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。

●東京商工会議所からも情報流出（のべ約12,000）

http://www3.nhk.or.jp/news/html/20150610/k10010109131000.html
http://www.tokyo-cci.or.jp/page.jsp?id=59029

このニュースをザックリ言うと･･･

- 6月10日（日本時間）、東京商工会議所（以下、東商）が5月に標的型サイバー攻撃を受け、東商国際部主催による過去3年間のセミナー参加者のべ12,139人分の個人情報（氏名・住所・電話番号・メールアドレスおよび会社名）が流出したと発表されました。

- 東商によれば、5月11日にセキュリティ専門機関JPCERT/CCからの指摘をうけ調査したところ、国際部の1台のノートPCがマルウェアに感染していたことが同22日に発覚しており、そこから共有サーバに保存されていたデータにアクセスされたものとみられています。

- 共有サーバ上のデータは国際部の職員のみがアクセス可能であった一方で、パスワードはかけられていなかったとのことです。

AUS便りからの所感等

- 被害規模は少ないとはいえ、データの暗号化を怠っていたことが流出の大きな要因となるなど、日本年金機構の事件とは状況的に似通ったものとなっており、単一の攻撃者がこれら2組織の事件を含め多数の組織に対して標的型攻撃を行っている可能性を指摘する声も挙がっています。

- 今回のように「データへのアクセスが制限されていることに依存し、一度そこが破られたらあとは流出するのみ」といった状況に陥らないよう、単一のセキュリティ対策だけではなく、添付ファイル付メールの取り扱いに関する社員への注意喚起やUTMの導入など、取り得る複数の対策を確実に実行することによる多層防御が不可欠であることは間違いありません。

NHK NEWSWEB

トップページ ＞ 社会ニュース一覧 ＞ 東商の情報流出は1万2000人余か

ニュース詳細

東商の情報流出は1万2000人余か

6月10日 12時08分

東京23区内の中小企業などが加盟している「東京商工会議所」は10日、記者会見を開き、いわゆる「標的型メール」による外部からの不正アクセスを受けてパソコンがウイルスに感染し、延べ1万2000人分余りの個人情報が流出した可能性があることを明らかにしました。

東京商工会議所の会見によりますと、先月11日にセキュリティーの専門機関から事務所内のパソコンに問題があるのではないかと指摘されて調査したところ、国際部のパソコン1台がウイルスに感染していることが先月22日に分かったということです。
これによって、東商が過去3年間に会員の企業などを対象に開いた投資セミナーなどの参加者名簿にあった会社名や電話番号に加え、個人の名前やメールアドレスなど延べ1万2139人分の個人情報が流出した可能性があるとしています。

東京商工会議所
The Tokyo Chamber of Commerce and Industry

ニュースリリース

当所パソコンのウィルス感染による情報漏えいについて

平成27年6月10日
東京商工会議所

当所事務局員が使用しているパソコンが、標的型メールによるウィルスに感染していたことが5月22日に判明し、国際部で管理しておりました個人情報（氏名に加え住所/電話番号/メールアドレス/会社名の一部または全部）が漏えいした可能性があることを確認しました。
個人情報をご提供いただいた皆様をはじめ、関係者の皆様に多大なご迷惑とご心配をおかけしましたことを深くお詫び申し上げます。
当所では、対象となる方を特定し、すでに直接ご連絡申し上げました。
今回の事態を厳粛に受け止め、現在、関係当局および捜査機関に協力を頂きながら、二次被害の防止を図るとともに、再発防止に向けて個人情報の取扱いに万全を期し、セキュリティ対策を強化するよう努めております。
今後、ご関係の皆様にお知らせすべき新たな情報が判明しましたら、随時ホームページ等にてお知らせいたしますが、まずはお詫び申し上げますとともに、ここにご報告申し上げます。

NHK NEWSWEB　**専門家「何者かが同時攻撃の可能性」**

東京商工会議所で、いわゆる「標的型メール」によってパソコンがウイルスに感染し個人情報が流出したおそれがあることについて、情報セキュリティー会社「FFRI」の鵜飼裕司社長は、「標的型メールによる攻撃は、日本年金機構への攻撃と同じようなタイミングで複数確認されていて、何者かが一連のキャンペーンのように重要な情報を持っているところを同時に攻撃している可能性がある。**攻撃は公的機関だけなく、大企業から中小企業まで幅広く行われているが、被害が表に出ないことが多く、今回のケースも氷山の一角と捉えるべきだ**」と指摘しています。

そのうえで、**「標的型メールはセキュリティの専門家でも開いてしまいそうになるほど巧妙で、メールを開いてしまうことを前提とした対策が必要だ。**ウイルスに感染しても情報が流出しないよう、重要な情報を分けて管理することは有効な対策だが、仕事の効率が著しく低下するのでは現実的ではない。標的型の攻撃で情報を盗もうとする際には特有の不審な通信のパターンがあり、これを検知して被害を防ぐことは可能なので、専門家に相談して、それぞれの企業や団体に合った対策を考えてほしい」と話しています。

