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。

●狙われるのは人間のスキ…JASA、2018年の情報セキュリティ十大トレンド発表

http://itpro.nikkeibp.co.jp/atcl/column/14/346926/010901265/
http://www.jasa.jp/seminar/security_trend_top10.html

このニュースをザックリ言うと・・・

- 1月5日（日本時間）、特定非営利活動法人日本セキュリティ監査協会（JASA）より、「2018年 情報セキュリティ十大トレンド」が発表されました。

- 発表は昨年10月に実施したアンケートに基づくもので、十大トレンドのうちトップ3には「ランサムウェア」「標的型攻撃」「IoT機器への攻撃」が挙げられています。

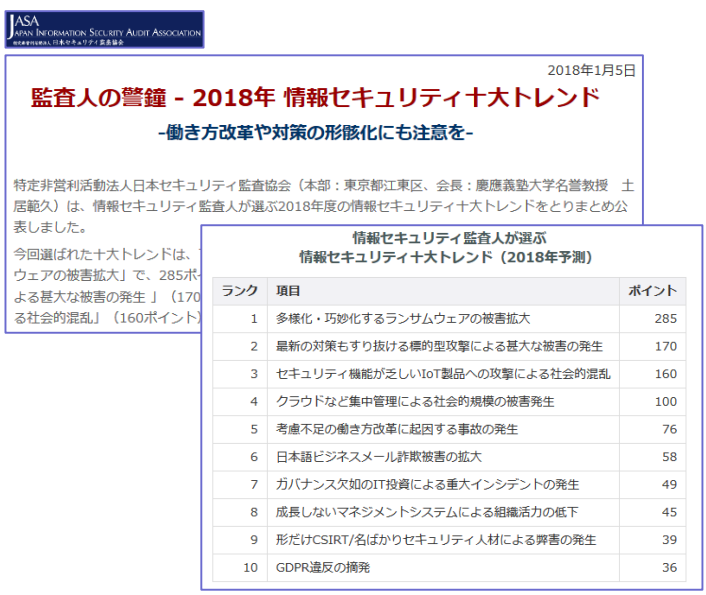
- トップ3や6位「日本語ビジネスメール詐欺」のような2017年に猛威を振るった攻撃のみならず、今年注目されるとみられるトピックも挙げられており、例えば、4位「クラウドなど集中管理による社会的規模の被害発生」では設定ミス等により大量消去あるいは意図しない書き換えが発生する可能性、5位「考慮不足の働き方改革に起因する事故の発生」ではテレワーク推進に伴う十分なセキュリティが保たれない作業環境下での事故の可能性がそれぞれ指摘されています。

- JASAではこの発表をもとに、「(ビジネスメール詐欺等は)技術的な対策に加え、人的な対策も必要になる」「就業環境が変化したとき、新たにどんなリスクが発生するのか特定する必要がある」、また制定したルールの形骸化が「攻撃されやすいスキ」につながるとし、このスキをなくすため「第三者による監査」を行うことを推奨しています。

AUS便りからの所感等

- インターネットの普及、ノートPCの登場、そしてスマホやタブレットといったスマートデバイスの登場といった出来事があるたびに、旧来のルールのままでの運用は難しくなり、またそれを頑なに強要することは、いたずらに不便を強いるだけでセキュリティ対策として意味がない場合もあります。

- 旧来のルールのままセキュリティを維持しようとして、日々登場するトレンドを否定するのではなく、それを取り入れる場合に発生するセキュリティ上の問題と対策を洗い出すこと、以前に制定され実行されているルールが現状に合っているかの見直し、現状に合わず形骸化しているルールの見直し、および現状に対する新たなルールの作成、これらは随時折を見て実行されるべきものと言えるでしょう。



