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。

●JNSA「セキュリティ十大ニュース」発表…ロシア・ウクライナ関連の話題が1位、国内セキュリティ事件発生も日常的に

https://www.jnsa.org/active/news10/2022.html

このニュースをザックリ言うと・・・

- 12月23日(日本時間)、日本ネットワークセキュリティ協会(JNSA)より、「2022セキュリティ十大ニュース」が発表されました。
- 今回は1位に「ロシアがウクライナへ軍事侵攻」が取り上げられ、次いで2位「取引先企業へのサイバー攻撃でトヨタ自動車の国内全工場が稼働停止」、3位「全市民46万人余の個人情報入ったUSBを紛失 尼崎市が発表」、4位「KDDI大規模通信障害 丸2日間」、5位「大阪急性期・総合医療センターでランサム被害」と、国内で大きく報じられたセキュリティインシデントが挙がっています。
- またマルウェア関連では7位「休眠から再び戻ってきたEmotetが活動再開」、ソフトウェアの脆弱性関連では10位に「Log4jの脆弱性」が挙がっています。
- 昨年はランクインしていなかった「セキュリティにかかわる制度の発足や世相などのニュース」も、今年は6位「経済安全保障推進法公布」、8位「改正個人情報保護法施行」、9位「デジタル庁発足1周年」が挙がりました。

AUS便りからの所感等

- 1位のロシア対ウクライナ関連では、侵攻開始前後から発生しているサイバー攻撃の他、双方がニュースメディア・ブログ・SNS等において自軍への支持を得るための戦いを繰り広げていることにも言及しています。
- 2～5位に相次いで挙がっている国内のインシデント等も鑑み、JNSAでは「セキュリティの事件事故は日常茶飯事になり、毎日起こる交通事故と大差ない報道ぶりになってきた」等としています。
- 年末年始にこのような振り返りが行われるのはどの分野でも定番で、セキュリティ関連でも他の団体・企業がそれぞれの立場や視野から発表する同種のランキングはそれぞれ異なった顔ぶれ・順位となるとみられ、視点や取り上げる範囲等の違いによる差異を踏まえながら複数の記事を参照することにより、情報セキュリティに関するトレンドを幅広くキャッチアップすることが大切でしょう。

JNSA

セキュリティのプロが選ぶ！

JNSA 2022セキュリティ十大ニュース

～セキュリティニュースの二極化は何を示唆するのか～

2022年12月23日
セキュリティ十大ニュース選考委員会委員長　大木 榮二郎

今年のトップニュースはロシアのウクライナ侵攻。昨年の十大ニュースで「きな臭さが漂う不気味さを秘めている」としたが、その不気味さが表面に現れてきた。ロシアのウクライナ侵攻に際してのサイバー攻撃に、米国もサイバー攻撃の作戦を実行していた。

ウクライナの領土のみが主戦場と化す異様な光景の背後には、NATOと戦術核をちらつかせるプーチンロシアとの直接対決の構図を避けたい意図があり、サイバー戦が核戦争にもつながりかねない不気味さがある。世界にはこのような侵攻が懸念される状況がほかにもあり、サイバー攻撃はますますエスカレートすると考えておかなければならない。日本でも「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）、の論議が始まり、その「司令塔」の新設や、自衛隊・警察庁への民間ハッカーの登用も検討されている。

第2位以降には、トヨタ自動車や医療機関などが取引先へのランサム攻撃で被害が拡大し、サプライチェーン全体の安全確保の課題を浮き彫りにした事件やEMOTET、Log4Jなど民間へのサイバー攻撃のニュースが続き、第6位には経済安全保障推進法の公布がランクイン、インフラの安全確保や供給網の強化などにサイバーセキュリティ対策の強化が求められている。

● Twitterアカウント情報流出、2億件超に…2021年時点の情報、パスワードは含まれず

https://news.mynavi.jp/article/20230107-2556341/
https://gigazine.net/news/20230106-twitter-users-email-leaked-online/
https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/

このニュースをザックリ言うと・・・

- 1月4日(現地時間)、米IT系メディア「Bleeping Computer」等より、2億件を超えるTwitterアカウント情報がハッカーフォーラムで販売されていることが報じられています。

- 含まれている情報は、メールアドレス・ユーザー名・ユーザーの本名・フォロワー数・アカウント作成日等で、パスワードは含まれないとのことです。

- 2022年1月に修正されたTwitterの脆弱性が修正前に悪用されて奪取された、2021年当時の情報とされ、2022年7月に540万人分がハッカーフォーラムで販売されていた(AUS便り 2022/08/16号参照)ものと同じ出所とみられています。

AUS便りからの所感

- 直前に2022年12月にも約4億件のデータが20万ドルで販売されていましたが、今回報じられたのはこれを精査した約2億2,160万行のデータで、わずか2ドルで販売されていたとのことです。

- 流出したメールアドレス・パスワードのデータベースを運営するWebサイト「Have I Been Pwned」(以下HIBP)では、当該データリストが追加され、Twitterに登録したメールアドレスが流出していないかの確認が可能となっています。

- Twitterユーザーにおいては、これが新たな不正アクセスではなく、過去に攻撃者に奪取されたデータであり、現時点でパスワードが流出した様子はなく、直接不正ログインはできないとみられること、一方で攻撃者がこれで得られたメールアドレスをもとにフィッシング等の攻撃を行う恐れがあることに留意し、正しい情報をもとに慎重に行動することが肝要です。

● 12月フィッシング報告件数は65,474件…3か月連続で減少

https://www.antiphishing.jp/report/monthly/202212.html

このニュースをザックリ言うと・・・

- 1月6日(日本時間)、フィッシング対策協議会より、12月に寄せられたフィッシング報告状況が発表されました。

- 12月度の報告件数は65,474件で、11月度(https://www.antiphishing.jp/report/monthly/202211.html)の70,204件から4,730件減少しています。

- フィッシングサイトのURL件数も13,810件と、11月度(24,114件)から10,304件の減少、フィッシングに悪用されたブランド数は78件で11月度(87件)から9件減少となっています。

- Amazonを騙るフィッシングが全体の約51.7%と2か月連続で急増(11月度36.5%)、以下イオンカード・ETC利用照会サービス・オリコ・えきねっと・国税庁を騙るものと合わせて全体の約82.2%を占めたとのことです。

AUS便りからの所感

- フィッシングサイトで使用されるTLD(トップレベルドメイン)の割合は、.tkが約25.0%でトップ、次いでtop(約22.4%)、.org(約16.1%)、.com(約13.1%)、以下 .shop、.cn、.icuが上位に挙げられています。

- ETCを騙るフィッシングではフィッシングサイトへの誘導手段としてQRコードを用いるケースがみられている他、フィッシングメールからキャッシュレス決済の正規サービスへ誘導し、送金させる手口も報告されているとして、同協議会ではそれぞれ注意喚起しています。

- 9月度には10万件を超えた報告件数は、3か月連続で減少傾向を見せていますが、いつまた爆発的な拡散がみられるかわからないため、利用しているWebサイトへのアクセスは事前に登録したブックマークや公式のモバイルアプリからアクセスし、メールなどで通常と異なるサービスサイトへのアクセス、通常と異なる決済方法等を示された場合には十分に警戒するよう心掛けましょう。

フィッシング対策協議会
Council of Anti-Phishing Japan