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。

●VPN装置と全PCで管理者アカウントに推測されやすいパスワードの使い回し…2024年5月ランサムウェア事案の調査報告

https://www.nikkei.com/article/DGXZQOUF13ARY0T10C25A2000000/
https://www.popmc.jp/home/consultation/er9dkox7/lromw3x9/

このニュースをザックリ言うと･･･

- 2月13日(日本時間)、岡山県精神科医療センターより、2024年5月に同センターで発生した不正アクセス・個人情報流出事案についての調査報告が発表されました。

- ランサムウェア感染により、電子カルテシステムが停止、患者最大約40,000人分の個人情報等が流出したことが明らかになっています(AUS便り 2024/06/19号参照)。

- 報告書では不正アクセスの原因として、未更新だったファイアウォール装置・SSL-VPN装置の脆弱性を突かれたことの他、SSL-VPN装置と院内全てのPCで管理者アカウントにID「administrator」・パスワード「P@sswOrd」を使用していたことが指摘されています。

- 本件について報告書では「厚労省ガイドラインの遵守で十分に防げた事案であった」「脆弱性の放置や推測可能なパスワードの使いまわしなどは、サイバー攻撃が進化する中で『閉域網神話』による思考停止が招いた『人災』」等としています。

AUS便りからの所感等

- 医療機関へのランサムウェア攻撃事案としては他にも徳島県つるぎ町立半田病院、大阪急性期・総合医療センターの件が大きく報じられており、これらの調査報告書の策定に携わったSoftware ISACが今回の報告書にも関わっています。

- LAN上の各Windows PCへ侵入する「水平展開」にあたり、Windows PCに標準で作成される、管理者アカウントがリモートからアクセス可能な「管理共有」に接続した可能性がある等、技術的な詳細が報告されており、各システム管理者においては安全なシステムの構築・改修にあたり是非とも読み込んで参考とすることが望まれます。

- 報告書冒頭では、ウイルス対策ソフトの稼働とソフトウェアの脆弱性を確実に修正することの他、パスワードに使用するものとして、完全なランダムな文字列でなくとも、単語を複数組み合わせた20文字程度の「パスフレーズ」により、ランサムウェア等による不正ログイン攻撃リスクを大幅に低下させられるとしており、ユーザー側においても有用な内容を含んだものと言えます。

日本経済新聞

岡山の患者情報流出は「人災」　IDやパスワード使い回し

岡山　＋フォローする
2025年2月13日 18:55

保存

岡山市北区の岡山県精神科医療センターで昨年、システムがサイバー攻撃を受け最大約4万人分の患者情報が流出した問題で、センターの調査委員会は13日、厚生労働省の指針を守れば防げた「人災」だったとする報告書を発表した。

報告書によると、身代金要求型コンピューターウイルス「ランサムウエア」による攻撃で、近年同様の被害に遭った徳島県つるぎ町立半田病院や大阪市住吉区の大阪急性期・総合医療センターと同じく、パスワードの使い回しなどを突かれた。

昨年5月、国際的な犯罪組織が岡山県精神科医療センターの電子カルテシステムなどを暗号化し使えなくなった。「情報を窃取した。連絡しないと公開される」と脅迫があったが、連絡は取らず、身代金も払わなかった。

●ランサムウェアによる身代金支払い額、2024年は2023年から35%減少

https://gigazine.net/news/20250207-crypto-crime-ransomware-victim/
https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

このニュースをザックリ言うと・・・

- 2月5日(現地時間)、ブロックチェーン情報会社であるChainalysis社より、2024年にランサムウェア攻撃に対して支払われた身代金は2023年に比べ約35%減少したと発表されました。
- 2020年以降の年毎の統計では、2023年の身代金支払い額が約12億5,000万ドルだった一方、2024年は約8億1,355万ドルに減少したとしています。
- また2024年における月毎の統計(データ漏洩サイトの調査結果を基にしたとされる)でも、4月以降の身代金支払いは概ね減少傾向にあることが示されています。

AUS便りからの所感

- 一方で、2024年は被害件数が最も多く、計5263件のランサムウェア攻撃が成功したとする発表があり、また同上半期において(個別の攻撃としては)過去最高となる7,500万ドルが支払われる事案が報じられています。
- 前述した月毎の統計でも、下半期にかけて件数は増えていることが示されています。
- 各組織でのランサムウェア攻撃への対策に進展があったか、それが効果を上げたのか(データ復元を期待しての身代金支払いが不要なケースが増えたのか、等)という明確な言及はみられませんでしたが、ともあれ引き続きランサムウェア攻撃とデータ損失等の被害を外部で起きていることと考えず、アンチウイルス・UTMによる防御やデータ保護を意識したバックアップ実施等を心掛けることが重要です。


GIGAZINE

2025年02月07日 08時00分 セキュリティ

2024年のランサムウェアによるデータ身代金の支払いは2023年と比較し35%も減少していた

仮想通貨ランサムウェアによるデータ身代金の支払額が、2024年は過去最高となった2023年の12億5000万ドル(約1900億円)から約35%下落し、8億1330万ドル(約1230億円)に減少していたことがブロックチェーン情報会社・Chainalysisの調査で明らかになりました。

Crypto Ransomware 2025: 35.82% YoY Decrease in Ransomware Payments
https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

Chainalysis

35% Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments

● Microsoft・Adobe等、月例のセキュリティアップデートリリース

https://forest.watch.impress.co.jp/docs/news/1661987.html
https://msrc.microsoft.com/blog/2025/02/202502-security-update/
https://forest.watch.impress.co.jp/docs/news/1661985.html

このニュースをザックリ言うと・・・

- 2月12日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対するセキュリティアップデートがリリースされています。
- Windowsの最新バージョンはWindows 10 22H2 KB5051974(ビルド 19045.5487)、11 23H2 KB5051989(ビルド 22631.4890)および11 24H2 KB5051987(ビルド 26100.3194)等となります。
- 同日にはAdobe社より「InDesign」「Commerce」「Illustrator」「Photoshop Elements」等7製品について脆弱性が報告され、セキュリティアップデートがリリースされています。

AUS便りからの所感

- MSの月例アップデートでは、DHCPの脆弱性含む3件が特に危険度が高い(4段階中最高の「Critical」)と評価されています。
- Adobeの月例アップデートでは、「Commerce」について30件と特に多くの脆弱性が報告されています。
- MS以外にも他のベンダーも含めた月例のセキュリティアップデートのリリースが集中する、いわゆる「パッチチューズデー(米国時間での第2火曜日)」を、特にシステム管理者においては忘れず意識し、OSや機器のファームウェアから各種アプリケーションに至るまで確実かつ可能な限り速やかにアップデートを適用することにより、攻撃に備えること、またそれまでに発生する攻撃に対しアンチウイルス・UTM等による防御策をとることが肝要です。


Impress Watch

2025年2月の「Windows Update」が公開 ～ゼロデイ、「Critical」を含む57件の脆弱性に対処

Surfaceデバイスにもセキュリティパッチ

樽井 秀人 2025年2月12日 08:31

米Microsoftは2月11日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで57件（サードパーティーのものも含めれば67件）の脆弱性が新たに対処されている。