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。

●標的型攻撃の対策にはネットワークのセグメント化が重要 - TrendMicro

http://news.mynavi.jp/news/2015/05/22/522/
http://blog.trendmicro.co.jp/archives/11476

このニュースをザックリ言うと･･･

- 5月19日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、標準的攻撃を防ぐためにはネットワークの「セグメント化」が重要であるとの見解が同社ブログにて発表されました。

- ブログではセグメント化の利点として、以下の例を挙げています。

① ひとたび乗っ取ったPCを踏み台にして同一LAN上のPCに次々攻撃を仕掛けるケースが標的型攻撃では特に多く、そこで乗っ取られる可能性のあるPCを最小限に抑えられる

② 取引先企業がデータやり取りの際に自社ネットワークにアクセスするケースにおいて取引先を守ることができる

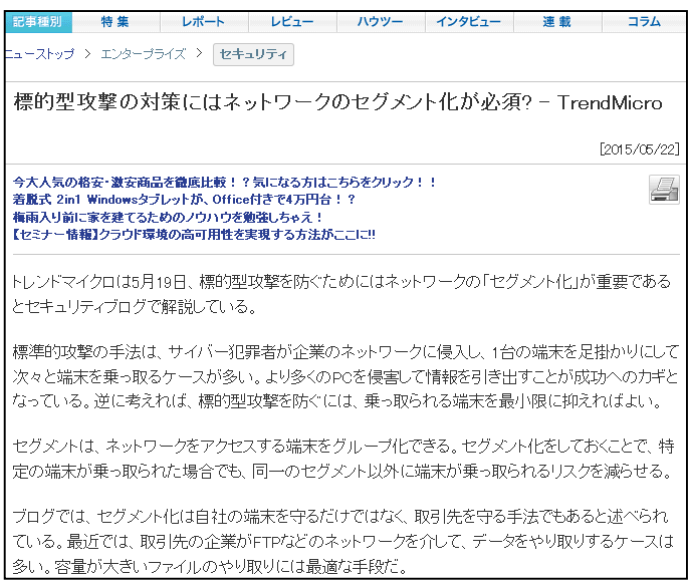
③ ユーザ権限・ネットワークトラフィックの適切な分割で企業の機密情報にアクセスする社員を制限することにより、社員等の内部犯行による機密情報へのアクセスの可能性を抑制できる

AUS便りからの所感等

- ネットワークのセグメント化によるセキュリティの確保は長年言われてきたことですが、特にマルウェア感染や内部犯行による個人情報の流出が取り沙汰されたことから、その重要性が増してきていることと見受けられます。

- 究極的には、ユーザ毎ないし機器毎に他とは独立したLAN上に配置するような構成も考えられるでしょう。

- 今日ではインテリジェントハブやUTMといったネットワーク機器がセグメント化のための機能（VLAN等）を持っており、既に設置している機器においてそれらを活用していないのであれば、有効にすることを検討すべきでしょう。


記事種別 | 特集 | レポート | レビュー | ハウツー | インタビュー | 連載 | コラム

ニュースTOP > エンタープライズ > セキュリティ

標的型攻撃の対策にはネットワークのセグメント化が必須? - TrendMicro

[2015/05/22]

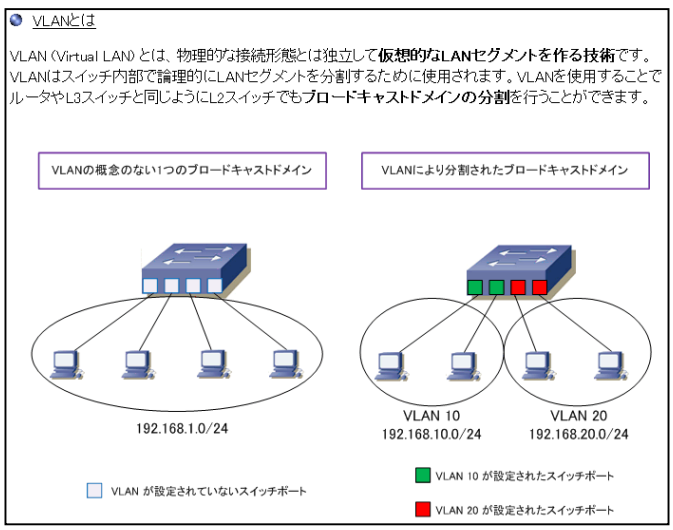
今大人気の格安・激安商品を徹底比較！？気になる方はこちらをクリック！！
着脱式 2in1 Windowsタブレットが、Office付きで4万円台！？
梅雨入り前に家を建てるためのノウハウを勉強しちゃえ！
【セミナー情報】クラウド環境の高可用性を実現する方法がここに!!

