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。

● WordPress不正アクセスでLPサイト改ざん、SaaSへの移行発表で一時Twitterトレンドに

https://www.itmedia.co.jp/news/articles/2306/06/news106.html

このニュースをザックリ言うと･･･

- 6月1日(日本時間)、「バズレシピ」で知られる料理研究家のリュウジ氏より、同氏が監修した食品のランディングページ(宣伝ページ、LP)が改ざんされていたと発表されました。

- LPで使用していたWordPressへの不正アクセスにより、悪意のあるサイトへのリダイレクトが仕掛けられたとされ、同氏は対策として「今後はWordPressは使用せずにセキュリティの高いBASE(ネットショップ提供サービス)を使用する」とTwitter上で発表しています。

- この発表についてTwitterでは、WordPressと、BASEのようなSaaSとのセキュリティの差に関する議論が発生し、一時「WordPress」がトレンドワードになる程の話題となっています。

AUS便りからの所感等

- 後日リュウジ氏もこの議論を受け、「(WordPressでは)扱いが難しい」「サービスが徹底している方に移行する」という趣旨だったとコメントしています。

- WordPressのみならず、ソフトウェアをサーバーに導入する形のCMS(コンテンツ管理システム)では、単にページを立ち上げるだけで後は放置できるようなものではなく、Webサイトを公開し続ける場合、自前で面倒を見るか、管理業者に任せるかに拘らず、その後もソフトウェアを最新に保つ等セキュリティ面を含めた管理を徹底することが必要となり、SaaSと契約してのサイト運営はソフトウェア管理等をサービス提供者に概ね一任できる点で有用と言えます。

- SaaSの利用に費用がかかるからとはいえ、WordPressを利用する形でWebサイトを公開し続ける場合は最低限セキュリティを強化するプラグインのインストール等が不可欠、一方でLPのようなシンプルなコンテンツについては静的HTMLでの公開も有用ながら、その場合にはファイルアップロード用はじめサーバーにログイン可能なアカウントについて管理の考慮が必要、加えていずれにおいてもIDS・IPS・WAF等のソリューション導入も検討すべきと、それぞれの運用形式においてとるべきセキュリティ対策は様々なれど、必要なコストを払うことを決して怠らないことが肝要です。

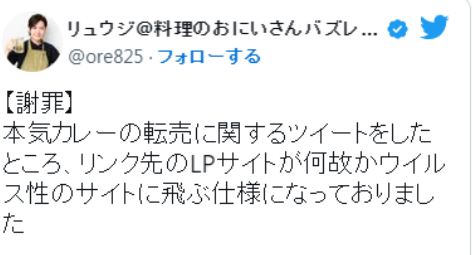
ITmedia NEWS

WordPressは低セキュリティ？　“バズレシピ”リュウジ氏のBASE移転で議論に

2023年06月06日 10時49分 公開　[岡田有花，ITmedia]

人気料理YouTuber・リュウジ氏監修の食品を販売するサイトが不正アクセスにより改ざんされ、ウイルスを含むサイトにリダイレクトされていた問題をめぐり、WordPressのセキュリティが議論になっている。

リュウジ氏は「ランディングページのWordPressがハックされたので、よりセキュリティが高いBASEに移行した」と告知したのだが、「WordPressも適切に運用すればセキュリティは高い」などの反論が、ITに詳しい一部のフォロワーから届いていた。



● VPNパスワードを推測され侵入、ランサムウェアによるデータ暗号化

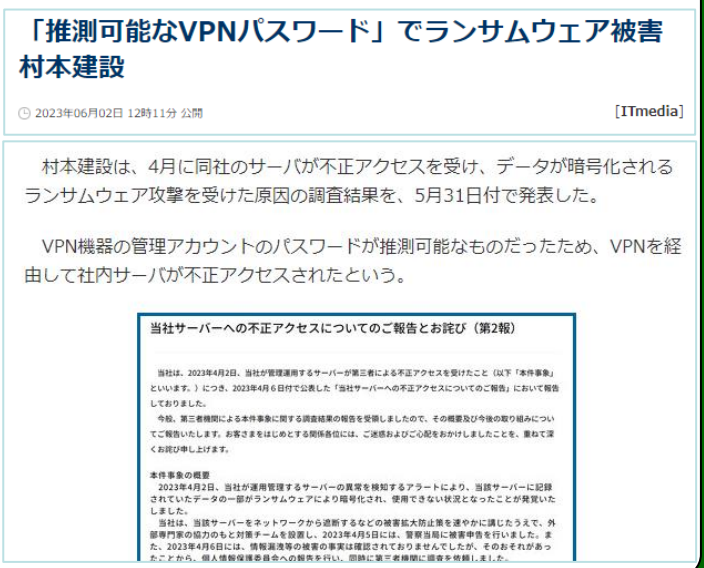
https://www.itmedia.co.jp/news/articles/2306/02/news116.html

このニュースをザックリ言うと･･･

- 4月6日(日本時間)、村本建設より、同2日に同社が運営管理するサーバーが不正アクセスを受けたため、ネットワークから遮断したことが発表されました。
- 5月31日、同社より続報が発表され、サーバー上のデータの一部がランサムウェアによるデータ暗号化攻撃を受け、使用できない状況となったことが明らかになっています。
- また、不正アクセスの原因は、VPN機器の管理アカウントに設定されたパスワードが推測可能なものだったためとされています。

