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。

●「ドメイン名の終活」に関する発表・資料…終了後のアクセス分析等も考慮を

https://www.itmedia.co.jp/news/articles/2411/13/news144.html
https://speakerdeck.com/mikit/domeinming-nozhong-huo-nituite-jpaawg-7th

このニュースをザックリ言うと･･･

- 11月12日、インターネット不正利用対策の研究者による「Japan Anti-Abuse Working Group(JPWAAG)」のミーティングにおいて、「ドメイン名の終活について」と題した発表が行われました。

- 発表では、「アクセスがそれなりにあるサイトのドメイン名」の廃止により、第三者に取得(ドロップキャッチ)され、フィッシングサイトに転用される等の恐れがあることから「ドメイン名の使い捨て、ダメ絶対」と呼び掛けるとともに、対策としての「終活」を取り上げています。

- 発表資料では、企業組織等既存のドメイン名下ではない、独自のドメイン名の登録で発生するコスト(費用・手間)と、サービスが終了したドメイン名を一定期間休眠の上で廃止させる段取りについてまとめられています。

AUS便りからの所感等

- ドメイン名の廃止までにかかる費用面のコストとして、ドメイン名自体の更新費用のみならず、DNSサーバー・Webサーバー(リダイレクトやお知らせページのため)やWebサイト証明書の更新費用についても言及されています(証明書についてはLet's Encrypt等無償のサービスへ移行することを提案しています)。

- 他にも、サーチエンジンに表示されないようにする「逆SEO」、外部リンクからのアクセスやDNSクエリが続いているか等のログの分析、メールについても送信あるいは受信を行わないことを示すSPF・DMARC・MX各レコードの設定等の考慮する面があるとしています。

- ドロップキャッチが話題となった事例はサービス終了から長くても3年程で失効し、終了時点でドメイン名の自動更新を取りやめたとみられるケースが多く見受けられ、当AUS便りでは終了後10年程度はドメイン名を保持することを度々推奨していますが、発表で挙げられた以外で、例えばサブドメインであっても、使われなくなったDNSレコードの参照先が第三者に悪用される等の問題が起こり得ることを鑑み、終了したサービスについても完全な廃止まで一貫した管理体制をとることが重要と言えます。

ITmedia NEWS

ドメイン名にも"終活"が必要？　休眠・廃止方法の解説資料が話題　「ドメイン名の使い捨て、ダメ絶対」

2024年11月13日 13時43分 公開　[ITmedia]

DNSについての情報発信などをする団体・日本DNSオペレーターズグループが11月12日に公開した、ドメイン名の"終活"について解説する資料が、Xやはてなブックマークなどで話題を呼んでいる。資料では、ドメイン名の安易な廃止にはリスクが伴うとして、適切な休眠や廃止の方法を紹介。「全エンジニアが読んでおくべき」「ドメインは取得するより手放す方が大変だと常々思っていた」などの声が上がっている。

ドメイン名の"終活"に関する資料がXなどで話題（画像は資料より、以下同）

資料ではまず、アクセスがあるサイトのドメイン名を安易に廃止した際のリスクを紹介。ドメイン名がオークションで取引され、悪意ある第三者の手に渡ると、フィッシングなどの詐欺サイトに使われる。同団体は「ドメイン名の使い捨て、ダメ絶対」と注意を呼び掛けた。新たなドメイン名を登録する際も、本当に必要か一考してほしいという。

●薬局チェーンのECサイト、サポート詐欺による不正アクセスでのべ40,736人分の個人情報流出

https://www.itmedia.co.jp/news/articles/2411/08/news186.html
https://www.welcia-yakkyoku.co.jp/wp-content/uploads/2024/11/info_241108.pdf
https://www.e-welcia.com/news/detail/38

このニュースをザックリ言うと･･･

- 11月8日(日本時間)、大手薬局チェーンのウエルシア薬局(以下・同社)より、同社のECサイト「ウエルシアドットコム」に関連する個人情報が不正アクセスで流出したと発表されました。