●モバイルWi-Fi接続がマルウェアの感染経路に…日本を狙った「XXMM」亜種の特徴的な感染経路

https://internet.watch.impress.co.jp/docs/news/1099223.html

このニュースをザックリ言うと・・・

- 12月中旬、セキュリティベンダーのカスペルスキー社より、サイバー攻撃グループ「The Bald Knight Rises」が日本の組織・企業から情報を盗み出すための攻撃の手口について、報道関係者向けセミナーで発表されています。

- 発表では、攻撃グループはWindowsに感染するマルウェア「XXMM」やその亜種「Wali」、Waliがダウンロードするバックドア「Datper」、あるいはVBスクリプトで作成されたトロイの木馬「VBEダウンローダー」等、複数のマルウェアをターゲットとなる組織に感染させ、どれかのマルウェアが駆除されてしまっても攻撃が根絶しないようにする処置をとっているとしています。

- マルウェア検証サイト「VirusTotal」に対してXXMMのアップロードを行ったアクセス元の75%が日本であること、XXMMが通信を行う指令サーバの場所も52.9%であり、日本国内の正規のWebサイトが改ざんされて指令サーバに仕立て上げられているとみられていること、不正な通信が怪しまれないよう、日本時間の業務時間帯にあたる8～19時の間でのみ通信を行うこと等、日本の組織をターゲットとする様々な事象が挙げられています。

- また、XXMMに感染したIPアドレスの多くがモバイルインターネット接続サービスを提供しているISPのものであり、モバイルWi-FiルータがUSB接続され、グローバルIPアドレスが割り振られている状態のPCに感染を試みるというWaliの特徴を挙げ、外回りのセールス・営業職等が主な感染先になっている可能性を指摘しています。

AUS便りからの所感等

- 有線LANやモバイルルータへのWi-Fi接続においては、通常PCにはプライベートIPアドレスが割り当てられ、外部から直接アクセスされる可能性は低いですが、今回はUSB接続によるブリッジモードでグローバルIPアドレスが割り当てられる場合にXXMM等に狙われる可能性について指摘されています。

- こういったケースが発生しえるという意味でも、OS・アプリケーションを最新に保ち、Windowsファイアウォール等の設定を適切に行うこと等、PC自体についても怠りなく防御を固めることが肝要です。

●大麦製品のECサイトでカード情報2.4万件が漏えいか

https://netshop.impress.co.jp/node/5032

このニュースをザックリ言うと・・・

- 12月25日（日本時間）、大麦製品のECサイト「大麦工房ロアオンラインショップ」を運営する大麦工房ロア社より、同サイトで利用されたクレジットカード情報が流出した可能性があると発表されました。

- 発表によれば、対象となるのは2015年10月1日～2017年8月7日の間に同サイトで決済に利用された最大24,780件分の氏名・クレジットカード番号・クレジットカード有効期限およびセキュリティコードとされています。

- 同社では8月7日にカード会社から連絡を受け、直ちにサイトを閉鎖、専門調査会社に調査を依頼し、不正アクセスの監視強化、カード会社に対する不正利用モニタリングの実施要請、個人情報保護委員会等関係官庁への報告、警察への被害の申告及び相談を行ったとしています。

AUS便りからの所感等

- 今回の流出について、前述のとおり専門調査会社による調査が行われ、不正アクセスの直接的な証跡は発見できなかったとのことですが、現在不正アクセスの被害を受けていない組織であっても、証跡を取得できる可能性を高め、より迅速で確実な対策に役立てる意味では、可能な限り速やかにUTMの導入等による監視体制の強化に取り組むべきです。

- クレジット取引セキュリティ対策協議会が取りまとめた「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」において、EC事業者は2018年3月末までに、カード情報を保持しないシステムとする、またはPCIDSSに準拠することが要求されています（http://www.meti.go.jp/press/2016/03/20170308003/20170308003.html）。

- 今回の流出においても、クレジットカード情報をサイト上に保存していた可能性が高いとみられますが、不正アクセス等による流出の被害を最小限に抑えるためには、重要な情報を可能な限り自前で保持しないことも重要な方策と言えます。