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。

●新聞社サーバーがランサムウェア感染…紙面ページ数縮小の事態

https://xtech.nikkei.com/atcl/nxt/news/18/16480/
http://www.nagano-np.co.jp/articles/119535

このニュースをザックリ言うと･･･

- 12月21日(現地時間)、長野県の地方新聞「長野日報」を発行する長野日報社より、同社の社内サーバーがランサムウェアに感染したと発表されました。

- 同19日23時過ぎにサーバーと組版用端末において感染が確認され、製作に影響が出たとしており、発表が掲載された21日発行分の紙面は通常の16ページから8ページに縮小した特別紙面となっています。

- 被害を受けたサーバーは公開を前提として紙面に使用する記事と写真データが蓄積されていたもので、個人情報の流出はなく、ホームページやメールシステムは通常通り稼働しているとのことです。

AUS便りからの所感等

- 22日には同社ホームページにもお詫びが掲載され、同日発行分も引き続き特別紙面になるとしており、またこの時点では被害の長期化も予想されるとしています。

- 警察庁の発表では2022年に過去最大の230件のランサムウェア被害、また2023年も上半期に103件の被害が報告されており、7月には名古屋港のコンテナターミナル管理システムが「LockBit」に感染して搬出入作業に影響が出る(AUS便り 2023/07/11号参照)等、依然猛威を奮っています。

- ランサムウェアへの対策において重要なのは、クライアント・サーバー共に感染しないこと以上に、感染が発生した場合のシステム・データの保護、およびバックアップから確実に復旧できる体制を整えることであり、バックアップデータをも暗号化されて復旧に使えなくなる事態とならないよう、「複数コピー」をとる」「オンラインから隔離された場所あるいは書き換え不可能なストレージ(サービス)に保管する」「バックアップとリストアが確実に実行できるようテスト」することが推奨されています(同2021/09/14号参照)。

日経 XTECH

長野日報社がランサムウエア被害、ページ数半減など新聞製作に影響

永田 雄大　日経クロステック／日経コンピュータ

2023.12.21

長野日報社は2023年12月21日、ランサムウエアに感染したと発表した。被害を受けたのは新聞製作のためのメインサーバー。この影響により、同社は同日付の朝刊を通常の16ページから8ページに半減する特別紙面を発行した。

> 社会

おわび（サーバーダウンによる特別紙面）

社会　2023年12月21日 6時00分

いいね！　ポスト　Pocket

弊社のサーバーが悪意のあるコンピューターウイルス（ランサムウエア）に感染し、新聞製作に影響を及ぼしています。このため、２１日付本紙は特別紙面体制として発行します。

１２月１９日深夜に、弊社サーバーが身代金要求型ウイルス（ランサムウエア）による被害が発生していることを確認しました。今回の被害に対応するため、ネットワークからサーバーを切り離しています。当社のホームページやメールシステムは通常通り稼働しています。

現在、外部専門家や警察と連携の上、システムの保護と復旧に向けて作業を進めていますが、長期化も予想されます。読者や広告クライアントの皆さま等関係者には多大なるご迷惑をおかけすることをおわび申し上げます。

長野日報社

長野日報社はランサムウエア感染の影響で、2023年12月21日付の朝刊が特別紙面になったことをおわびした

（出所：長野日報社のホームページを日経クロステックがキャプチャー）

[画像のクリックで拡大表示]

同社が被害を確認したのは2023年12月19日午後11時過ぎのこと。被害の規模は調査中だ。長野日報社の宮坂康弘専務取締役編集局長によれば、「新聞製作のメインサーバーと紙面を作るための組み版端末がランサムウエアに感染した」。現在は緊急用の端末で対応している。

● SSHプロトコルに脆弱性、サーバー側およびクライアント側のアップデートを

https://gigazine.net/news/20231220-terrapin-attack/
https://terrapin-attack.com/

このニュースをザックリ言うと・・・

- 12月18日(現地時間)、ドイツの大学のセキュリティ研究者より、SSH(セキュアシェル)プロトコルに存在する脆弱性(CVE-2023-48795他)を突く攻撃「Terrapin Attack」が発表されました。

- SSH通信時に特定の暗号化形式もしくは特定のMAC(メッセージ認証符号)を使用している場合、いわゆる「中間者攻撃」により、攻撃者が安全な通信を妨害することが可能としています。

- SSHの最もメジャーな実装であるOpenSSHには9.5までのバージョンに脆弱性が存在するとし、対策等を行った最新バージョン9.6をリリースしている他、 PuTTYやTeraTerm等SSHに対応した各種ターミナルソフトでも対策が進んでいます。

AUS便りからの所感

- 攻撃はSSHポートが開いているサーバーに対し直接実行できる類のものではなく、SSH通信を途中のルーター等で傍受できる場合に可能となるものです。

- 脆弱性が発生する条件は、暗号化形式としてChaCha20-Poly1305、あるいはMACとしてEncrypt-then-mac(eth)に対応するものを利用していること、とされていますが、OpenSSHのデフォルトの設定(サーバー・クライアント共)ではこれら(MACについては「eth@openssh.com」という文字列を含むもの)を優先して使用するため、影響範囲は比較的広いとみられます。

- Terrapin Attackに関する公式サイトでは、SSHサーバーやクライアントに脆弱性が存在するか検証可能なツールも提供されています。

- ともあれ、Linuxサーバー等への安全な接続・ログインに欠かせないSSHに影響する脆弱性であり、サーバー側はもちろんクライアント側でもセキュリティアップデートを確実に適用することが重要です。

●年末年始における情報セキュリティの注意喚起、IPAより発表

https://www.ipa.go.jp/security/anshin/heads-up/alert20231221.html

このニュースをザックリ言うと・・・

- 12月21日(日本時間)、IPAより、年末年始を迎えるにあたっての、情報セキュリティに関する注意喚起が出されました。

- 多くの企業・組織において、この時期に従業員等が長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。

- IPAは毎年のゴールデンウィークと夏季・冬季休暇の時期に注意喚起を行っています(https://www.ipa.go.jp/security/measures/vacation.html)。

AUS便りからの所感

- 注意喚起の内容は、システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性から、従業員が旅行先等でSNSへの書き込みを行った場合に、最悪関係者にも思わぬ被害が及んでしまう可能性まで、多様なものとなっています。

- 挙げられているセキュリティ対策の内容は毎回大きく異なるようなものではなく、この他にも長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策(https://www.ipa.go.jp/security/measures/everyday.html)」として別途まとまっており、常日頃において準備・点検を行うよう意識していくことが肝要です。