- 被害を受けた個人情報は、ウエルシアドットコムの利用者(退会者含む)39,805名分(氏名・住所・電話番号・生年月日・性別・アカウント情報および購入商品)と、同社およびグループ企業の従業員931名分(氏名・所属組織・メールアドレス)とされています。

- 10月24日、同社従業員がサポート詐欺の誘導により遠隔操作ソフトをインストールしたことにより、外部から不正アクセスを受けたとされています。

AUS便りからの所感

- 同社では、対象となった利用者に対し個別に連絡をとり、パスワードの変更を呼び掛けています。

- サポート詐欺へ誘導しようとする不審な画面の表示は、大手新聞社等普通のWebサイトへのアクセスでも広告を通して発生するケースが報告されており(AUS便り 2024/07/25号参照)、いつどこで遭遇してもおかしくないものと心得、IPAが公開している特集ページ(https://www.ipa.go.jp/security/anshin/measures/fakealert.html)等を参考に慎重に行動できるよう用意しておくことが望ましいでしょう。

ITmedia NEWS

「ウエルシアドットコム」から約4万人分の個人情報漏えいのおそれ　従業員がサポート詐欺に

2024年11月10日 08時50分 公開　[ITmedia]

ウエルシア薬局（東京都千代田区）は11月8日、外部からの不正アクセスにより個人情報が漏えいしたおそれがあると発表した。公式通販サイト「ウエルシアドットコム」に携わる従業員がサポート詐欺に遭った。

10月24日に従業員がサポート詐欺のWebサイトに誘導され、遠隔操作ソフトをインストールさせられたことで不正アクセスを受けた。これにより、ウエルシアドットコム利用者3万9805人分の個人情報や、ウエルシア薬局グループ社員931人分の情報が漏えいしたおそれがある。

● Microsoft・Adobe・Zoom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/1638950.html
https://msrc.microsoft.com/blog/2024/11/202411-security-update/
https://forest.watch.impress.co.jp/docs/news/1638948.html
https://forest.watch.impress.co.jp/docs/news/1639278.html

このニュースをザックリ言うと･･･

- 11月14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月例のセキュリティアップデートがリリースされています。

- WindowsのバージョンはWindows 10 22H2 KB5046613(ビルド 19045.5131)、11 23H2 KB5046633(ビルド 22631.4460)および11 24H2 KB5046617(ビルド 26100.2314)等となります。

- 同日にはAdobe社より「Photoshop」「Illustrator」等8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。

- またZoom社からも「Zoom」クライアントに複数の脆弱性が存在し、最新バージョン6.2.7での修正が発表されています。

AUS便りからの所感

- MSの月例アップデートでは、Exchange Server・Active Directory 証明書サービス等4件の脆弱性が既に悪用を確認、これと別に3件の脆弱性が特に危険度が高いと評価されています。

- Zoomクライアントについては月例以外でも頻繁にアップデートがリリースされますが、自動更新を有効に設定していても起動していない間にはアップデートが適用されず、特に使用頻度が少ない場合等に「会議の直前でアップデートが発生する」というトラブルも散見され、可能な限りトラブルを回避するよう随時クライアントを起動し、明示的に「アップデートを確認」を開くことを心掛ける必要があるでしょう。

- 各社のセキュリティアップデートが集中する「パッチチューズデー(米国時間での第2火曜日)」において根本的対策としてパッチの適用を必ず行うことを前提とし、社内における パッチの展開・適用完了までに発生し得る攻撃に対しアンチウイルス・UTM等による防衛を怠りなく実施することが肝要です。

Impress Watch

致命的な脆弱性4件、ゼロデイ攻撃も ～Microsoft、2024年11月セキュリティ更新を公開

「Windows Server 2025」に初のセキュリティアップデート

樽井 秀人　2024年11月13日 09:40

2024年11月のセキュリティ更新プログラム

米Microsoftは11月12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89件（サードパーティーのものも含めれば92件）の脆弱性が新たに対処されている。