AUS便りからの所感

- VPNを経由しての不正アクセス・社内LANへの侵入については、近年ファームウェアが更新されていない機器の脆弱性を突かれるケースも多く報告されており、片やルーター・NASや各種IoT機器において管理用パスワードが簡単なものはおろか、デフォルトのものから変更していなかったために侵入されたケースもまた昔から多く存在します。
- 6月6日には製薬会社のエーザイからもサーバーがランサムウェアに感染したと発表されており、ランサムウェアに限らずあらゆるサイバー攻撃のターゲットになること、また被害が発生してしまうことは、組織の大小に限らず発生し得ると心得、サーバーOSからIoT機器のファームウェアまで最新に保つとともに、管理者はもちろんユーザーに発行するアカウントに至るまで十分に強固なパスワードを設定することが重要です。



「推測可能なVPNパスワード」でランサムウェア被害 村本建設

2023年06月02日 12時11分 公開 [ITmedia]

村本建設は、4月に同社のサーバが不正アクセスを受け、データが暗号化されるランサムウェア攻撃を受けた原因の調査結果を、5月31日付で発表した。

VPN機器の管理アカウントのパスワードが推測可能なものだったため、VPNを経由して社内サーバが不正アクセスされたという。

当社サーバーへの不正アクセスについてのご報告とお詫び（第2報）

当社は、2023年4月2日、当社が管理運用するサーバーが第三者による不正アクセスを受けたこと（以下「本件事象」といいます。）につき、2023年4月6日付で公表した「当社サーバーへの不正アクセスについてのご報告」において報告しておりました。

今般、第三者機関による本件事象に関する調査結果の報告を受領しましたので、その概要及び今後の取り組みについてご報告いたします。お客さまをはじめとする関係各位には、ご迷惑およびご心配をおかけしましたことを、重ねて深くお詫び申しあげます。

本件事象の概要

2023年4月2日、当社が運用管理するサーバーの異常を検知するアラートにより、当該サーバーに記録されていたデータの一部がランサムウェアにより暗号化され、使用できない状況となったことが発覚いたしました。

当社は、当該サーバーをネットワークから遮断するなどの被害拡大防止策を速やかに講じたうえで、外部専門家の協力のもと対策チームを設置し、2023年4月5日には、警察当局に被害申告を行いました。また、2023年4月6日には、情報漏洩等の被害の事実は確認されておりませんでしたが、そのおそれがあったことから、個人情報保護委員会への報告を行い、同時に第三者機関に調査を依頼しました。

●5月度フィッシング報告件数は113,789件、過去最多を更新

https://www.antiphishing.jp/report/monthly/202305.html

このニュースをザックリ言うと･･･

- 6月6日(日本時間)、フィッシング対策協議会より、5月に寄せられたフィッシング報告状況が発表されました。
- 5月度の報告件数は113,789件で、4月度(https://www.antiphishing.jp/report/monthly/202304.html)の92,932件から20,857件増加、2022年9月度以外の10万件越えかつ過去最多を更新しています。
- 5月度ではファミペイが最も多く悪用されたブランドとなり(全体の21.5%)、以下それぞれ1万件以上の報告があったセゾンカード・Amazon・イオンカードを含む4ブランドで全体の約60.0%、また1,000件以上の報告があった18ブランドで全体の約89.1%を占めたとしています。
- 同協議会の調査用メールアドレスへ配信されたフィッシングメールの約94.6%が中国のISPからの配信(4月度約88.3%)とされ、また約99.0%がDNS逆引き設定がされていないIPアドレスからの送信(4月度約96.5%)となったとのことです。

AUS便りからの所感

- フィッシングサイトのURL件数は18,991件で4月度(21,230件)から2,239件減少していますが、4月まで多かった短縮URLやCDN事業者のサービスを悪用したものが減少し、同一URLの使い回しが増えたためと分析しています。
- Amazonを騙るフィッシングの報告数や割合が減少した(それでも割合としては3位に入っています)ことについては、同社からの正規のメールであることを視認できる各種機構に対応し、国内大手メールサービスでもフィッシングメールを見分けやすくなったことが要因としており、悪用するブランドとしてこういった機構に対応していないサービスに移行するケースがみられているようです。
- 6月に入ってからも同協議会からはエムアイカードを騙るフィッシングなどへ注意喚起が出され、また特に発表はないものの手元ではクロネコヤマトのサービス変更に便乗したとみられるフィッシングメールが目立っています。
- 発表においては「事業者のみなさまへ」および「利用者のみなさまへ」と題し、それぞれがとるべき対策法・採用すべき機構についてまとめられていますが、前者ではDMARCを単に採用するのみならずレポートの分析をもとにより厳格なポリシーの設定を推奨、後者ではフィッシング対策機能が強化されているメールサービスの利用等を呼び掛けており、システム管理者から一般のユーザーに至るまで是非とも目を通し、実行可能な対策を検討して頂ければ幸いです。

フィッシング対策協議会 Council of Anti-Phishing Japan