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。

●地方議会の情報システムにサイバー攻撃…90以上の議会に一時影響

https://www.sankei.com/article/20230413-CFJZJIX4ABNBFIDB3OMSE7W4TE/
https://www.futureinn.co.jp/solution/1000009/1000219/1001408.html

このニュースをザックリ言うと･･･

- 4月13日(日本時間)、国内メディア各社より、全国地方自治体の議会向け情報システムが不正アクセスを受けたと報じられました。
- 報道によれば、横浜市・広島市・滋賀県等全国90以上の地方議会において、インターネット議会中継・議事録検索等一部サービスが停止したとのことです。
- 翌14日、当該システムを運営する名古屋市内の業者からも、同11日に不正アクセスによるサーバーへの侵入を受けたことが正式に発表され、一時議会用サーバー8台全てを停止させる事態になったとのことですが、システムからの情報漏洩は確認されていないとしています。

AUS便りからの所感等

- 運営業者からの発表では、4月11日にID・パスワードの総当たり攻撃が確認され、一部のサーバーへ侵入されたとのことですが、同14日には対策を完了、一時停止したサービスは順次再開しており、他のサービスへの影響はみられなかったとしています。
- サービスの不正アクセスにより、利用している多数の組織に影響が出た事例としては、2021年に発生した富士通製プロジェクト情報管理ツール「ProjectWEB」への不正アクセスが挙げられ、このときは129のユーザー組織が内部情報・個人情報流出の被害を受けました。
- アカウント情報の総当たり攻撃はきわめて古典的な攻撃ながら、脆弱なパスワードが設定されたアカウントや攻撃への十分な対策を行っていないシステムでは現実的に侵入に繋がる恐れが強く、また企業Webサイトで WordPress等を使っている場合ログイン画面がどこにあるかも容易に推測可能な場合があるため、推測されにくい強力なパスワードを設定することはもちろん、特定IPアドレスからの不自然に多数のアクセス試行が行われた場合に遮断する、あるいは可能であれば多要素認証(MFA)を要求する等、ログイン機構を防御する各種機能を導入することが肝要です。

THE SANKEI NEWS

地方議会にシステム障害　９０以上、サイバー攻撃で

2023/4/13 19:56

社会 | 事件・疑惑　政治 | 地方自治

みんなの反応

インターネット中継の停止を知らせるメッセージ（左下）が表示された横浜市議会のウェブサイト＝１３日

横浜市や広島市、滋賀県など全国９０以上の地方議会の情報システムがサイバー攻撃を受け、インターネット議会中継や議事録検索などのサービスを停止したことが１３日、横浜市などへの取材で分かった。システムの運営を担う名古屋市のＩＴ企業のサーバーが、攻撃によって障害を起こした。個人情報の流出は確認していないとしている。

障害を起こした地方議会の情報システムは、名古屋市のフューチャーインが運営。同社は「対策を取り、１４日午後に復旧する予定だ」と説明している。

●「強制BCCシステム」がライセンス期限切れで機能せず…メールアドレス652件流出

https://xtech.nikkei.com/atcl/nxt/column/18/00598/021000210/
https://www.city.toyota.aichi.jp/pressrelease/1053884/1053940.html
https://www.city.toyota.aichi.jp/pressrelease/1053884/1053944.html
https://www.himawari.co.jp/news/info/ct5002/

このニュースをザックリ言うと･･･

- 4月4日(日本時間)、愛知県豊田市より、メール送信システムの問題により、メールアドレスが他者に流出する事象が発生していたと発表されました。

- 4月1日から同4日にかけて送信された24通のメールにおいて、計652件のメールアドレスが「To:」「Cc:」ヘッダーに含まれた状態で送信されたとのことです。

- 同市ではメール送信時に「To:」「Cc:」に含まれたメールアドレスを削除する「強制BCCシステム」を導入していましたが、これを提供していた同市内の運営業者が、システムの稼働に必要なソフトウェアのライセンス更新を怠ったため、一時的に作動しない状態となったとしています。

AUS便りからの所感

日経 XTECH

個人情報の流出原因は外部サービスのライセンス更新忘れ、愛知県豊田市で発生

piyokango　セキュリティーリサーチャー

2023.04.18

豊田市は「強制BCCシステム」の停止によりトラブルが発生したと説明。強制BCCシステムとは、複数の人に同時に配信する同報メールにおいて、宛先のメールアドレスが「TO」もしくは「CC」に入っていた場合に、そのメールアドレスを「BCC」に変更するシステム。メールの受信者はBCCに設定されたメールアドレスを確認できない。

