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。

●マイナンバーをきっかけにセキュリティ対策の見直しを･･･シマンテックが特別サイト公開

http://www.atmarkit.co.jp/ait/articles/1509/10/news131.html
http://www.symantec.com/ja/jp/mynumber/

このニュースをザックリ言うと･･･

- 9月10日（日本時間）、大手セキュリティベンダーのシマンテック社より、10月から施行（2016年1月より運用開始）されるマイナンバー制度に対する対策と指針をまとめた「マイナンバープロテクションガイド」および「シマンテックマイナンバーサイト」が公開されました。

- マイナンバープロテクションガイドでは、マイナンバーを含む個人情報（特定個人情報）が流出する要因として「標的型攻撃からの漏えい」および「企業内部からの漏えい」を挙げ、それぞれに対するソリューションの適用について解説しています。

- 「標的型攻撃による漏えい」のケースでは、攻撃の「侵入」「発見」「取得」「流出」の各ステップで対策措置を講じることがリスク低減につながるとし、多層的なマルウエア対策、ホワイトリスト型アプリケーション実行制御／振る舞い検知、ストレージ内での機密情報検出、流出防止などのソリューションをそれぞれ利用することを推奨しています。

- 一方の「企業内部からの漏えい」についても「情報漏えい対策(DLP)」についてのソリューションが重要であるとし、一例として「マイナンバーの12桁が含まれると思われる通信」を見つけるポリシーを同社ソリューションでは提供しているとのことです。

AUS便りからの所感等

- マイナンバー制度においては、全従業員のマイナンバーの提出を受け管理する必要が生じることから、全ての組織についてその制度を意識したシステムの見直しが不可欠となるとみられます。

- 一つの対策で全ての個人情報流出を食い止めることは不可能であり、アンチウイルスやUTMを含めた複数のソリューションの適用が流出の効果的な抑止に貢献することでしょう。

15th ANNIVERSARY @IT

2015年09月10日 18時00分 更新

事業者や地方公共団体へのガイドを無償提供：

マイナンバーをきっかけにセキュリティ対策の見直しを――シマンテックが特別サイト公開

マイナンバーだけではなく、長期的な対策を――。シマンテックは「シマンテックマイナンバーサイト」を公開し、同社が提供するソリューションの紹介とともに、事業者や行政機関、地方公共団体に向けてのガイドを無償提供する。

[宮田健, @IT]

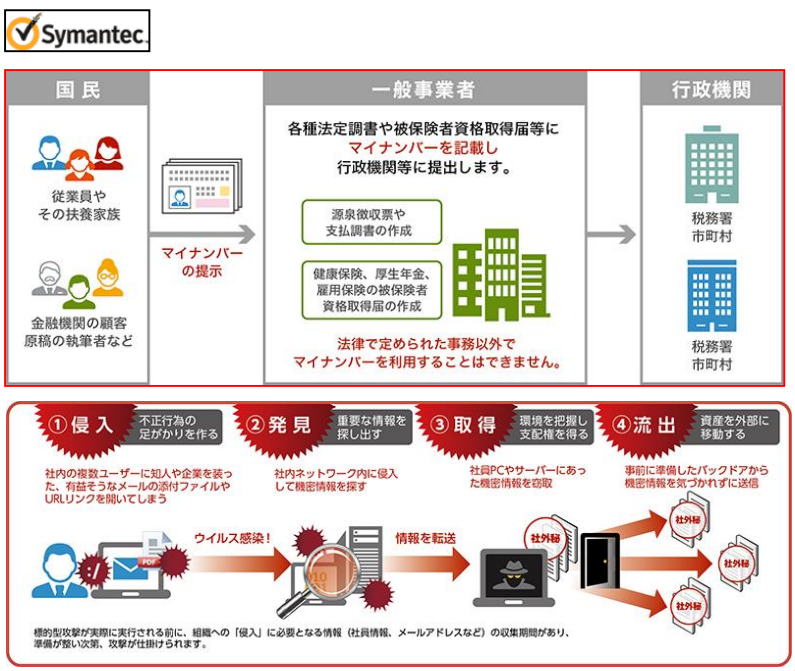
シマンテックは2015年9月10日、マイナンバー対策の指針と対策をまとめた「マイナンバープロテクションガイド」を公開した。同日公開された「シマンテックマイナンバーサイト」では、同社が提供するソリューションとともに、事業者や行政機関、地方公共団体に向けてのガイドを提供する。

企業の特定個人情報管理とシマンテックのソリューションをマッピング

シマンテック APJソリューションマーケティング 金野隆氏

シマンテック APJソリューションマーケティング 金野隆氏は、マイナンバーを取り扱うことで、いままで企業が保持していた個人情報が「特定個人情報」として取り扱われ、利用に違反があったり漏えいがあったりしたときには罰則が科せられることを改めて解説した。そのため、これまで個人情報を取り扱っていなかった企業も、改めて特定個人情報の流出、漏えいリスクを見直すべきだとした。

