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。

●未修正のWindows脆弱性と攻撃が報告…MS回避策発表、Defenderでも対応

https://pc.watch.impress.co.jp/docs/news/1413507.html
https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e

このニュースをザックリ言うと･･･

- 5月30日(現地時間)、米Microsoft社より、Windowsの診断ツール「Microsoft Support Diagnostic Tool(MSDT)」に未修正の脆弱性(CVE-2022-30190)が発見されたとして、回避策等が案内されています。

- 脆弱性は外部のセキュリティ研究者によって「Follina」という名称で発表されたもので、例えば悪意のあるOfficeドキュメントファイルから不正なコマンドの実行が可能になるとされ、これを悪用した攻撃が既に確認されているとのことです。

- 回避策として、レジストリの操作により「ms-msdt」URLプロトコルハンドラを無効化する方法が提示されている他、OS内蔵のアンチウイルス機能「Microsoft Defender Antivirus」でもウイルス対策のバージョン「1.367.719.0」で攻撃を検出するようになっているとのことです。

AUS便りからの所感等

- 悪意のあるOfficeファイルからの攻撃は不正なマクロの実行によるものが多く、ファイルを保護ビューで開く限り回避可能とされていますが、Follinaと命名した前述のセキュリティ研究者の発表によれば、今回の脆弱性については「.rtf(リッチテキスト)」形式のファイルをプレビューしただけでも不正なコードが実行される恐れがあるとされています。

- 脆弱性は現時点で修正されていないいわゆる「ゼロデイ脆弱性」であり、6月15日(日本時間)に予定される月例セキュリティアップデートあるいはそれ以前に緊急でパッチがリリースされる可能性があります。

- 前述したMicrosoft Defender Antivirus以外のベンダーによるアンチウイルス製品においても今後対応されるとみられますが、今回に限らずアンチウイルスソフトやUTMの導入、メーラー・ブラウザー等の各種セキュリティ機能を確実に有効にすること、そしてアンチウイルスソフトとそのパターンファイル等を必ず最新に保つことは重要です。

Impress Watch

Microsoftの診断ツールにリモートコード実行の脆弱性

宇都宮 充　2022年5月31日 18:59

Microsoftは30日(米国時間)、同社の診断ツール「Microsoft Support Diagnostic Tool(MSDT)」において、リモートコード実行につながりうるゼロデイ脆弱性(CVE-2022-30190)があったとして情報を公開した。深刻度はImportantと評価している。

Microsoft WordなどからURLプロトコルを通じてMSDTを呼び出すさいに、リモートコード実行ができてしまう脆弱性で、攻撃者が悪用すると、呼び出し元のアプリケーションの権限で任意のコードを実行できてしまう恐れがある。これにより、その権限の下でプログラムのインストールやデータの閲覧、改変、消去、新規アカウントの作成などが可能となるという。

●釜石市職員が全市民分の個人情報持ち出し…住基データ約32,000人分

https://www3.nhk.or.jp/lnews/morioka/20220526/6040014383.html
https://www.asahi.com/articles/ASQ5V6SMHQ5VULUC01G.html
https://www.city.kamaishi.iwate.jp/docs/2022053000033/

このニュースをザックリ言うと･･･

- 5月26日(日本時間)、岩手県釜石市より、同市が管理する個人情報が同市職員2名によって持ち出されていたと発表されました。
- 発表によれば、持ち出されていたのは、住民基本台帳に掲載されていた全市民分にあたる約32,000人分の氏名・住所・生年月日・収入額等および約600人分のマイナンバーのデータとされています。
- 当該職員はデータを自宅PCに送信する等していましたが、それ以外の外部への流出や被害は確認されていないとのことです。
- 同市では当該職員を懲戒免職処分とした他、住民基本台帳法違反の疑いで刑事告訴したとのことです。

