています。

- 前後して、みずほ銀行、三井住友銀行、スルガ銀行、楽天および楽天カード等をかたるメールも確認されており、それぞれ特徴がまとめられています。

AUS便りからの所感等

- URSNIFはインターネットバンキングサイトへの不正ログイン・不正送金を狙うマルウェアで、以前から頻繁に拡散しています。

- どういった不審なメールが拡散しているかといった攻撃の手段を常日頃から把握しておくことや、アンチウイルスによるウイルスチェックやUTMによる不正な通信の出入りの遮断等、複数の防衛手段を組み合わせての防御が肝要となります。

- URSNIFの他にもインターネットバンキングを狙うマルウェアが存在し、中にはログイン・送金のためにスマホアプリを用いるケースを狙ってスマホに感染しようとするものもありますので、スマホ向けアンチウイルスアプリの導入等を行うようにしましょう。

●石けんECサイトでカード情報392件漏えいか? セキュリティコードも

https://netshop.impress.co.jp/node/4883

このニュースをザックリ言うと・・・

- 11月13日（日本時間）、ミヨシ石鹸株式会社より、同社の通販サイトが不正アクセスを受け、利用者のカード情報が流出したと発表されました。

- 被害を受けたのは、6月6日～8月31日の間に同サイトでクレジットカード決済を行った最大392件のカード会員氏名、カード番号、有効期限、およびセキュリティコードとされています。

- 8月31日に決済代行会社より連絡を受けて決済を停止し、第三者機関の調査の結果、10月19日に流出が判明したとのことです。

AUS便りからの所感等

- 同社の発表では、Webサーバ外部からの不正アクセスがあり、アプリケーションファイルが改ざんされ、カード会員データが不正に取得されたことが原因と推測しています。

- 今年3月に「Apache Struts2」の重大な脆弱性が発表されて以降、それを突いたとみられる不正アクセスによるクレジットカード番号を含む個人情報の流出が続発していますが、今回の件がその一環なのかは不明なものの、アプリケーションやフレームワークのアップデート、WAFによる攻撃の防御、あるいはUTMを用いた出口対策等、複数の防御策をとることが情報の流出を防ぐためには重要です。

- また、今回のような流出事件の多くにおいて、カード情報を自前で保持するようなシステムだったために被害を受けた業者は、決済業務を「PCI DSS」に準拠する決済代行業者に委託するなどの対策をとっており、「流出してはいけない情報を可能な限り自分では保持しない」こともまた大事なセキュリティ対策の一つです。