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。

●任天堂を騙るフィッシングメールに注意喚起、アカウント不正ログインの恐れも

https://www.itmedia.co.jp/news/articles/2410/29/news143.html
https://www.itmedia.co.jp/news/articles/2409/27/news196.html
https://support.nintendo.com/jp/information/2024/1029.html

このニュースをザックリ言うと･･･

- 10月29日(日本時間)、任天堂より、同社メールアドレス(no-reply@accounts.nintendo.com等)を使用するなりすましメールが確認されているとして注意喚起が出されています。

- 同社では、なりすましメール中に記載されたリンク(URL)は詐欺サイトの可能性があるとして、リンクをクリックせず、すぐにメールを削除するよう呼び掛けています。

- ただし、no-reply@accounts.nintendo.comからのメールを一律で受信拒否した場合、ニンテンドーアカウントの認証コード通知等、同社からの正規のメールも受信できなくなる可能性があることにも注意するよう呼び掛けています。

- 注意喚起を取り上げたITMediaからも、詐欺サイトにアクセスし、ニンテンドーアカウントの情報を入力してしまった場合、不正ログインされる恐れがあり、速やかにパスワードを変更する必要があると警告しています。

AUS便りからの所感等

- 同社は9月27日にもX(旧・Twitter)において同様の警告を行っています。

- 10月30日現在、@accounts.nintendo.comあるいは@nintendo.comについてはSPF・DMARCが設定済みであり(ただし@nintendo.comの方のDMARCはp=noneとなっています)、メール受信側でこれら(およびDKIM)による正当性のチェックを行うことにより、フィッシングメールは効果的に回避できるでしょう。

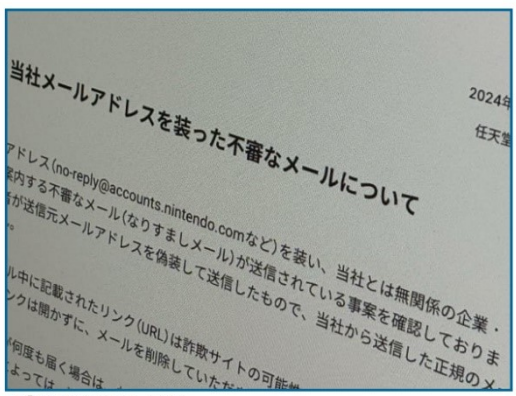
- 一方で、本物のサービスと全く関係のない、SPF・DKIM・DMARCのチェックを通過するよう設定したドメイン名で迷惑メールを送信するケースも以前から常態化しており、メールサーバー・UTMおよびPC上でのメーラーやアンチウイルスソフトにおいて、件名・文面の内容から迷惑メールか否かをチェックする機構も怠りなく有効化することが肝要です。

ITmedia NEWS

任天堂、なりすましメールに改めて注意喚起　対応を誤ると不正ログインされる可能性も

2024年10月29日 13時49分 公開　[ITmedia]

任天堂は10月29日、実在する同社のメールアドレスを装い、無関係の企業やサービスについて案内する不審なメールが確認されたとして注意喚起した。9月末に任天堂サポートの公式Xアカウントも同様の告知をしていた。



(出典：任天堂のWebサイト、以下同)

確認されたのは「ニンテンドーアカウント」に関する連絡に使用している「no-reply@accounts.nintendo.com」などを装ったメール。不審なメールからリンクされているURLは詐欺サイトの可能性があり、任天堂は開かずにメールを削除することを求めている。誤ってリンクを開いてしまった場合はWebブラウザ自体を閉じる。

●「FortiManager」にゼロデイの脆弱性、セキュリティアップデート適用を

https://www.itmedia.co.jp/news/articles/2410/24/news150.html
https://www.fortiguard.com/psirt/FG-IR-24-423
https://www.bleepingcomputer.com/news/security/fortinet-warns-of-new-critical-fortimanager-flaw-used-in-zero-day-attacks/

このニュースをザックリ言うと･･･

- 10月23日(現地時間)、米Fortinet社より、同社製品「FortiManager」「FortiManager Cloud」の脆弱性「CVE-2024-47575」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。
- 脆弱性の悪用により、外部の攻撃者にFortiManager等を乗っ取られる恐れがあり、バージョン6.2.13・6.4.15・7.0.13・7.2.8・7.4.5・7.6.1で対策されている他、回避策が提示されています。
- 米IT系メディアBleeping Computerによれば、アップデートリリース前の10月13日に顧客に対する通知がありましたが、さらにそれより前に脆弱性の悪用が一部で報告されていた(いわゆる「ゼロデイ脆弱性」である)としています。

