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。

●3月の「ドコモ光」「ぷらら」顧客情報流出、原因は元派遣社員による持ち出し…被害は約596万件に

https://internet.watch.impress.co.jp/docs/news/1519004.html
https://www.docomo.ne.jp/info/notice/page/230721_00_m.html

このニュースをザックリ言うと･･･

- 7月21日(日本時間)、NTTドコモより、3月に発生した「ぷらら」「ひかりTV」ユーザーの個人情報流出に関する続報が報告されました。
- 3月の発表の時点で、被害を受けたのは両サービスユーザーの氏名・住所・電話番号・メールアドレス・生年月日・フレッツ回線ID・お客さま番号の一部(クレジットカードおよび口座情報は含まれていない)とのことです)、同社の業務委託先の業務PCからの情報流出が原因とされていました。
- 今回新たに、委託先の元派遣社員が不正に情報を持ち出していたこと、また被害件数は最大約596万件に上る可能性がある(当初は最大529万件と見積もられていました)ことが明らかになっています。

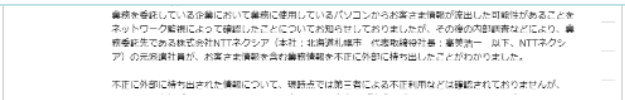
AUS便りからの所感等

- 持ち出された情報は元派遣社員が個人契約する外部ストレージに保存されていましたが、外部ストレージへの第三者からのアクセスないし不正利用は確認されていないとのことです。
- 3,504万件の個人情報流出被害を出した2014年7月のベネッセホールディングスの事例では、業務委託を受けたシステムエンジニアがUSBメモリーへのデータ保存を繰り返し行っていたとされていますが、今回は業務PCから外部ストレージへのアクセスを行ったことで持ち出しが発覚しており、大容量の個人情報データが外部に送信されたこと以上に、業務PCに保存することが可能な状態にあったと推測されます。
- サーバー側において、機密情報・個人情報へのアクセスに際し詳細なログが記録され、不自然な件数・容量の情報アクセスについて検知・遮断等が行えるシステムの構築、また従業員のPC側においても、意図的か否かに拘らず常時多数の情報が保存されないような仕組みやルールの導入により、不正な持ち出し以外にもマルウェア感染や不正アクセス時に情報が流出してしまうリスクを最小限に抑止するための対策を検討頂ければ幸いです。

Impress Watch

NTTドコモ、「ぷらら」や「ひかりTV」の顧客情報約596万件が流出と発表

大東 奈央　2023年7月26日 11:20



株式会社NTTドコモは7月21日、「ぷらら」および「ひかりTV」の顧客情報約596万件が流出したと発表した。

3月31日に情報流出の可能性を発表していた件について、その後の内部調査などにより明らかになったもの。3月30日に、同社が業務を委託していた企業で、情報流出の可能性を確認したとしていた。

3月30日、ネットワーク監視によって、NTTネクシアの元派遣社員が使用していたPCから、業務では行うことがない外部への通信が発生したことを検知した。ただちに当該のPCをネットワークから隔離し、フォレンジック調査やログの確認、当該元派遣社員へのヒアリングなどにより持ち出された可能性があるファイルの特定を進め、警察への相談も行っていたという。

●「To:」に1000件のメールアドレス表示…メール送信の設定ミス

https://www.itmedia.co.jp/news/articles/2307/24/news148.html
https://www.nikkei.co.jp/nikkeiinfo/news/information/1133.html

このニュースをザックリ言うと･･･

- 7月21日(日本時間)、日本経済新聞社より、メール送信時の問題で、送信相手のメールアドレスが流出した可能性があると発表されました。

- 7月20～21日に開催されたイベントの事前登録者6,444人に対し同19日に案内メールを送信した際、1人ずつ個別に送信するところ、プログラムの設定ミスにより最大1,000人分がまとめて送信され、かつ送信先がTo:に表示されていたとのことです。

- 同社ではメールシステムの速やかな改修により、対応するとしています。

AUS便りからの所感

- 多数の相手にメールを送信する際に、「To:やCc:にアドレスを入力したために他の送信相手のアドレスが閲覧可能な状態になる」「アドレスを間違えて無関係の相手に送信する」といった事故は過去も多数発生しており、2021年度には個人情報漏洩の事故原因の37.0%がメール誤送信だったとする調査結果も出ています(AUS便り 2023/07/19号参照)。

