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。

●西日本大手スーパーでランサムウェア感染…業務・サービス提供に影響

https://www.itmedia.co.jp/news/articles/2402/22/news199.html
https://www.izumi.co.jp/corp/outline/news_release/

このニュースをザックリ言うと･･･

- 2月16日(日本時間)、広島県を中心に西日本で展開するスーパー「ゆめタウン」「ゆめマート」を運営するいずみ社より、同社のシステムがランサムウェアに感染したと発表されました。

- 感染により、同社アプリ、クレジットカード、ECサイト、チラシの配布さらには実店舗でのサービスが一部休止する事態となり、また社内でもメールシステムを含む各種システムの使用を停止、電話・FAX・郵送による連絡を余儀なくされているとのことです。

- 同22日・26日の発表によれば、個人情報の漏えいについては調査中ながら現時点では確認されておらず、クレジットカード情報は障害が発生したシステムと別のシステムでの運用のため漏洩していないとのことです。

AUS便りからの所感等

- 2月中を目途に被害全容の把握、のち段階的にシステムの再稼働を行い、完全な復旧は5月1日を予定しているとのことです。

- 実店舗に関しては一時食品売場の品薄状態も発生(2月23日に惣菜コーナー以外は解消)、3月7日に予定されていたゆめマート新店舗の開店も延期になる等の影響が出ています。

- IPAが1月に発表した2023年における「情報セキュリティ10大脅威」においても組織向け脅威の1位に「ランサムウェアの被害」が挙げられ(AUS便り 2024/01/24号参照)、2023年12月にも地方新聞社が感染によって紙面製作に影響が出る(同2023/12/27号参照)等、今も組織活動に深刻な影響をもたらし得るものであり、感染によるシステム・データの破壊から迅速に復旧できるよう、単にデータバックアップを行うのみならず、バックアップデータを保護する体制(複数のコピーをとりオフラインに保存する等)、バックアップから確実に復旧できる体制を確立することが肝要です。

ITmedia NEWS

地方スーパーにランサム攻撃、復旧は5月の見込み　メールシステムも停止、連絡手段は電話・ファクス・郵送のみに

2024年02月22日 20時31分 公開　[松浦立樹，ITmedia]

総合スーパー「ゆめタウン」を展開するイズミ（広島県広島市）は、社内システムがランサムウェア攻撃を受けたと発表した。2月22日現在も復旧しきれておらず、配達サービスや各店舗のチラシ配布など一部サービスを休止している。食品売り場でも一部品薄状態が続いているという。同社は「5月1日の完全復旧を目指す」と説明している。

総合スーパー「ゆめタウン」がランサムウェア被害に

ランサムウェア被害があったのは2月15日。システム障害が発生したため、原因を調べたところ、ランサムウェアによって複数のサーバが暗号化されていることが分かったという。22日時点では個人情報の漏えいは確認できておらず、調査を継続中。同社はクレジット払いサービス「ゆめカードクレジット」を提供しているが、被害に遭ったシステムとは別システムで運用しているため、カード情報は漏えいしていないとしている。

●中小企業のWordPress製Webサイトの多くで脆弱性…大阪商工会議所・立命館大学調査

https://j-net21.smrj.go.jp/news/j84vtt000000202e.html

このニュースをザックリ言うと・・・

- 2月5日(日本時間)、大阪商工会議所より、立命館大学との共同研究で実施した「中小企業等のホームページの脆弱性診断」における調査結果が発表されました。

- 2023年10月3日～11月10日にかけ、全国111社・192のWordPressを使用したWebサイトに対し調査したところ、66%で管理画面へのログインページおよびユーザーリストの双方が露出していたとのことです。

- 発表では、この状態にあることにより、ユーザーIDを取得した上でパスワードを推測しての不正ログインが試行され、改ざんや不正プログラム埋め込み等が行われる危険性があるとして、注意喚起を行っています。

AUS便りからの所感

- 発表では、WordPressサイトが不正アクセスを受け内容が改ざんされた事例として2023年9月の鹿児島王将を、また改ざんによるより具体的な被害の事例として、アクセスによりマルウェア「Emotet」がダウンロードされることを挙げています。

- WordPressにはログインページやユーザーページへのアクセスを困難にする、不正なログイン試行を遮断する等のセキュリティ機能を提供するプラグインが多く提供されているため、評判の高いものを選んで導入すること、本体から各種プラグインに至るまで頻繁に脆弱性が報告される傾向があるため、随時管理画面にアクセスし、更新機能によって最新に保つよう努めましょう。

