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。

●VPN装置の脆弱性から侵入、アンチウイルスは無効化…半田病院サイバー攻撃事案の報告書発表

https://www.asahi.com/articles/ASQ6731D3Q62ULZU00L.html
https://xtech.nikkei.com/atcl/nxt/column/18/00001/06927/
https://www.handa-hospital.jp/topics/2022/0616/index.html

このニュースをザックリ言うと･･･

- 6月7日(日本時間)、徳島県つるぎ町立半田病院より、昨年10月に発生した同病院へのサイバー攻撃事案に関する報告書が発表されました。

- 同病院の電子カルテシステムがランサムウェア「Lockbit2.0」に感染し、今年1月4日の通常診察再開までの間、カルテの閲覧をはじめ各種業務に支障をきたす事態となったものに対し、外部の有識者を交えた会議による調査・分析結果等となっている他、コンピュータソフトウェア協会のSoftware ISACによる「情報システムにおけるセキュリティ コントロール ガイドライン」も併せて発表されています。

- 攻撃者が侵入した経路としては、米Fortinet社製のVPN装置が更新されていないことにより、機器の脆弱性を突かれた可能性が高いとされていますが、周辺のシステム環境や運用体制にも様々な問題があったことが明らかになっています。

AUS便りからの所感等

- 侵入のために悪用されたとされる脆弱性「CVE-2018-13379」は2019年5月に発表、セキュリティアップデートがリリースされていたものですが、攻撃発生直前の2021年9月には国内外の未対策のVPNホスト約87,000台へ不正アクセスするためのパスワード情報が攻撃者によって公開されたとしてFortinet社から注意喚起が出される等、深刻な問題となり続けていたものです。

- 「内部LANは安全である」という認識のもと「(電子カルテシステムの導入時に不具合が生じたという理由で)アンチウイルスソフトが無効にされる」「端末のパスワードが最短で5桁、ロックアウト等もなく総当たり攻撃による不正ログインが可能な状態」といった問題が発生していたこと等が報告書に記載されていた一方で、一部報道等により、コスト節約のためベンダーとの適切な保守契約を結んでいなかったとみられる節があることに対する指摘の声もある模様です。

- 奇しくも6月19日には、同じく徳島県の鳴門市の病院がランサムウェアに感染する被害を受けていますが、こちらは幸いにもオフラインバックアップからの速やかな復旧が行われたとの発表があり、半田病院の事案を他山の石としたものと見受けられます。

- ともあれ、病院のみならずあらゆる会社・組織において、今回の報告書およびセキュリティコントロールガイドラインをもとに、自組織のシステムがマルウェアや各種攻撃への十分な耐久力あるいは速やかな復旧等の体制が整っているかの見直しを図る等の行動を是非ともとって頂ければ幸いです。

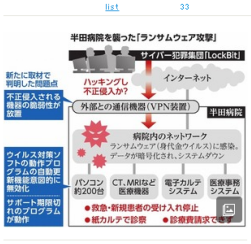
朝日新聞 DIGITAL

電子カルテが古く、ウイルス対策無効に　サイバー攻撃受けた半田病院

有料会員記事

編集委員・須藤龍也、藤野隆晃　2022年6月7日 11時43分

シェア　ツイート list　ブックマーク 33　メール　印刷



昨年10月にランサムウェア(身代金ウイルス)による サイバー攻撃 を受け、約2カ月間にわたり病院の機能が停止した 徳島県 つるぎ町立 半田病院 で、仕様が古い電子カルテシステムを動かすため、セキュリティー対策に必要な機能が意図的に無効にされていたことが、関係者への取材で分かった。パソコンのウイルス対策ソフトを停止させるなどしており、対策ソフトが動作していれば被害拡大を防いだ可能性があったと専門家は指摘している。

これらの経緯については7日午前、町議会に提出された同病院の有識者会議による調査報告書でも、問題点として指摘したとみられる。病院は今後、抜本的なセキュリティー対策の見直しに取り掛かる。

● 1,020社のWebサイトがデータ消去で閲覧障害…サイト管理者ら逮捕

https://www.sankei.com/article/20220607-DWZCNIFBXBNSDC2WADV5GJRL5A/

このニュースをザックリ言うと･･･

- 6月7日(日本時間)、愛知県警より、Web制作会社が管理するサイトを閲覧不能にさせた容疑で、派遣会社所属の男AとWeb制作会社の男Bを逮捕したと発表されました。

- 発表によれば、容疑者Aは昨年11月、愛知県あま市のネットカフェから容疑者Bが所属するWeb制作会社(以下・同社)が管理するサーバーに接続し、4件のサイト表示に必要なデータを消去、サイトの閲覧障害を発生させた容疑が持たれています。