- 「メーラーのBcc:に多数のアドレスを入力する」方法をとっているケースに対し、事前のチェックや事故防止のためのシステム採用等はもちろん重要ですが、今回のように、システムの設定ミス等があった場合、どのような問題が発生し得るかについての情報も調査し、今後の対策にあたり参考とされることも望ましいでしょう。

ITmedia NEWS

日経新聞、「To」に最大1000件のアドレス入れたままメール送信　設定ミスで

2023年07月24日 17時23分 公開　[ITmedia]

日本経済新聞社は7月21日、最大1000件のメールアドレスが漏えいした可能性があると発表した。6000人超が参加するイベントの案内を、参加者一人一人に送ろうとしていたところ、最大1000件のアドレスを「To」欄に入力したまま送ったという。

当該メールは19日（水）午前8時30分ごろ、日経メッセ大阪の運営事務局（messeosaka@nikkeineon.jp）から来場事前登録者6,444人に対し、「日経メッセ大阪2023 いよいよ明日から開催」という件名で送信いたしました。本来であれば、お一人お一人個別にメールをお送りすべきところ、メール送信システムのプログラムの設定ミスによって最大1,000人にまとめて送信され、「To」に最大1,000人のメールアドレスがまとめて表示された状態となっておりました。

日経新聞の発表

●リモートデスクトップの脆弱性を突く攻撃に注意喚起…パッチ適用しにくいケースに要警戒

https://news.mynavi.jp/techplus/article/20230723-2732337/
https://thehackernews.com/2023/07/a-few-more-reasons-why-rdp-is-insecure.html
https://cyolo.io/blog/dll-hijacking-strikes-back-exploiting-windows-on-arm-rdp-client-cve-2023-24905
https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2023-24905
https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2023-35332

このニュースをザックリ言うと･･･

- 7月20日(現地時間)、「The Hacker News」より、リモートデスクトップ(RDP)における2件の脆弱性を取り上げ、これらを悪用する攻撃に対し注意を促す記事が出されています。

- 記事では、5月に発表されたRDPクライアントの脆弱性「CVE-2023-24905」と、7月に発表されたRDPゲートウェイの脆弱性「CVE-2023-35332」に言及しており、それぞれクライアントPCの乗っ取りと、セキュリティ機能の回避が可能になるとされています。

- いずれもマイクロソフトによる月例のセキュリティアップデートで修正されていますが、特に前者をはじめとする「リモートコード実行(RCE)脆弱性」の発見が後を絶たないことから、堅牢なアクセス制御等を行うことを推奨しています。

AUS便りからの所感

- 記事から参照されている、セキュリティベンダーCyoloのブログによれば、CVE-2023-24905は不正なrdpファイルを開いた場合に発生するもので、かつARMデバイス上のWindowsでのみ発生が確認されているとのことですが、一般的なx86-64アーキテクチャ(Intel・AMD)のWindowsでも有効な別の脆弱性が今後発見されることは容易に予想され、油断は禁物です。

- 記事では、セキュリティアップデートを適用しにくいとされるOT/ICS、即ち工場や産業用システムでRDPを使用しているケースが特にターゲットとなり易いとしており、一般企業のネットワークであっても、セキュリティアップデートの適用が間に合わず、また侵害されたあるクライアントからサーバーや別のクライアントに攻撃される可能性を考慮し、個々のクライアントを可能な限り隔離するネットワーク・システム構成とすることも検討に値するでしょう。

TECHR Powered by マイナビニュース

Windowsリモートデスクトッププロトコル（RDP）に複数の脆弱性、注意を

掲載日 2023/07/23 18:16　著者：後藤大地

The Hacker Newsは7月20日(米国時間)、「A Few More Reasons Why RDP is Insecure (Surprise!)」において、リモートデスクトッププロトコル(RDP: Remote Desktop Protocol)の危険性について伝えた。RDOが安全ではないことを示す最近の脆弱性が紹介されており、システムを保護するためのセキュリティ対策が重要であることが強調されている。