トレンドマイクロは5月19日、標的型攻撃を防ぐためにはネットワークの「セグメント化」が重要であるとセキュリティブログで解説している。

標準的攻撃の手法は、サイバー犯罪者が企業のネットワークに侵入し、1台の端末を足掛かりにして次々と端末を乗っ取るケースが多い。より多くのPCを侵害して情報を引き出すことが成功へのカギとなっている。逆に考えれば、標的型攻撃を防ぐには、乗っ取られる端末を最小限に抑えればよい。

セグメントは、ネットワークをアクセスする端末をグループ化できる。セグメント化をしておくことで、特定の端末が乗っ取られた場合でも、同一のセグメント以外に端末が乗っ取られるリスクを減らせる。

ブログでは、セグメント化は自社の端末を守るだけではなく、取引先を守る手法でもあると述べられている。最近では、取引先の企業がFTPなどのネットワークを介して、データをやり取りするケースは多い。容量が大きいファイルのやり取りには最適な手段だ。



出典：ネットワークエンジニアとして
http://www.infraexpert.com/study/vlanz1.html

●日本でランサムウェア被害が増加中 - JPCERT/CCが注意喚起

https://www.jpcert.or.jp/at/2015/at150015.html
http://news.mynavi.jp/news/2015/05/26/201/

このニュースをザックリ言うと･･･

- 5月26日（日本時間）、一般社団法人JPCERT/CCより、国内でのランサムウェア（感染したPCのファイルを人質に金銭等を要求するマルウェア）への感染が増加していることについて警告が発表されました。

- 警告では、ランサムウェアの感染経路の一例として、
①何らかの手法でWebサイトを改ざん　→　②閲覧したユーザを攻撃用ツールキットを設置した別のWebサイト（攻撃サイト）に誘導　→　③Flash Playerの脆弱性（CVE-2015-0313）およびWindowsの脆弱性（CVE-2014-6332、MS14-064）を悪用して感染、
というケースを挙げており、Windows・Flash Playerの他、JavaやIEについて最新版に更新することを推奨しています。

JPCERT CC®

<<< JPCERT/CC Alert 2015-05-26 >>>

ランサムウエア感染に関する注意喚起

https://www.jpcert.or.jp/at/2015/at150015.html

I. 概要

JPCERT/CC では、いわゆるランサムウエアと呼ばれるマルウエアを用いて、端末内のファイルを暗号化し、復号の為に金銭等を要求する攻撃の被害を多数確認しています。

これらの攻撃では、攻撃者はなんらかの手法で Web サイトのコンテンツを改ざんし、Web サイトを閲覧したユーザを攻撃用ツールキットを設置した Web サイト（以下、攻撃サイト）に誘導することを試みます。攻撃サイトに誘導された場合 OS や各種ソフトウエア（Adobe Flash Player や Java など）の脆弱性を用いた攻撃が行われ、ユーザの PC に脆弱性が存在した場合、結果としてランサムウエアに感染する可能性があります。

JPCERT/CC では、ランサムウエアの感染被害に関して、以下の脆弱性が攻撃に使用されていることを確認しています。

AUS便りからの所感等

- ランサムウェアの話題、および、感染によるファイルの暗号化が事実上ファイルを破壊されることに等しいことは当便りでもしばしば述べていますが、重要なファイルを人質にとられ、「金を払えば取り返せるかも」という精神的揺さぶりに屈して身代金を払ってしまうケースが残念ながら目立っているようです。

- 他のマルウェア以上に「感染しないこと」を意識するのであれば、OSと各種アプリケーションを最新に保つこと、アンチウイルス・UTMの導入による防御、その両方が必要となることでしょう。

●米納税者10万人の情報に不正アクセス、組織的犯行か

http://www.nikkei.com/article/DGXLASGM27H39_X20C15A5EAF000/
http://jp.reuters.com/article/worldNews/idJPKBN0OB2P920150526

このニュースをザックリ言うと･･･

- 5月26日（現地時間）、日本の国税庁に当たる米内国歳入庁（IRS）より、今年2月から5月にかけて約10万人の納税情報が不正にアクセスされていたことが発表されました。

- 発表によれば、過去に申告した納税情報を呼び出す同庁のオンラインシステム「ゲット・トランスクリプト」が約20万回の不正アクセスを受け、うち半分が成功した模様です。

- 犯行は組織的なものと推測されており、不正アクセスにあたっては、個人認証のための情報として納税者の生年月日・住所・社会保障番号などを事前に入手したものとみられます。

日本経済新聞
2015年5月30日(土)

Web刊 速報 ビジネスリーダー マーケット マネー テクノロジー ライフ スポーツ 映像 朝刊・

全て 経済 企業 国際 政治 株・金融 スポーツ 社会 ニュース18時 その他ジャンル▼

速報＞国際＞記事

米で10万人の納税情報に不正アクセス　内国歳入庁

2015/5/27 12:34

小 中 大 保存 印刷 リプリント ▼共有

【ワシントン＝共同】日本の国税庁に当たる米内国歳入庁（IRS）は26日、今年2～5月にかけて約10万人の納税情報が不正にアクセスされたと公表した。米メディアは、IRSのコスキネン長官が組織的犯行との見方を示し、当局が捜査していると伝えた。

IRSによると、過去に申告した納税情報を呼び出すIRSのオンラインシステム「ゲット・トランスクリプト」が約20万回の攻撃を受け、約10万人のアカウントが不正にアクセスされたという。

個人認証に必要な納税者の生年月日や住所、社会保障番号などの情報を事前に入手して不正アクセスを試みたもようだ。

AUS便りからの所感等

- 今回の不正アクセスは米国独自の納税情報管理システムがターゲットにされましたが、日本においては10月より施行、翌年1月より運用開始される社会保障・税番号（マイナンバー）制度において、今後マイナンバーとその他個人情報の組合せでアクセスするシステムの構築が行われた場合、そういった情報の適切な保護・管理が行われていない企業・組織が狙われ、今回のような事件が起こらないとも限りません。

- 個人から、情報を託される企業･組織に至るまでセキュリティを意識した慎重な行動のもとに情報の管理・保護を行うこと、それを行うことを意識したシステムの構築が重要であり、そこではクライアントPCにおけるアンチウイルス、ネットワークにおけるUTM、それぞれの導入が欠かせないものとなるでしょう。