

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」「トラブルのためメイ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。

- 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せる。
- 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。



企業版振り込み詐欺
犯人は1カ月以上メールを監視、振り込め詐欺対策は3つ

竹崎 智久=日経コンピュータ 2017/11/17 日経コンピュータ

日本企業が被害に遭いやすいのは、犯罪者が海外の取引先になりすます手口だ。振込口座の番号や口座名義、メールの宛先利用といった商談履歴の多い、商談のやり取り、金取引システムの...

ビジネスメール詐欺の典型的手口
 実行まで高度警戒に準備する
 [画像のクリックで拡大表示]

犯罪者は担当者同士がメールで商談を進めている間、不正アクセスしたメールシステムでやり取りを盗み見る。ビジネスメール詐欺を分析するある国内企業のIT担当者は「1カ月以上は観察することが多い」と指摘する。観察と並行して攻撃対象のメールアドレスと見た目が似ている詐欺用のメールアドレスを用意する。

商談の大詰め、請求段階に入ったところで犯罪者は詐欺用のメールアドレスを使い、取引先になりすましてメールを送る。「監査中なので通常とは違う口座になる」「トラブルのためメイン銀行で入金を受けられない」といったもっともらしい理由をつけて犯罪者の口座を指定してくる。

企業版振り込み詐欺
犯人は1カ月以上メールを監視、振り込め詐欺対策は3つ (2/3)

竹崎 智久=日経コンピュータ 2017/11/17 日経コンピュータ

ビジネスメール詐欺はITによる対策だけでは不十分。システム部門は対策として3つの策を社内に応用したい。

受信中に取引先詐欺

ビジネスメール詐欺対策の3カ条
 ITだけでは守れない
 [画像のクリックで拡大表示]

まずはリスク管理部門などに働きかけ、海外拠点を含め、社員全員に存在を周知する。詐欺の存在を知れば、不自然さを読み取る感覚は高くなる。

三菱東京UFJ銀行は9月にビジネスメール詐欺への注意喚起する文書を全店に配布し、取引先に配布するように指示を出した。「不自然な口座変更があったら従前から知っている電話など、必ずメール以外の手段で確認する作業を徹底させて、詐欺を未然に防いでほしい」と同行の松野室長は呼びかける。

企業版振り込み詐欺
犯人は1カ月以上メールを監視、振り込め詐欺対策は3つ (3/3)

竹崎 智久=日経コンピュータ 2017/11/17 日経コンピュータ

即座の対応で参考になるのが伊藤忠商事だ。詐欺のメールを受信したと相談を受けたら、その即座の対応で参考になるのが伊藤忠商事だ。詐欺のメールを受信したと相談を受けたら、それ以上の盗み見をストップさせるため、すぐに受信者や取引先が騙手側の社員メールアドレスのパスワードをリセットする。さらに転送ルールなどが勝手に設定されていないかを確認させる。

取られるのはほとんどがWebブラウザでアクセスできるタイプのメールシステムという。乗っ取り防止には2段階認証の導入や普段と異なる端末からのログイン時に警告を発する機能の利用なども有効だ。

最後の対策は原因追求の体制を整えておくこと。ビジネスメール詐欺は自社と取引先のどちらかのメールへの不正アクセスが発端となる。自社がたかると取引先が詐欺に遭うケースもある。自社のメールに不正アクセスがなかったかどうかの分析・証明が自社を守ることにつながる。

自社でメールサーバーを持って入れればアクセス履歴を入手・分析できるが、厄介なのがクラウドベースのメールサービスだ。ほとんどの事業者がアクセス履歴の提供を明示していない。どんな履歴データがどれだけ取得できるかを事業者から確認して、いざというときに備えるべきだろう。

前へ 1 2 3

● 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.ic3.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(gozil)」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してされています。

- 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、以前から頻りに拡散しています。

- 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たの防御が肝要となります。

- URSNIF以外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。



ゆうちょ銀行をかたる不審なメールに注意

磯谷 智仁 2017年11月20日 15:12

ツイート リスト いいね! 232 シェア B! 8 Pocket! 21

ゆうちょ銀行をかたるウイルスメールが拡散中として、警視庁サイバー犯罪対策課がTwitterアカウントを通じて注意を呼び掛けている。

警視庁サイバーセキュリティ対策本部 @MPD_cybersec

【サイバー犯罪対策課】
ウイルスをダウンロードさせるメールが拡散中。件名は「ゆうちょ銀行 入金のご連絡 (N71019788477G)」。実際の会社を装っていますが、本文中のリンクをクリックしてダウンロードされるファイルはウイルスです。ご注意ください。
10:58 - 2017年11月20日
👍 12 🗨️ 3,213 ❤️ 1,050

● 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。

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。



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

Webサーバに外部から不正アクセスがあり、アプリケーションソフトが改ざんされた可能性がある

11月15日 いいね! 1 🗨️ 25 📄 1

石けんボディソープなどを販売するミヨシ石鹸は11月13日、通販サイト「ミヨシ石鹸 通信販売サイト」から顧客のクレジットカード情報が最大392件漏えいしたと発表した。

流出した可能性がある情報はカード会員の氏名、カード番号、有効期限、セキュリティコード、

Webサーバに外部から不正アクセスがあり、アプリケーションソフトが改ざんされ、カード会員のデータが不正に取得された可能性があるという。

情報流出の対象は、2017年6月6日から8月31日の間に「ミヨシ石鹸 通信販売サイト」でクレジットカード決済を利用した顧客。