AUS便りからの所感

- 報道によれば、少なくとも7年前から21回にわたって、個人情報の自宅PCへの送信等を行っていたとしており、違法行為であるという意識も希薄であった模様である一方、同市ではマイナンバーの持ち出しの対象者に対し変更の意向を確認する等の事態となっています。
- 内部の人間による個人情報の持ち出しは2014年のベネッセのような大規模な事例も含め様々な企業・組織で発生し、多くは明確に不正利用を意図したものとなっています。
- 組織内に対し個人情報の厳密な取り扱い、外部からの攻撃・内部からの持ち出しに拘わらず流出がもたらす被害についての啓発・教育は重要であり、同時に内部からの悪意による持ち出しにも、標的型攻撃等によって内部に侵入した攻撃者・マルウェアによる流出にも有効な防御策となる「出口対策」のソリューションについても導入を検討すべきでしょう。

NHK

市民３万人分の個人情報流出 釜石市職員２人が懲戒免職

05月26日　18時37分

釜石市は、市民全員にあたるおよそ３万人分の氏名や住所などの個人情報のデータを自宅のパソコンにメールで送るなどして持ち出したとして、職員２人を懲戒免職にしました。

これは、釜石市の野田武則市長が記者会見して明らかにしたものです。

それによりますと、総務企画部の４０代の女性の係長と建設部の４０代の男性の主査が、氏名や住所、生年月日などが記載された住民基本台帳や業務上作成した表計算ソフトのデータを、少なくとも７年前から２１回にわたって、自宅のパソコンのメールアドレスに送ったり、お互いに送り合っていたということです。

データが持ち出されたのは、市の人口全体にあたるおよそ３万人分にも上るということです。

●ランサムウェアからのデータ復元成功は約69%に留まる…Veeam社発表

https://internet.watch.impress.co.jp/docs/news/1410453.html
https://www.veeam.com/jp/news/veeam-publishes-trend-survey-report-on-cyber-security.html

このニュースをザックリ言うと･･･

- 5月17日(現地時間)、バックアップ等データ保護ソリューションを提供する米Veeam Software社より、世界でのランサムウェア攻撃に関する調査レポート「Veeam 2022 Ransomware Trends Report」が発表されました。
- 調査は、日本を含む16ヶ国における、過去12ヶ月間に少なくとも一度はランサムウェア攻撃の被害を受けた経験のある企業のITリーダー1,000人を対象に行ったものとなっています。
- 被害を受けた企業の76%が身代金を支払っていますが、データの復元に成功した企業は支払いを行った企業の約69%に留まるとの結果が出ています。
- また、攻撃者の94%が、相手が自力でデータ復旧できないようバックアップストレージの破壊を試みていた等の結果も出ています。

AUS便りからの所感

- Veeam社ではランサムウェアからのデータ保護等に有用なソリューションを提供するとともに、適切なバックアップルールとして「最低でも3つのデータコピーを」「2種類のメディアに保存」「1つはオフサイト(別の場所)に保管」さらには「1つの書き換え不可能またはオフライン上のバックアップ」「バックアップ・リストアを確実に行う(エラー発生を0に)」とする「3-2-1-1-0ルール」を提唱しています(AUS便り 2021/09/14号)。
- 2021年10月には地方の病院で電子カルテシステムのデータが暗号化され、システムの復旧に2ヶ月かかる事態となる(AUS便り 2021/11/09号参照)等、ランサムウェアは依然として脅威となっており、システムの可用性と完全性の維持のため、データのバックアップソリューションの導入と、確実な復旧のための体制を整えることは常に検討が必要です。

Impress Watch

ランサムウェア被害企業の76%が身代金要求に応じるも…… 31%の企業がデータ復元に失敗

犯罪者はバックアップストレージを破壊することで復旧能力を無効化することも

大河原 克行　2022年5月19日 13:35

Veeam Softwareは、ランサムウェアに関する調査レポート「Veeam 2022 Ransomware Trends Report」の内容を公開した。

過去12カ月間に、少なくとも一度はランサムウェア攻撃の被害を受けた経験がある企業のITリーダー1000人を対象に行った調査で、ランサムウェア攻撃を受けた企業の76%が身代金を支払い、31%の企業がデータの復元に失敗していることが分かった。Veeam Softwareでは、「ランサムウェア攻撃に対する企業の防御策は、依然として不十分であることが判明した」と総括している。