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。

●2020年は上場企業とその子会社から2,515万人分の個人情報が流出…原因の多くは「ウイルス感染・不正アクセス」

https://www.itmedia.co.jp/news/articles/2101/15/news131.html
https://www.tsr-net.co.jp/news/analysis/20210115_01.html

このニュースをザックリ言うと･･･

- 1月15日(日本時間)、東京商工リサーチ(以下TSR)より、上場企業およびその子会社から2020年に公表された情報漏洩・紛失事故についての調査結果が発表されました。

- 2020年については88社から103件の事故が公表、漏えいした個人情報は25,150,047人分に上るとしており、うち「ウイルス感染・不正アクセス」が原因となった事故が件数では51件(49.5%)、被害を受けた個人情報でも23,727,268件(94.3%)という結果となっています。

- 最も漏洩・紛失が多かった事故は12月に公表されたPayPay関連情報への不正アクセスの20,076,016件(AUS便り 2020/12/14号参照)で、次いで楽天グループの情報への不正アクセスの1,486,291件(同 2020/12/21号参照)となっています。

AUS便りからの所感等

- TSRが2012～2020年について行った調査結果によれば、9年間に上場企業から公表された分だけでも日本の人口に匹敵する個人情報の漏洩が発生しているとのことです。

- また、2020年はこれまで社数・件数において最多だった2013年(87社・107件)に匹敵するものとなっていますが、新型コロナウイルス感染症の急激な拡大によるテレワークへの移行等の過程で、セキュリティ対策が不十分なまま新たなシステムが導入されている所が狙われた可能性も考えられます。

- 調査結果では「新型コロナで広がった様々な働き方の変化により、企業はより柔軟なネットワークシステムなどのIT投資が必要となっている」「これまで以上にセキュリティ対策や情報管理の体制づくりが、あらゆる組織で対策すべき重要課題として浮上している」と結んでおり、新たに導入されたシステムについてセキュリティ面での不安な点を洗い出し、たとえ後付けであっても適切なセキュリティ対策を、速やかに十分な予算のもとで行うよう検討すべきと考えます。

ITmedia NEWS

2020年は2515万人分の個人情報が流出　原因の多くは「ウイルス感染・不正アクセス」

2021年01月15日 17時08分 公開　[ITmedia]

2020年、個人情報の漏えい・紛失事故を公表した上場企業とその子会社は88社、事故件数は103件、流出した個人情報は2515万47人分――そのような調査結果を東京商工リサーチが1月15日に発表した。事故の原因で最も多かったのは「ウイルス感染・不正アクセス」。同社は「サイバー攻撃は巧妙化かつ高度化し、セキュリティ対策の重要性が改めて問われている」としている。

調査を始めた2012年以来、個人情報の漏えい・紛失事故を公表した上場企業と子会社は88社と最多

●1行のコマンドでWindowsのディスクが破損する脆弱性…MSが修正へ

https://pc.watch.impress.co.jp/docs/news/1300447.html
https://pc.watch.impress.co.jp/docs/news/1300761.html
https://www.bleepingcomputer.com/news/security/windows-10-bug-corrupts-your-hard-drive-on-seeing-this-files-icon/

このニュースをザックリ言うと・・・

- 1月14日(現地時間)、PC情報サイトの米Bleeping Computerより、Windowsを起動不能に追い込む恐れのある未修正の脆弱性が存在するとして注意喚起が出されています。

- 脆弱性はWindowsのNTFSファイルシステムに存在するもので、わずか1行のコマンドを実行するだけでハードディスク領域が破損し、OSを再起動してディスクチェックを行うよう要求され、最悪の場合OSが起動しなくなる場合もあるとのことです。

- 脆弱性を発見したセキュリティ研究者は、細工されたショートカットの表示だけでも攻撃が可能であり、数年前からMicrosoftへ報告していたにも拘らず未修正のままであったとしていましたが、その後Microsoftの広報担当者から「影響を受けるデバイスに対しアップデートをできる限り早く提供する」と発表されています。

