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。

●更新されていないVPN機器から侵入か…ランサムウェア感染で最大4万人分の個人情報流出

https://www.yomiuri.co.jp/national/20240611-OYT1T50115/
https://www.sanyonews.jp/article/1565381
https://www.popmc.jp/home/organization/5w64e269/5bid3p49/zx2nd5xq/

このニュースをザックリ言うと･･･

- 6月11日(日本時間)、岡山県精神科医療センターより、同センターのシステムが不正アクセスを受け、個人情報が流出した可能性があると発表されました。
- 被害を受けたとされるのは、同センターで過去約10年間に受診した患者最大約40,000人分の氏名・住所・生年月日・病名等、および病棟会議の議事録等とのことです。
- 5月19日にランサムウェアによる攻撃を受けデータの暗号化とシステムダウンが発生、その後被害届を受けた岡山県警から6月7日に情報の流出を確認したとの連絡があったとしています。

AUS便りからの所感等

- 医療機関のシステムがランサムウェア攻撃を受け、データの暗号化や電子カルテが使用できなくなる等の被害が発生したケースが過去にも報告されています。
- VPN装置に脆弱性が報告されていたにも拘らず機器の更新がされていなかったことが一部で報じられており、侵入経路となった可能性が考えられます。
- システム全体において脆弱性の悪用による侵入や情報流出等の被害を受けないようOS・ファームウェア等の確実な更新、アンチウイルス・UTMによる防御を行うことと、データ暗号化や消去等に備えバックアップは多重に行いかつバックアップデータの保護も必ず行うことが重要です。

読賣新聞オンライン

岡山県精神科医療センターにサイバー攻撃...最大４万人分の個人情報流出の可能性

2024/06/11 18:24　この記事をスクラップする

岡山県精神科医療センター（岡山市北区）は１１日、電子カルテなどを管理するシステムが身代金要求型ウイルス「ランサムウェア」によるサイバー攻撃を受け、最大４万人分の患者の個人情報が流出した可能性があると発表した。電子カルテが閲覧できなくなったが、紙のカルテを使うなどし、診療に影響はないという。

山陽新聞さんデジ digital

県精神科センター 患者の情報流出　最大４万人分、サイバー攻撃

地方独立行政法人・岡山県精神科医療センター（岡山市北区鹿田本町）は１１日、サイバー攻撃によって患者の個人情報が流出したと発表した。最大で約４万人の氏名や生年月日、居住する市町村、病名、入院期間などが漏れた可能性があり、岡山県警が不正アクセス禁止法違反容疑も視野に捜査している。悪用の報告はない。

法人によると昨年６月、自治体病院の全国組織から、病院の情報システムに外部から接続する際に使うＶＰＮ（仮想専用線）に関してサイバー攻撃に脆弱（ぜいじゃく）な機種の通知があり、センターの機器が該当すると判明。更新に向け業者と協議したが具体的な進展がなく、今年４月以降は棚上げになっていたという。

●最高裁がメール送信ミス、計900人分のメールアドレス等流出

https://www.itmedia.co.jp/news/articles/2406/04/news098.html
https://www.courts.go.jp/saikosai/sihokensyujo/sihosyusyu/300-71syuusyuuseihe/0603syuusyuusikin/index.html

このニュースをザックリ言うと･･･

- 6月3日(日本時間)、最高裁判所より、メール送信時の問題で、送信相手のメールアドレス・氏名等が流出した可能性があると発表されました。

- 同3日に行った修習資金の貸与対象者900人へのメール連絡時、450人毎のグループで計2通のメールを送ろうとした際、メールアドレス(および氏名・修習資金に関するID)をBcc: ではなく宛先欄(To: とみられる)に入力し、受信者が相互にこれらを閲覧可能な状態となったとしています。

- 最高裁では、「できる限り速やかに原因を分析した上で、その分析結果を踏まえ、再発防止策を検討する」等としています。

AUS便りからの所感

- 数百件という多数のメールアドレスをメーラーのBcc: 欄にコピー＆ペーストするやり方は、たとえダブルチェック等で万全を期そうとしても、ケアレスミスから流出に至ることを根本的に防止できるものではないでしょう。

