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。

●大阪のテレビ局二局の放送前番組素材紛失…保存媒体が盗難に-

https://www.itmedia.co.jp/news/articles/2212/13/news120.html
https://www.ytv.co.jp/corp/updata/file_ytivxgt9i6ekemxqpr3dnhw93hzslx.pdf
https://www.ktv.jp/info/ktvinfo/2022/20221214/

このニュースをザックリ言うと･･･

- 12月12日(日本時間)、読売テレビより、放送前の番組素材が保存された媒体が紛失したと発表されました。
- 同局の発表では、被害を受けたのは同局の3番組のロケ収録・スタジオ収録およびMVの素材とされており、同10日早朝に番組スタッフが電車内で媒体が入ったカバンを盗まれたものとされています。
- 同14日には関西テレビからも同様の発表があり、当該スタッフ所有の同じ媒体に二局の番組素材が含まれていたとみられています。

AUS便りからの所感等

- 紛失した媒体はスタッフの個人所有で、両局では記録媒体の使用時にロックをかけるよう指導していましたが、紛失時にはロックされていなかったとのことです(また読売テレビでは個人所有の媒体使用を禁止していました)。
- 外部に持ち出した保存媒体の紛失事案としては、6月に尼崎市において全市民分の個人情報を記録したUSBメモリーが紛失した事例があり(AUS便り 2022/06/28号参照)、11月から12月にかけて同市や委託先会社からの調査報告書が発表されています。
- 両局とも、社内ルール徹底および管理の適正化による再発防止に努めるとしていますが、媒体紛失の事故が度々報じられる今日、システム面からの機密情報・個人情報流出の抑制(今回で言えば登録された媒体へのみの転送、ロックや暗号化を強制的に行う等)を図る仕組みが確立されることを期待したいものです。

ITmedia NEWS

読売テレビ、記録媒体を紛失　番組スタッフが電車で居眠り、その間に盗難か　放送前の映像素材などを収録

2022年12月13日 13時46分 公開　[松浦立樹，ITmedia]

印刷　172　Share　B!　20

讀賣テレビ放送（大阪市中央区、以下読売テレビ）は12月12日、同社番組スタッフが放送前の映像素材が入った記録媒体を紛失したと発表した。紛失したのは10日。記録媒体が入ったカバンごと電車内で紛失した。番組スタッフは電車内で居眠りをしており、その間に盗難に遭った可能性が高いとしている。

読売テレビの番組スタッフが放送前の映像素材が入った記録媒体を紛失（公式Webサイトから引用）

紛失した記録媒体は、番組スタッフが個人所有していたもので、ロックはかかっていなかった。記録媒体の中には、放送前を含む複数の番組のロケ取材やスタジオ収録した映像素材を収録していた。同社では番組映像素材を社外に持ち出す際、私物の記録媒体の使用を禁止していたが、このルールが守られていなかった。

● SVG画像に悪意のあるファイルを仕込む攻撃、Cisco研究チームが注意喚起

https://news.mynavi.jp/techplus/article/20221218-2539543/
https://blog.talosintelligence.com/html-smugglers-turn-to-svg-images/

このニュースをザックリ言うと・・・

- 12月13日(現地時間)、ネットワーク機器大手である米Cisco社のセキュリティ研究チームTalosより、SVG(Scalable Vector Graphics)画像を悪用した攻撃について注意喚起が出されています。

- SVGの実体はXMLファイルであり、仕様上内部にJavaScriptや別の画像ファイルを含めることも可能とされていますが、これを悪用し、不正なZIPアーカイブを含むJavaScriptをSVGファイルに埋め込むことにより、PC上でスクリプトによるマルウェアの生成を行うとされています。

- 既にマルウェア「Qakbot(Qbot)」が、この手法を用いていることを確認しているとのことです。

AUS便りからの所感

- マルウェア等に関連するファイルを外部から取得せず、HTML文書あるいは添付メールに含めたスクリプトで生成する、いわゆる「HTMLスマグリング(HTML smuggling)」と呼ばれる攻撃の一種とされています。

- 不正な形式の画像を読み込んだだけで攻撃を受けるという事例はこれまで皆無だったわけではありませんが、バッファオーバーフロー等のバグを悪用したものであったこれまでの事例と異なり、Webブラウザーエンジンにおける SVG画像の正当な処理を悪用するものであり、Chrome等のブラウザー側で何らかの対策が行われるか、あるいはアンチウイルス等で適切に検出されるようになるか、今後の動向が注目されます。

TECHR Powered by マイナビニュース

SVG画像を悪用したHTMLスマグリング攻撃が発見される

掲載日 2022/12/18 17:13　　著者：後藤大地

Cisco Talos Intelligence Groupは12月13日(米国時間)、「HTML smugglers turn to SVG images」において、スケーラブル・ベクター・グラフィックス(SVG: Scalable Vector Graphics)画像を悪用した比較的新しいHTMLスマグリング手法が攻撃者に使われていると伝えた。HTMLスクリプトタグを含むSVG画像をエンコードしたHTML添付のフィッシングメールを発見したと報告されている。

●経産省・総務省・警察庁・NISC、年末年始における情報セキュリティの注意喚起を合同で発表

https://internet.watch.impress.co.jp/docs/news/1465305.html
https://www.npa.go.jp/cybersecurity/

このニュースをザックリ言うと・・・

- 12月20日(日本時間)、経済産業省・総務省・警察庁および内閣官房内閣サイバーセキュリティセンター(NISC)より、「年末年始休暇において実施いただきたい対策について」と題した注意喚起が連名で発表されました。

- 4機関では8月にも夏季休暇を迎えるにあたり同様の注意喚起を行っていたものの、以後もランサムウェア攻撃の被害やEmotetの活動再開、あるいは9月に政府機関等を狙ったDDoS攻撃の発生を鑑み、国民の誰もがサイバー攻撃の懸念に直面していると述べています。

- 今回の注意喚起においては、テキスト以外にポスター形式でもまとめられたものがPDFで公開されています。

AUS便りからの所感

- 特に重要なポイントとして「対処手順・連絡体制(休暇期間中の監視体制の確認・強化、インシデントの対処手順の確認、連絡体制)」「バックアップ」に関する要点、その他にもセキュリティ対策責任者・システム担当者向け、およびユーザー向けに休暇前・休暇後に行うべき対策の要点がまとめられています。

- IPA等も同様の注意喚起を行っています(AUS便り2022/12/13号参照)が、各種対策・確認ポイントはそれぞれで概ね共通しており、特定の攻撃に特化したものでもなく、今後もゴールデンウィーク等の長期休暇時期に向けて、あるいはそれでなくとも常時において、準備・点検を行うよう是非とも意識しておきましょう。

警察庁 National Police Agency