トラブルの調査結果は4月5日に発表された。TOもしくはCCにメールが入ったまま同報メールが送られたのは2023年4月1日午後6時9分～4月4日午後4時56分までの約3日間で、この間は強制BCCシステムが停止していたという。対象となる同報メールは24通で、他の受信者に確認できるようになっていたメールアドレスは合計で652件。

- AUS便りでは、「To:」「Cc:」ヘッダーに誤ってメールアドレスが記入されることによる流出の事例を度々取り上げ、人間のチェックだけではなくシステム面での解決を呼び掛けていましたが、今回はシステム提供者側での運用上の見落としでシステムが適切に稼働せず、ユーザーの情報漏洩に繋がるというまた別の問題が発生しています。

- 近しい事例として、2022年9月には、顧客の個人情報を保存していたサーバーの契約終了時にデータを移行し忘れたため、個人情報が削除されたという事象が発表されています(AUS便り 2022/09/06号参照)。

- 運営業者では、ライセンス有効期限の管理と期限に関するアラートの導入およびテストメール送信による稼働状態の確認を行うとしており、多重の対策によるトラブルの防止の余地がないかは適宜考慮すべきでしょう。

- 一方の豊田市でも「To:」「Cc:」ではなく「Bcc:」にアドレスを入力するよう徹底することを防止策に挙げていますが、メーラーにチェック用のアドオンを導入する、あるいはメーラーを使わない配信システムを構築する、等も是非とも検討してほしいところです。

●MSとAdobeがセキュリティアップデートリリース、Oracleもリリース予定

https://www.jpcert.or.jp/at/2023/at230007.html
https://helpx.adobe.com/security.html
https://www.oracle.com/security-alerts/

このニュースをザックリ言うと･･･

- 4月12日(日本時間)、マイクロソフト(以下・MS)より、Windows等の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。

- 特にWindows共通ログファイルシステムのドライバーの脆弱性(CVE-2023-28252)について、リリースによる修正の前からランサムウェア攻撃への悪用が確認されているとして、同社やJPCERT/CC等より、速やかな適用が呼び掛けられています。

- 翌13日にはAdobe社からもAdobe Acrobat・Acrobat Reader他のセキュリティアップデートがリリースされている他、19日にはOracleからもJava・MySQL等について四半期に一度のアップデートがリリース予定です。

AUS便りからの所感

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

2023年4月マイクロソフトセキュリティ更新プログラムに関する注意喚起

JPCERT-AT-2023-0007
JPCERT/CC
2023-04-12

I. 概要

マイクロソフトから同社製品の脆弱性を修正する2023年4月のセキュリティ更新プログラムが公開されました。これらの脆弱性を悪用された場合、リモートからの攻撃によって任意のコードが実行されるなどの可能性があります。マイクロソフトが提供する情報を参照し、早急に更新プログラムを適用してください。

マイクロソフト株式会社
2023 年 4 月のセキュリティ更新プログラム
https://msrc.microsoft.com/update-guide/ja-JP/releaseNote/2023-Apr

マイクロソフト株式会社
2023 年 4 月のセキュリティ更新プログラム (月例)
https://msrc.microsoft.com/blog/2023/04/202304-security-update/

これらの脆弱性の内、マイクロソフトは次の脆弱性について悪用の事実を確認していると公表しています。マイクロソフトが提供する情報を参考に、速やかに対策適用を検討いただくことを推奨します。

CVE-2023-28252
Windows 共通ログ ファイル システム ドライバーの特権の昇格の脆弱性
https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2023-28252

- CVE-2023-28252は通常リモートから直接攻撃可能なものではありませんが、PC上で不正なプログラムを実行するだけで攻撃者に管理者権限が乗っ取られる恐れがあり、こういった攻撃を可能な限り阻止できるよう、アンチウイルス・UTM等による防御も併せて実施することが重要です。

- Windows 10 21H2については6月14日の月例アップデートをもってサポート終了が予定されており、以後も引き続きセキュリティアップデートが受けられるよう、必ず22H2へのバージョンアップを行うようにしてください。

- 今日ではAcrobat Readerのインストールをせずともchrome・Edge等のWebブラウザーでPDF文書を開くことができますが、EdgeのPDFリーダー機能は今後Acrobat Readerベースに移行することが発表されており、「ヘルプとフィードバック」→「Microsoft Edgeについて」(もしくはedge://settings/help)において最新バージョンへアップデートされているか随時確認する習慣をつけることを強く推奨致します。