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。

●WindowsのWi-Fi機能に脆弱性、PC乗っ取りの恐れ…月例アップデート適用の確認を

https://www.gizmodo.jp/2024/06/wi-fi-vulnerability-in-windows.html
https://www.forbes.com/sites/daveywinder/2024/06/14/new-wi-fi-takeover-attack-all-windows-users-warned-to-update-now/
https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2024-30078

このニュースをザックリ言うと･･･

- 6月20日(現地時間)、ネットメディア「GIZMODO」より、WindowsのWi-Fi機能における脆弱性(CVE-2024-30078)について注意を喚起する記事が掲載されています。

- 記事によれば、未対策のPCと同じWi-Fiネットワーク上に攻撃者がいる場合、リンクを送ったりメールを開かせるようなことなしに、細工したパケットを送信するだけでPCが乗っ取られ、マルウェア感染をも引き起こされる等の恐れがあるとしています。

- 脆弱性は6月12日(日本時間)にマイクロソフト(以下・MS)から月例アップデートでの修正が発表されていたもので、MSでは特に頻繁にパブリックWi-Fiを利用するユーザーに対して、アップデートを適用するよう注意喚起しています。

AUS便りからの所感等

- この一週間前、6月14日にForbesからも当該脆弱性に関する記事が発表されており、GIZMODOもその記事を参照しています。

- いわゆる公衆Wi-Fi、特に無料で提供されたり、暗号化キーが設定されていないものは盗聴の危険性が従来から指摘されていました(これについてはHTTPS等TLS暗号化通信の利用が一般的になり概ねリスクはカバーされています)が、盗聴のみならず脆弱性を持った機器を狙う攻撃者も潜んでいる可能性を常にはらんでいることに注意が必要です。

- 脆弱性の特性上、外部インターネットから直接攻撃される類のものではありませんが、社外に頻繁にPCを持ち出すケースはもちろん、社内に何らかの手口で攻撃者が侵入し社内Wi-Fiに接続するケースにも警戒(別途UTM等のソリューションによる防御も推奨)するため、また他にも多くの脆弱性が修正されていることから、Windows Updateを必ず実行し、OSを最新の状態に保つことが重要です。

GIZMODO

Wi-Fiに関する脆弱性発覚。全Windowsユーザーは今すぐアップデートを

2024.06.25 14:00 ⚡ 58,216
Dua Rashid - Gizmodo US［原文］（mayumine）

今すぐアップデートするか、パブリックWi-Fiには絶対に繋がないようにするか。

Microsoft（マイクロソフト）は、Windowsに新たに「深刻度が重要」なWi-Fiに関する脆弱性を確認しました。この脆弱性が悪用されると、ハッカーは同じWi-Fi-ネットワーク上にいるだけで、**Windowsデバイスを則りマルウェアに感染させる**ことが可能になります。Microsoftは、特に頻繁に**パブリックWi-Fiを利用するユーザー**に対して、今すぐにWindows PCをアップデートするように勧告しています。

●委託先社員が私物HDDを業務利用、情報削除せず廃棄…個人情報流出の可能性

https://www.itmedia.co.jp/news/articles/2406/14/news130.html
https://www.bandaispirits.co.jp/press/2024/240611.php

このニュースをザックリ言うと・・・

- 6月11日(日本時間)、BANDAI SPIRITS社より、同社運営のバンダイグループ公式通販サイト「プレミアムバンダイ」会員の個人情報が外部に漏洩した可能性があると発表されました。
- 対象となるのは、2012年11月実施のキャンペーン参加者233件のメールアドレス、および2013年11月18日に出荷した会員1,951件の住所・氏名・電話番号とされています。
- 同サイトに関する開発保守支援等の業務委託先従業員が私物の外付けHDDを業務に使用し、当該情報を保存後削除せずに廃棄しており、そのHDDを入手した第三者から連絡を受けたことで発覚したとのことです。
- サイトへのログインパスワードやクレジットカード番号は含まれておらず、またダークウェブ等のモニタリングにおいて当該情報が実際に流出したことは確認されていないとのことです。

AUS便りからの所感

- 過去には個人情報の売却を目的としてスマートフォンのUSB接続により大規模な情報持ち出しが行われたベネッセの事例、日経新聞社元社員が別社員の業務用PCを分解してHDDを抜き取った事例(AUS便り 2018/07/09号参照)、またセキュリティ大手のLAC社元社員が業務上のビジネス文書を保存した私物HDDを売却し、購入した第三者から通報を受けたという事例(同 2022/01/25号参照)等があります。
- 他にも機密情報を保存した媒体が紛失する事案は現在に至るまでUSBメモリーや外付けHDD・SSD等で度々発生しています。
- 委託先も含め不必要に外部媒体に情報を保存されないようなソリューションの導入、第三者へのデータ漏洩を防ぐための暗号化の徹底(適切に運用されれば安全に媒体を廃棄することも期待できます)、また外付け・内蔵に拘らず媒体の確実な物理的破壊による廃棄(SSDについては破壊が不十分だったためにデータが取り出された事例もあります)等、情報漏洩を防止するための多角的な対策の検討・採択を強く推奨致します。

ITmedia NEWS

委託先が私物HDD使用、データ削除せず廃棄　「プレミアムバンダイ」顧客情報漏えいの可能性

2024年06月14日 12時32分 公開　[ITmedia]

通販サイト「プレミアムバンダイ」を運営するBANDAI SPIRITSは、業務委託先が保存していた会員の個人情報が漏えいした可能性があると6月11日に発表した。委託先社員が私物の外付けHDDを業務に利用し、データを削除せずに廃棄したため。このHDDを入手した人からの連絡で発覚した。

ダークウェブなどのモニタリングを行っているが、個人情報が外部へ流出した事実は確認できず「データが外部へ漏えいした可能性は極めて低い」とみている。

● 5月のフィッシング報告件数は143,680件、先月度より急増

https://www.antiphishing.jp/report/monthly/202405.html

このニュースをザックリ言うと・・・

- 6月21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143,680件で、4月度(https://www.antiphishing.jp/report/monthly/202404.html)の106,757件から36,923件増加しています。
- フィッシングサイトのURL件数は38,089件で4月度(39,863件)から1,774件減少、悪用されたブランド件数も91件で4月度(92件)から1件減少となっています。
- 最も多く報告されたのはAmazonを騙るフィッシングで報告数全体に対する約31.3%、次いで報告が多かった東京電力、三井住友カード、イオンカード、エポスカードと合わせて約73.6%、さらに1,000件以上報告された16ブランドまで含めると約94.0%を占めたとのことです。

AUS便りからの所感

- 報告件数は、2023年10月の156,804件、同6月の149,714件に続く歴代3位を記録しており、6月度については記録を更新する可能性も十分に考えられます。
- フィッシングサイトURLで使用されるTLD(トップレベルドメイン名)の割合は上位から .com(約55.4%)、.cn(約16.1%)、.dev(約8.0%)、.ru(約5.7%)等となっており、.com、.cnおよび.devが増加しているとのことです。
- Gmailが@gmail.com(および @googlemail.com)宛にメールを送信する相手にSPF・DKIM・DMARCの設定等のメールセキュリティ要件を満たすよう要請する「メール送信者のガイドライン(https://support.google.com/a/answer/81126?hl=ja)」に基づき、要件を満たしていない送信元からのメールが迷惑メール扱いされたり、受信されなくなったりすることが今後考えられ、相手がGmail等に限らず、取引相手が自組織になりすましたフィッシング等の被害を受けることのないよう、前述した各種なりすまし対策技術の導入を確実に行うことが肝要です。

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