The Osaka Chamber of Commerce and Industry
大阪商工会議所

記者配布資料
2024年1月30日

大阪経済記者クラブ会員各位

大阪商工会議所・立命館大学共同研究
「中小企業等のホームページ脆弱性診断」調査結果
ー定割合のホームページに改ざんや不正プログラム埋め込み等の危険性あり

〔お問合せ〕大阪商工会議所　経営情報センター（登坂、古川、野田、石田）
TEL:06-6944-6353

- 大阪商工会議所は、正しく安全なホームページの運用を促すことを目的に、立命館大学との共同研究調査として、**中小企業等のホームページの脆弱性診断を実施**した。日本国内で約８割のシェアを有する「WordPress」※1で作られたホームページを対象に調査を行った結果、**66%のURLに、改ざんや不正プログラム埋め込み等が行われる危険性（ユーザーリスト※2とログインページの双方が露出）**が見受けられた。
- この結果を受け、２月８日（木）に、**「ホームページ作成ツール『WordPress』注意喚起セミナー」を開催**する。同セミナーでは、診断結果から見えた中小企業のセキュリティに関する実態を報告するとともに、ホームページ設定の確認方法や対策ポイントを解説する。

＜調査概要＞
○背　景　：　2023 年 9 月に、鹿児島王将㈱のホームページが改ざんされ、実在する弁護士事務所の名で「破産手続きを開始した」などとする事実無根の表記がなされた。また、同年 12 月には、大阪商工会議所経営情報センターにも改ざんの相談が寄せられた。

●エレコム製Wi-Fiルータに脆弱性…ファームウェアのアップデートを

https://scan.netsecurity.ne.jp/article/2024/02/26/50629.html
https://www.elecom.co.jp/news/security/20240220-01/

このニュースをザックリ言うと・・・

- 2月20日(日本時間)、エレコム社より、同社製のWi-Fiルーターに脆弱性が報告されたと発表されました。

- 管理画面において、ログインしたユーザーにより機器上で任意のコマンドを実行される可能性、およびクロスサイトスクリプティング(XSS)やクロスサイトリクエストフォージェリ(CSRF)により、管理者の権限で任意のスクリプトを実行される可能性があり、不正な設定の実行に繋がる恐れがあります。

- 脆弱性が報告されたのはWRC-1167GS2-B・WRC-1167GS2H-B・WRC-2533GS2-B・WRC-2533GS2-W・WRC-2533GS2V-Bの5製品で、メーカーではいずれも販売終了状態となっていますが、ファームウェアのアップデートがリリースされており、適用が強く推奨されています。

AUS便りからの所感

- 機器の初期状態ではファームウェアが自動更新される設定となっていますが、設定の有効・無効に拘らず管理画面においてファームウェアのバージョンを確認することを推奨致します。

- 今回の対象機器は2019年9月～2022年1月に発売された比較的新しい機種のため、ファームウェアのアップデートが提供されていますが、2023年8月に同社製ルーターで脆弱性が発表された際は、2017年2月以前発売とその時点で6年以上経過した機種が対象だったため、アップデートが提供されず代替機器への切り替えが呼び掛けられた経緯があります(AUS便り2023/08/22号参照)。

- 組織内に設置した全てのネットワーク機器を管理する際は、メーカーサポート情報へも随時アクセスできる状態としておくこと、サポート終了時あるいは指定した期間での確実なリプレースが行えるよう準備しておくこと、加えて機器によっては品番が筐体から確認できず、脆弱性の対象となるかわかりにくい可能性も出てくることを鑑み、設置時点で品番・外見・設置場所等の情報を詳細に記録することが重要です。

ScanNetSecurity by IID

脆弱性と脅威／セキュリティホール・脆弱性

2024.2.26 Mon 8:00

エレコム製無線 LAN ルータに複数の脆弱性

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は2月20日、エレコム製無線 LAN ルータにおける複数の脆弱性について「Japan Vulnerability Notes（JVN）」で発表した。

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は2月20日、エレコム製無線 LAN ルータにおける複数の脆弱性について「Japan Vulnerability Notes（JVN）」で発表した。富士通株式会社の山口翔生氏と株式会社サイバーディフェンス研究所の永岡悟氏が報告を行っている。影響を受けるシステムは以下の通り。

WRC-1167GS2-B v1.67 およびそれ以前のバージョン
WRC-1167GS2H-B v1.67 およびそれ以前のバージョン
WRC-2533GS2-B v1.62 およびそれ以前のバージョン
WRC-2533GS2-W v1.62 およびそれ以前のバージョン
WRC-2533GS2V-B v1.62 およびそれ以前のバージョン