- 特に今回は、(恐らくはメーラーのアドレス帳から)メールアドレス以外の氏名等の情報も含め入力していたとのことで、Bcc: 欄への入力を想定していたのであれば無意味なものであり、ミスによって本来流出しなくていい情報まで流出する事態となっています。

- 同報メール配信システムやメーリングリストの活用、メーラーで対応せざるを得ない場合はメーラー自身やアドオンの誤送信防止機能の使用、またメールサーバーやUTMにおける不審な大量送信時のチェック機構等があれば併せて使用するといった、システム側での対策を行うことを検討すべきです。

- ただし、システムによる対策においても、複雑な機構に潜むバグ(AUS便り 2021/08/03号参照)であったり、有償サービスの更新忘れで機能しなくなる(同 2023/04/18号参照)ケースも報告されており、大量送信を想定したテスト等は不可欠でしょう。

ITmedia NEWS

最高裁、メールのBCCとTOを間違え漏えい

2024年06月04日 10時38分 公開 [ITmedia]

最高裁判所は6月3日、メールの送信時にBCCとTOを誤り、メールアドレスなどが漏えいしたと発表した。司法試験に合格した司法修習生に貸し出す修習資金を借りている人に向け、住所変更がある場合は届け出てほしい旨を通知するメールでミスがあったという。

最高裁判所（公式サイトから引用）

間違えがあったのは3日に送信したメール。2件のメールで間違え、各450人（計900人）の氏名、メールアドレス、修習資金に関するIDが、メールを受け取った人同士で確認できる状態だったという。

● 「フィッシングレポート 2024」、対策協議会より発表

https://www.antiphishing.jp/report/wg/phishing_report2024.html

このニュースをザックリ言うと･･･

- 6月4日(日本時間)、フィッシング対策協議会より、フィッシングの被害状況、フィッシングの攻撃技術・手法などをとりまとめた「フィッシングレポート 2024」が発表されました。

- 半期ごとの同協議会へのフィッシング情報届出件数は上昇を続けており、近年では2021年下半期298,277件から2022年上半期450,082件、2023年上半期530,804件から下半期665,586件と急増しています。

- 一方でフィッシングサイト件数(URL)は2022年上半期に219,549件を記録しましたが、以後2023年は上半期95,682件、下半期98,272件と10万件未満に留まっているとのことです。

AUS便りからの所感

- フィッシングサイト件数ですが、2024年3月に急増がみられ、同1～4月では既に127,565件を記録しています。

- 海外の状況はまた異なり、米APWG(Anti-Phishing Working Group)へのフィッシング情報届出件数は例えば2020年下半期と2022年下半期に増加を見せ、以後は減少するといった状況となっています。

- レポートでは他にもフィッシングで多用された手法や技術的な対策の紹介を行っており、特になりすまし対策のSPF・DKIM・DMARCはGoogle等がメール送信者に対し採用を義務付ける等の状況となっていることから、利用者や管理者においてはレポートの熟読によりフィッシングメール等に対する慎重な行動あるいは対策技術の採用を進めていくことを強く推奨致します。

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

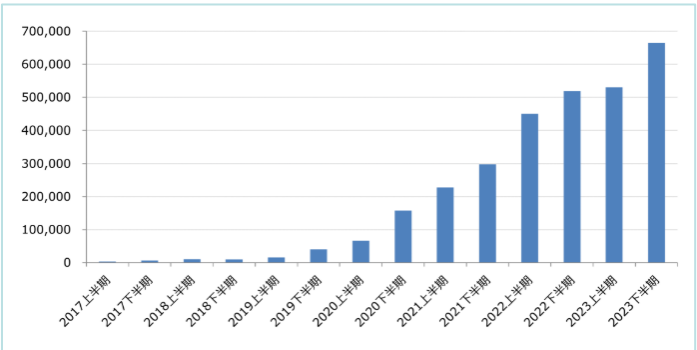

図 1-1 国内のフィッシング情報の届け出件数[2]