AUS便りからの所感

- Bleeping Computerの記事やそれを取り上げた各メディアの記事でも呼び掛けられていますが、脆弱性を悪用可能なコマンドが掲載されていたとしても、興味本位で決して実行しないようにしてください。

- 1月18日時点でセキュリティパッチはリリースされておらず、それまでの間に、アンチウイルスソフト等において脆弱性の悪用を遮断するよう対応することも考えられますが、根本的な対策としてはやはりOS側での対応が不可欠となるでしょう。

Impress Watch

アイコンを見るだけでディスクが破損するNTFSの脆弱性が修正へ

関根 慎一　2021年1月18日 13:51

画面上にアイコンが表示されただけでWindows 10のドライブが破損するNTFSの脆弱性について、米Microsoftが修正する旨の発言を行なったことが海外メディアで伝えられた。

この脆弱性は、Windows 10 1803以降のバージョンにおいて文字列"$i30"を含んだコードがWindowsショートカットに含まれる場合に、そのショートカットを実行しなくてもドライブが破損するというもの。コマンドプロンプトのcdコマンドなどでコードを実行した場合はもちろん、Windows上でアイコンが見えた時点で、そのショートカットがZIPファイルの中に存在するだけでも発生する。infosec所属のセキュリティ研究者Jonas Lykkegaard氏が発見し、数年前からMicrosoftに報告していたが、記事執筆時点でも修正アップデートは提供されていない。

●福岡県のコロナ感染者約9,500人の情報、第三者が閲覧可能な状態に…クラウドの設定不備原因

https://www.nishinippon.co.jp/item/n/679502/
https://www.pref.fukuoka.lg.jp/contents/covid19-rouei.html

このニュースをザックリ言うと・・・

- 1月6日(日本時間)、福岡県より、県内の新型コロナウイルス感染症陽性者ほぼ全員にあたる約9,500人の個人情報が第三者から閲覧可能な状態にあったことが発表されました。

- 同県の新型コロナウイルス感染症対策本部(調整本部)が作成した陽性者のデータを、2020年4月以降、医療関係者間においてクラウド(一部報道によればGoogle Drive)上で共有していましたが、11月30日にデータのアクセス権限を付与するメールを誤って第三者に送信した際の対応に不備があり、その後約1ヶ月間、当該第三者1名が文書ファイルへ外部から直接アクセスすることが可能な状態にあった模様です。

- 1月6日の報道機関からの取材をうけて問題が発覚し、現在情報はクラウド上から削除されているとのことです。

AUS便りからの所感

- コロナ感染者に関する情報が誤って公開状態にあった問題としては、昨年5月にも愛知県の事例があります(AUS便り 2020/05/11号参照)。

- 発表では、クラウドの共有領域には、フォルダーや文書ファイルのURLを直接指定した者、あるいは権限を付与された者がアクセス可能とされており、権限を付与するメールの誤送信後にフォルダーへのアクセス権限を削除する対応は行ったものの、フォルダー内の各ファイルへのアクセスについては対応されていなかった模様です。

- クラウド上に保存された機密情報が設定ミスで第三者にアクセス可能であった事例は度々報じられていますが、今回については第三者への権限の付与とその削除に関するオペレーションミスから問題の露見に繋がったもので、それがなければ設定面については問題が指摘されなかった可能性もありますので、攻撃者からの攻撃の他にこのようなオペレーションミスで機密情報が安易に晒されてしまう状態とならないよう、十分なセキュリティ設定が実施されているかの確認が肝要です。

西日本新聞

福岡県のコロナ感染者情報流出　名前など9500人分　外部からデータ閲覧可能に

2021/1/7 6:00 (2021/1/7 6:09 更新)
西日本新聞 一面 社会面 華山 哲幸

福岡県は6日、県内でこれまでに確認された新型コロナウイルス感染者の9割超に相当する約9500人分の名前や居住する市町村などの個人情報がインターネット上で第三者が閲覧できる状態になっていたと発表した。アクセス権限を持っているか、ホームページ上の住所に当たるURLを入力しないと閲覧できないが、県は権限付与のメールを誤送信した部外者の男性以外に流出がなかったか確認する。