今回公開されたマイナンバープロテクションガイドでは、特定個人情報の流出要因として「標的型攻撃からの漏えい」と「企業内部からの漏えい」のそれぞれにソリューションを適用すべきだと解説している。



●LinuxマルウェアのDDoS攻撃、アジアに集中砲火

http://www.itmedia.co.jp/enterprise/articles/1509/30/news137.html
http://japan.zdnet.com/article/35071236/

このニュースをザックリ言うと･･･

- 9月29日（米国時間）、CDN最大手の米Akamai社がLinuxサーバに感染するボットネット型マルウェア「XOR DDoS」によるDDoS攻撃が発生していると警告しました。

- 同社Security Intelligence Response Team（SIRT）は、ボットネットによるDDoS攻撃の帯域幅は最大150Gbps、ターゲットは1日最大20件、うちアジア地域に対する攻撃は90%にのぼるとしており、DDoS攻撃を行うための感染先として、これまでのWindowsからLinuxへとフォーカスを切り替えた可能性を指摘しています。

ITmedia エンタープライズ

2015年09月30日 15時58分 更新

LinuxマルウェアのDDoS攻撃、アジアに集中砲火

LinuxマルウェアのDDoS攻撃、アジアに集中砲火

「ITmedia」

アカマイの注意喚起

アカマイテクノロジーズは9月30日、Linuxシステムに感染する「XOR DDoS」のボットネットによるDDoS（分散型サービス妨害）攻撃が激化しているとして注意を呼び掛けた。ボット感染の確認や駆除をユーザーにアドバイスしている。

XOR DDoSは、遠隔操作型のトロイの木馬で、Linuxシステムに感染する。攻撃者は総当たりで感染先のシステムを探し、まずSSHサービスのパスワードを盗んでシステムへのログインを試みる。ログインに成功すると、root権限でBashシェルスクリプトを実行してシステムにマルウェアを感染させ、遠隔操作で標的にDDoS攻撃を仕掛ける。

AUS便りからの所感等

- Linuxに感染するマルウェアについては以前も同社が別種のDDoSボットネットを構築するものについて警告しています。

- Windowsを対象とするマルウェアが非常に多いため、警戒が緩くなるケースが珍しくありませんが、OSXやスマートフォンさらにはルータのようなネットワーク機器等、どんなOSにもマルウェアの感染の可能性があることに注意すべきです。

- マルウェアはLinuxサーバにSSHによってログインするため、侵入の可能性のあるパスワードが脆弱である等のユーザアカウントが存在しないか確認すること、その他にもLinuxサーバ内の各ソフトウェアを最新に保つこと、そして可能な限りUTMによる不正なトラフィックからの防御を行うことが重要です。

●マルウェアに感染したCisco社製ルータを探索するアクセス･･･警察庁の定点観測

http://www.npa.go.jp/cyberpolice/topics/?seq=16930
http://japan.zdnet.com/article/35070681/

このニュースをザックリ言うと･･･

- 9月20日（日本時間）、警察庁より、マルウェアに感染した米Cisco Systems社製ルータを探索していると考えられるアクセスを観測したとして警告が発表されました。

- 問題となっているマルウェアは、9月15日にセキュリティベンダーのFireEye社が発表した「SYNful Knock」で、ルータの管理者アカウントに不正にログインしバックドアを設置するものとされています。

- 警察庁では、現時点で探索アクセスの目的は不明としながらも、バックドアを悪用してルータに不正なアクセスを試みようとしているものと推測しています。

警察庁 National Police Agency

@police

目的別インデックス　用語集　サイトマップ

topics

■マルウェアに感染したCisco社製ルータを探索するアクセスの観測について　2015年09月20日

平成27年9月20日
警察庁

マルウェアに感染したCisco社製ルータを探索するアクセスの観測について

「SYNful Knock」マルウェアに感染したCisco社製ルータを探索していると考えられるアクセスを観測しました。Cisco社製ルータを使用している企業や組織においては、管理する機器の感染の有無について確認を実施することを推奨します。

詳細情報

- マルウェアに感染したCisco社製ルータを探索するアクセスの観測について

AUS便りからの所感等

- 今回のマルウェアはCiscoルータのOSにある脆弱性を悪用するような種類ではないようですが、FireEye社では、管理者パスワードを初期値のまま運用しているか、何らかの方法で攻撃者に漏えいしたことがルータに侵入された原因としており、PC等に比べネットワーク機器の管理・保守が十分になされていないケースが狙われたものと考えられます。

- 管理者アカウント情報は必ずデフォルトのままとせずに変更すること、また今回のような何らかの理由による漏えいの可能性が考えられる場合にはパスワードの変更を検討することも大切です。