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。

●2019年の情報セキュリティ十大トレンド、JASAが発表

https://securityblog.jp/news/20190117.html
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7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、同協会認定の情報セキュリティ監査人を対象としたアンケート結果に基づく「2019年 情報セキュリティ十大トレンド」が発表されました（2018年分は「AUS便り 2018/01/15号」参照）。

- ランクインしたトレンド（括弧内は前年度での順位、-はランク外）は以下の通りです。

1	(-)	：	仮想通貨の盗難、詐欺の拡大
2	(2)	：	巧妙化する標的型攻撃による被害の甚大化
3	(3)	：	家庭用IoT機器のセキュリティ不備によるプライバシー侵害の更なる拡大
4	(6)	：	ビジネスメール詐欺被害の更なる深刻化
5	(5)	：	働き方改革の推進普及による新たな脅威の発生
6	(-)	：	時代遅れとなりつつあるパスワード認証
7	(10)	：	GDPRを乗り越えても残る諸外国のプライバシー規制リスク
8	(1)	：	高度化するランサムウェアによる被害拡大
9	(-)	：	問われるサイバーセキュリティ経営の責任体制
10	(-)	：	クラウドバイデフォルトの情報セキュリティ体系化

AUS便りからの所感等

- 初めて発表された昨年にて1位だった「ランサムウェア」は8位となった一方、ランキングに入っていなかった「仮想通貨」についてが1位となっており、2位「標的型攻撃」、3位「家庭用IoT機器」については昨年同様となっています。

- こういったランキングは、ウォッチガード社が社昨年11月に発表した「情報セキュリティ業界の動向予測」（「AUS便り 2018/12/03号」参照）等、様々なセキュリティベンダーやセキュリティ関連団体等が挙げていますが、各々観点等が異なることにより、独特の項目が挙げられていることも多いです。

- これらのランキングの複数を参考にしつつ、各人が話題となっているセキュリティの脅威について随時情報収集を行い、特にシステム管理者においては、新しい脅威からの被害をも最小限に抑えられるようなシステム・ネットワークの随時見直しに柔軟に対応して頂ければ幸いです。

日立ソリューションズ Information security blog 情報セキュリティブログ

JASAが2019年のセキュリティ10大トレンドを発表

2019年1月17日

1月7日、特定非営利活動法人 日本セキュリティ監査協会(JASA)は、「監査人の警鐘 - 2019年 情報セキュリティ十大トレンド」を公開した。これは、同協会より認定を受けた情報セキュリティ監査人約1,700人を対象に実施したアンケートによって選ばれたもの。

第1位には「仮想通貨の盗難、詐欺の拡大」が前年のランク外からランクインした。また、第2位、第3位はそれぞれ「巧妙化する標的型攻撃による被害の甚大化」「家庭用IoT機器のセキュリティ不備によるプライバシー侵害の更なる拡大」がランクインする結果となった。

同協議会は、2019年のトレンドについて、被害の拡大や深刻化が指摘されていると言及した上で、「時代遅れとなりつつあるパスワード認証」(6位)、「問われるサイバーセキュリティ経営の責任体制」(9位)、「クラウドバイデフォルトの情報セキュリティ体系化」(10位)など、専門家の視点が反映された意見や、経営層へのメッセージなどがランク入りしたとコメントしている。

JASA JAPAN INFORMATION SECURITY AUDIT ASSOCIATION 日本セキュリティ監査協会

2019年1月7日

監査人の警鐘 - 2019年 情報セキュリティ十大トレンド

- 被害の拡大、深刻化に更なる注意を -

特定非営利活動法人日本セキュリティ
居範久）は、情報セキュリティ監査人
しました。

2019年の十大トレンドは、下記のと
ンク入りした「仮想通貨の盗難、詐欺
的型攻撃による被害の甚大化」及び
る拡大」です。

情報セキュリティ監査人が選ぶ
情報セキュリティ十大トレンド（2019年予測）

ランク	項目	ポイント
1 (-)	仮想通貨の盗難、詐欺の拡大	236
2 (2)	巧妙化する標的型攻撃による被害の甚大化	172
3 (3)	家庭用IoT機器のセキュリティ不備によるプライバシー侵害の更なる拡大	171
4 (6)	ビジネスメール詐欺被害の更なる深刻化	141
5 (5)	働き方改革の推進普及による新たな脅威の発生	127
6 (-)	時代遅れとなりつつあるパスワード認証	103
7 (10)	GDPRを乗り越えても残る諸外国のプライバシー規制リスク	102
8 (1)	高度化するランサムウェアによる被害拡大	93
9 (-)	問われるサイバーセキュリティ経営の責任体制	85
10 (-)	クラウドバイデフォルトの情報セキュリティ体系化	77