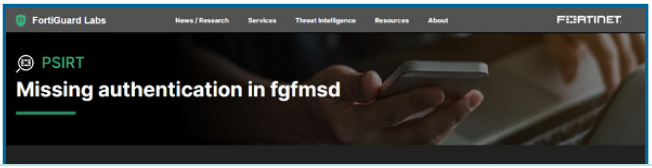
AUS便りからの所感

- FortiManagerはFortinet社製の各種製品を集中管理するためのアプライアンスです。
- 同社製品では、UTM「FortiGate」等でVPN関連機能に脆弱性が度々報告され、組織内ネットワークへ侵入される事案も頻発しています。
- 一般的な話になりますが、サーバー以外でもあらゆるネットワーク機器について、根本的な対策としてファームウェア等を最新バージョンに保つとともに、機器やそのサービスポート等へ不特定多数からアクセスされないよう可能な限りフィルタリング設定をかけることが重要です。

Fortinet、悪用されたFortiManagerのゼロデイ脆弱性について公表

2024年10月24日 14時30分 公開 [ITmedia]

米サイバーセキュリティ企業のFortinetは10月23日（現地時間）、同社の「FortiManager」に存在する重大な脆弱性「CVE-2024-47575」について公表した。この脆弱性は、悪意のある攻撃者が認証なしにFortiManagerにアクセスし、任意のコードを実行することを可能にするもので、既に悪用された形跡が見つかっている。



●シャープECサイトで7月発生の不正アクセス…のべ5,836人の個人情報・カード情報流出か

https://japan.cnet.com/article/35225521/
https://corporate.jp.sharp/info/notices/241030-a.html

このニュースをザックリ言うと･･･

- 10月30日(日本時間)、シャープ社より、同社オンラインストア「COCORO STORE」および食材宅配サービス「ヘルシオデリ」が不正アクセスを受け、クレジットカード情報を含むサイト利用者の個人情報が流出していたと発表されました。
- 第一報が7月29日に発表されており、6月30日にCOCORO STORE、同23日～30日にヘルシオデリで注文を行った203人分の個人情報(氏名・住所・電話番号・メールアドレス等の注文情報)が流出した可能性があるとされていました(これについてクレジットカード情報は含まれていないとのことです)。
- 10月30日の発表では、さらに7月19日～22日にCOCORO STOREで注文を行ったユーザー5,633人分の個人情報(氏名・住所・電話番号・メールアドレスおよびパスワード)、うち4,257人分はクレジットカード情報(名義人名・番号・有効期限・セキュリティコード)も流出したとされています。

AUS便りからの所感

- それぞれのサイトでソフトウェアの脆弱性を悪用され、入力されたカード情報・個人情報を窃取するプログラムが埋め込まれたのが原因としており、近年度々発生しているセキュリティコードも含めたカード情報流出事案での主要な手口となっています。
- ECサイト構築で利用される有名なフレームワークにおいて、SQLインジェクションの脆弱性が発見され、セキュリティアップデートが修正されたにも拘らず、それが適用されない状態のECサイトが攻撃を受けるケースも度々報告されています。
- 攻撃者による侵入や改ざんの余地をなくすため、Webアプリケーション・フレームワークからサーバーに至るまで最新のバージョンに保ち脆弱性の修正・対策を確実に行うよう心掛けるとともに、攻撃の形跡・兆候を検知・遮断するためのIDS・IPSおよびWAFの設置を行うことも検討するようにしてください。

CNET Japan

7月のシャープ「COCORO STORE」不正アクセス、クレカ情報流出の可能性は4257人

CNET Japan Staff 2024年10月30日 13時00分

シャープは10月30日、7月29日に公表した公式オンラインストア「COCORO STORE」・食材宅配サービス「ヘルシオデリ」における不正アクセスについての調査結果を発表した。

個人情報流出の可能性がある顧客は、7月29日に公表した影響を受けた可能性のある最大約10万人のうち5836人。そのうち4257人は、クレジットカード情報を含む個人情報が流出した可能性がある。対象者には、電子メールと書状であらためて個別に連絡したという。