●個人情報流出事件からの教訓とは…トレンドマイクロが発表

http://blog.trendmicro.co.jp/archives/11636
http://blog.trendmicro.co.jp/archives/11682

このニュースをザックリ言うと･･･

- 日本年金機構からの個人情報流出事件を受けて、大手セキュリティベンダーのトレンドマイクロ社が同社のブログにて相次いで記事を発表しています。

- 6月9日（日本時間）の記事では、感染被害に関して適切なタイミングで適切な関係者に報告がされていなかった点を問題とされていることを受け、日本国内の企業・官公庁・自治体において、インシデントの報告義務が徹底されていない傾向にあることを同社の「組織におけるセキュリティ対策実態調査 2015年版」をもとに指摘しています。

- 6月11日の記事では、事件と同様の標的型攻撃への対策を考える上での4つのポイントとして、次のように提示しています（右記参照）。

①防げない標的型メール、侵入を前提とした対策が必要:

標的型攻撃メールは一様にフィルタリングできるものではなく、侵入を前提とした対策を行うこと。

②「気付けない攻撃」発覚のきっかけは外部からの指摘、通信の監視が有用:

遠隔操作を行うマルウェア侵入の早期発見等のため、内部から外部への、あるいは内部ネットワークにおける不審な通信を監視すること。

③「業務の都合」が被害につながる、事前の準備がリスクを低減:

「業務の都合」によってセキュリティポリシーが守られない等によるリスクの発生を低減させるため、業務の実態を把握し、運用可能なポリシーと継続的な監査体制を構築するといった事前の準備を行うこと。

④最終的な被害は個人情報、企業規模や業種を問わず広がる標的型サイバー攻撃手法:

今回の事例のように個人情報が標的となるケースでは事業継続に大きな影響を与えるほどの損害が発生し得ることを認識し、自社の持つ情報資産とその重要性を把握した上で必要な対策を考えること。

AUS便りからの所感等

- 2つの記事に書かれていることは、今回のような大規模な事件発生時だけではなく、本来であれば常に意識し、少しずつでも対策を進めていくべきものであり、その際に重要なポイントとなることと言えます。

- 特に内部からの不正な通信を早期に検知あるいは遮断するための「出口対策」について、ゲートウェイやUTMに備わっているIDS・IPS機能を是非とも有効活用すべきでしょう。

●企業への標的型攻撃、31カ月続くケースも

http://www.itmedia.co.jp/enterprise/articles/1505/28/news062.html
http://www.ipa.go.jp/about/press/20150527.html

このニュースをザックリ言うと･･･

- 5月27日（日本時間）、独立行政法人情報処理推進機構（IPA）が国内重要産業における標的型攻撃の情報共有枠組みである「サイバー情報共有イニシアティブ(J-CSIP)」の2014年度レポートを発表しました。

- 2012年4月のJ-CSIP開始以降に参加組織から提供された攻撃メール情報の累計は1257件、うち939件が標的型攻撃とされ、さらにその12%にあたる114件について、同一と思われる攻撃者からの9組織に対しての攻撃と判断されています。

- また、その攻撃者による攻撃は2012年9月～2015年3月の31ヶ月連続で観測され、現在も続行中と見られています。

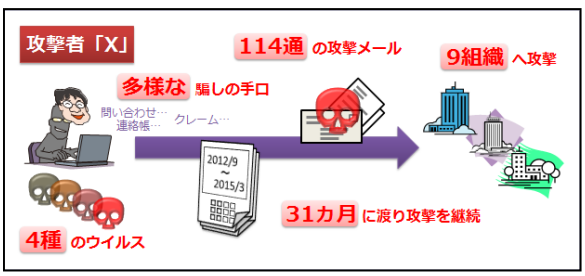

図1：攻撃者「X」による執拗な攻撃

AUS便りからの所感等

- もし3年間毎日攻撃を受け、ほぼ全て防御できたとしても、ただ1日・1件だけが成功してしまい、手薄な内部に侵入できたとなれば、攻撃者にとっては十分元が取れるというものであることに注意しなければなりません。

- レポートからはこの他、標的型攻撃のメールの送信元地域について、今年度は日本が最多だったことから、国内において攻撃インフラが構築されているものと推測しており、多数の国内PCがマルウェア感染等による乗っ取りを受け、攻撃に加担させられていることが考えられます。

- マルウェア感染ないし標的型攻撃の被害者になることは、転じてその加害者になる可能性をもはらんでいると言え、PCへのアンチウイルスの導入・UTMによるネットワーク防御等はさらなる攻撃の拡大を防ぐ意味でも重要な対策となるでしょう。