()は前年のランク

●「カード有効期限が切れています！」Amazonかたるフィッシングメール出回る

https://www.antiphishing.jp/news/alert/amazon_20190115.html

このニュースをザックリ言うと・・・

- 1月15日（日本時間）、フィッシング対策協議会より、Amazonをかたるフィッシングメールが出回っているとして警告が出されています。

- フィッシングメールは、件名が「Amazoneプライムのお支払いにご指定のクレジットカード有効期限が切れています！」で始まり（宛先のメールアドレス記載）、本文には「Amazonプライムの会費支払いに利用できる有効なクレジットカードアカウントが登録されていない」等と記載、リンク先は「asmazon-●●●●.com」といったドメインで、偽のログインフォームが表示されるサイトとなっています。

AUS便りからの所感等

- 今回のフィッシングサイトは、「Amazone.co.jp」や「メールボックス(※メールアドレスの意)」といった不審な記述こそあるものの、本物のサイトに極めて似通ったデザインとされている点には注意が必要でしょう。

- 現在確認されているフィッシングサイトと異なり、本物のAmazon.co.jpのサイトは「https:// 」で始まり、ログインフォームのメールアドレス入力欄に「Eメールまたは携帯電話番号」と表示されていますが、今後このような相違点も修正されたより洗練されたフィッシングサイトが登場する可能性も十分に考えられます。

- フィッシングサイトに対する防御としては、メーラー・ブラウザ・セキュリティソフトおよびUTMのアンチスパム機能・アンチフィッシング機能を必ず有効にした上で、普段利用しているWebサイトは事前にブラウザのブックマークに登録し、可能な限りメール上のリンクからではなく、ブックマークからアクセスするようにすることを強く推奨致します。

●クラウドサービスへの不正アクセスで約40万件の顧客情報が流出か？

https://japan.cnet.com/article/35130441/

このニュースをザックリ言うと・・・

- 昨年12月20日（日本時間）、ウェブマーケティングメディア「ferret」等を運営するベーシック社より、同社が運営する複数のサービスが不正アクセスを受け、約40万件の顧客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、被害を受けたのは前述の「ferret One」、ウェブマーケティングツール「ferret One」およびITサービス・ツール比較サイト「マケスト」における導入企業・ツールで取得した顧客・資料ダウンロード会員等の情報となっています。

- 上記サービスで利用しているクラウドサービスに9月26日に不正アクセスされ、顧客情報が格納されたファイルに攻撃者がアクセス可能な状態にあったとされていますが、攻撃の痕跡から仮想通貨採掘プログラムのインストールを目的としたものと想定されており、一次調査では情報流出の痕跡は確認されていないとのことです。

AUS便りからの所感等

- 攻撃者は、クラウドサービスへアクセスするための認証キーの一つを何らかの方法で奪取・悪用し、不正なサーバを内部で作成したとされており、最終的には全ての認証キーの無効化と再作成、不正アクセス経路の遮断を行うとともに、セキュリティ強化等の対策を講じたとしています。

- オンプレミスと異なり、クラウドサービスには比較的容易にサーバの追加等が可能な利点がある一方、サービスの認証キーや管理者権限を奪取されることにより、攻撃者にリソースを勝手に使用される可能性があります。

- オンプレミスとクラウドでどちらが安全・危険かはもはや一概に言えるものではありませんが、いずれの形をとるにしても、攻撃経路や不正アクセスを受けたとみられる対象の調査のため、アクセスログ等の取得と分析を行う体制をとることが重要でしょう。