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。

●在宅ワークでUSBメモリ紛失…児童らの個人情報3,083件が行方不明に

https://cybersecurity-jp.com/news/37573
https://www.sanyonews.jp/article/1028542/

このニュースをザックリ言うと・・・

- 7月6日(日本時間)、学校法人 おかやま希望学園より、同学園が運営する吉備高原のびのび小学校の児童等の個人情報が記録されたUSBメモリー3本が紛失したと発表されました。

- USBメモリーには同小学校の2019～2020年度の児童、オープンスクールや宿泊体験に参加した児童、およびその保護者等延べ3,083人分の氏名・住所・電話番号等が保存されていたとのことです。

- 6月12日、同学園の校長が在宅ワークのためUSBメモリーを持ち帰った後、2日後に紛失が発覚、後日警察に紛失届を提出しましたが、見つかっていないとのことです。

AUS便りからの所感等

- 個人情報が入ったUSBメモリーの紛失は今年に入っても頻繁に発生していますが、5月には大阪府の公立高校生徒の個人情報をテレワークの必要性から私物のUSBメモリーに保存したものを紛失する事例(https://cybersecurity-jp.com/news/36534)が発生しています。

- メモリースティック等USBデバイスの利用は、紛失のみならずマルウェア感染を拡散させる等のリスクもあり、使用を禁止する組織が多くなっていますが、情報のやりとりが不便になる状況を是認するままでは、暗黙のうちにルールに反してデバイスが利用される可能性がまた発生することでしょう。

- 適切に管理された有用な代替手段の用意、例えば紛失時に第三者が読みだせないようデータを暗号化してUSBデバイスに保存するといったソリューションの導入、あるいはテレワークへの移行も進んでいる現状においては厳密なアカウント管理のもとでWebからアクセス可能なストレージの提供等により、利便性とデータ保護等の安全性の双方を確保することも検討すべきでしょう。

● 6月のフィッシング報告件数、引き続き増加傾向に…対策協議会発表

https://www.antiphishing.jp/report/monthly/202006.html

このニュースをザックリ言うと・・・

- 7月2日(日本時間)、フィッシング対策協議会より、6月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 6月度の報告件数は16,811件で、5月度の14,245件から2,566件の増加、またフィッシングサイトのURL件数は5,481件で、5月度の4,052件から1,429件の増加となっています。

- Amazon・Apple・LINE・楽天を騙るフィッシングメールについての報告が全体の約88%、特にAmazonについては全体の約56%を占めているとのことです。

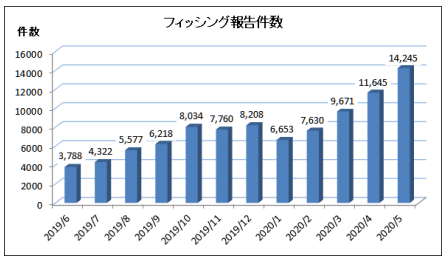
AUS便りからの所感

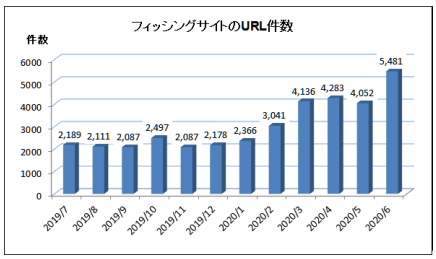
- フィッシングサイトのURL件数は、3月度4,136件、4月度4,283件と、5月度まで4,000件台前半を推移していましたが、今回急増しています。

- SNSの短縮URL機能等の悪用により、アンチフィッシング機能によるURLフィルタリングを回避するケース、あるいは大量に取得したランダムな文字列の独自ドメインに正規サイトのドメイン名を追加したURLにより、スマートフォン等で閲覧した場合に正規サイトと誤認させるケース等が報告されているとのことです。

- 今のところ、全く新しいフィッシングのパターンが報告されたわけではなく、引き続き普段からのフィッシング回避策として、不審なメールについてネット上の情報を調査して確認する、利用しているサービスのサイトにはブックマークからアクセスする、等を心がけることを強く推奨致します。

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





●ヨーロッパで過去最大規模のDDoS攻撃…国内回線からも攻撃

https://www3.nhk.or.jp/news/html/20200709/k10012506261000.html
https://foxsecurity.hatenablog.com/entry/2020/07/12/090000

このニュースをザックリ言うと・・・

- 7月9日(日本時間)、ヨーロッパの銀行に対し6月に大規模なDDoS攻撃が発生していたことがNHKのニュースサイトで報じられました。

- 攻撃が発生したのは6月21日とされ、情報セキュリティ会社の分析によれば1秒当たり8億900万パケットという大量の通信があったとのことです。

- DDoS攻撃は複数の国のネットワークから行われ、42%がアメリカ、10%が韓国、9%がベトナムからとされ、日本からのパケットも6%あったとされています。

AUS便りからの所感

- このDDoS攻撃については、銀行のシステム側で対策がとられ、防御に成功していたことから大事には至らず、メディア各社が報じる事態にもなっていなかった模様です。

- 一方で、対策を行ったとされるCDN最大手のアカマイ・テクノロジーズ社によれば、同社が防御したDDoS攻撃としては過去最大のもので、データ量が非常に小さいパケットを大量に送信することにより、DDoS防御機能を回避しようとしていたとみられています。

- 2016年以降流行した「Mirai」の例もあり、IoT機器にマルウェアが感染してDDoS攻撃に悪用される可能性を抑制するため、全ての機器を確実な管理下に置き、管理画面へのアクセス制限やパスワードの変更等の対策は必ず行うようにしましょう。

NHK

ヨーロッパで過去最大規模のサイバー攻撃 国内回線からも攻撃

2020年7月9日 16時28分　IT・ネット

大量のデータを送りつけてシステムをダウンさせる「DDoS攻撃」と呼ばれるサイバー攻撃で、先月、ヨーロッパの銀行に過去最大規模とみられる攻撃が行われたことが分かりました。日本の回線からも攻撃が行われていて専門家はネットワーク機器が不正アクセスを受けて悪用されたおそれがあると指摘しています。

6月21日、ヨーロッパの銀行のサーバーに大量のデータを送りつける「DDoS攻撃」が検知され、情報セキュリティー会社が分析したところ、1秒当たり8億900万パケットという大量の通信が行われていたということです。

これはDDoS攻撃としては過去最大の規模とみられるということですが、銀行のシステムは対策をとっていたため被害はありませんでした。