- 被害が及んだサイトは同社が作成・管理した計1,020社分におよび、被害総額は4,500万円を超えるとされています。

AUS便りからの所感

- 報道によれば、容疑者Bは「Aに騙されてやった」と否認したとされており、何らかの経緯で1,020社分のサイトの管理アカウント情報がAに渡された可能性があります。

- Webサイトやシステムの制作・管理を請け負う会社が多数の顧客のシステムにアクセスする情報を保持しているところでは、今回のように騙されてまとまった情報を引き渡す以外にも、攻撃者が情報を管理するサーバーに侵入することにより、根こそぎ情報を奪取され、そこから芋づる式に不正アクセスの被害を受ける可能性についても注意が必要でしょう。

- 顧客システムへのアクセス情報等を預かる管理者や請負業者が、アカウントを奪取される等から即所有する情報全てにアクセス可能となる事態を防ぐような体制を作ることは、中小零細企業～個人運営である場合にはこと困難な話と思われ、場合によっては多要素認証を持つクラウドサービスに情報を保存する等も検討に値するでしょう。

データ消去しウェブサイト閲覧不能に　容疑で男２人逮捕

2022/6/7 20:01

産経WEST | できごと　社会 | 事件・疑惑　地方 | 中部　愛知

愛知県警本部＝名古屋市

愛知県警は７日、ウェブ制作会社が管理するサイトを閲覧不能にしたとして、電子計算機損壊等業務妨害の疑いで、岐阜県大垣市波須、派遣社員、内藤良仁容疑者（３４）と、名古屋市中村区高道町、自営業、江川政之容疑者（３４）を逮捕した。

逮捕容疑は共謀して昨年１１月２３～２４日、愛知県あま市内のインターネットカフェのパソコンを使い、名古屋市中村区のウェブ制作会社が管理するサーバー内にあった、４社のサイト表示に必要なデータファイルを削除して閲覧不能にしたとしている。

●メルカリを装う偽サイト出現、公式が注意喚起…「手口が巧妙化し本物と区別がつきにくい」

https://www.itmedia.co.jp/news/articles/2206/14/news187.html
https://jp-news.mercari.com/articles/2022/06/dd/security/

このニュースをザックリ言うと･･･

- 6月14日(日本時間)、メルカリより、同サービスの公式サイトを装った不審なサイトが確認されたとして注意喚起が出されています。

- 偽サイトではログイン情報や認証番号の詐取を行うとされている他、入力後にカウントダウンを行うものがあり、詐取した情報を本物のサイトに入力して不正ログイン等を試行している可能性があるとしており、万が一偽サイトにパスワードを入力した場合は速やかにアカウント情報を変更するよう推奨しています。

- 同社では、詐欺の手口は非常に巧妙になっており、メルカリ公式サイトとの区別がつきにくくなっているとしており、他の対策として「広告から遷移したサイトではユーザー情報の入力やログインはせず、必ずアプリ・検索サイト経由で公式サイトを確認する」「メルカリを名乗るメール・SMSに記載のURLにはアクセスしない」等を呼び掛けています。

AUS便りからの所感

- 日本をターゲットとするフィッシングメール等においては、文面が稚拙なためにそれと判断しやすいケースが依然多いとはいえ、例えばEmotetが感染したPCから奪取した本物のメールの文面を参考にするように、相手に気づかれにくいレベルの偽装を行われた場合にたちどころに被害が増加する恐れは十分に考えられます。

- メールやSMSにURLを記載しないというアプローチは、サービスが公式に送信する全てのメール等でこれを行うことは利便性を損ねる場面が出てくる可能性があり、決して簡単ではないでしょうが、ユーザーをフィッシングの被害から守る強力な方策とされることもよくあります。

- ともあれフィッシング等が目的とみられる不審なメールに対し、ネット上での報告等を参考にしつつ、リンクが記載されていても安易に踏むことなく、メルカリが推奨するようなアプリからアクセス、あるいは事前に公式サイトをブックマークに登録したものからアクセスすることにより、回避するよう心掛けることは重要です。

メルカリを装う偽サイト出現、公式が注意喚起　「手口が巧妙化し本物と区別がつきにくい」

2022年06月14日 19時42分 公開　[松浦立樹，ITmedia]

メルカリは6月14日、メルカリ公式サイトを装った不審なサイトを確認したと発表した。詐欺の手口が巧妙化し本物の公式サイトと区別がつきにくくなっているという。偽サイトでアカウント情報などを入力すると、悪意のある第三者にアカウントを盗まれる可能性があるため注意するように呼び掛けている。