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。

●東北他7県利用予定のクラウドシステムに設定不備…計91万件メール不正送信の踏み台に

https://www.jiji.com/jc/article?k=2022032000438&g=pol
https://www.itmedia.co.jp/news/articles/2203/22/news096.html
https://www.pref.akita.lg.jp/pages/archive/63598
https://www.softbanktech.co.jp/news/topics/info/2022/006/

このニュースをザックリ言うと･･･

- 3月20日(日本時間)、秋田県より、同県が運営する「秋田県情報セキュリティクラウド」のメールシステムが不正アクセスを受けたと発表されました。

- 不正アクセスにより、3月18日16:46頃～18:55頃にかけて、秋田市のドメイン名(city.akita.akita.jp)で434,496件、横手市のドメイン名(city.yokote.lg.jp)で7件の不審なメールが外部に送信されたことが明らかになっています。

- この他、青森県八戸市・福島県郡山市および新潟県糸魚川市からも、セキュリティクラウドへの不正アクセスと、4県合わせて80万件に上る不正なメール送信の発生が発表されています。

- 3月22日にはクラウドサービスの導入を委託されていたSBテクノロジー社(以下SBT)からも発表があり、この時点で送信された不正なメールは合計912,299件とのことです。

AUS便りからの所感等

- 前述した秋田市・横手市の他、八戸市(city.hachinohe.aomori.jp)、郡山市(city.koriyama.fukushima.jp)、糸魚川市(city.itoigawa.niigata.jp)および長岡市(city.nagaoka.lg.jp)各ドメイン名のメールアドレスで、件名等が英語のスパムメールが送信されているとされ、メール内のURLをクリックしたり、添付ファイルを開いたりしないよう呼び掛けられています。

- 時事通信の報道等によれば、東北6県および新潟県において同一のクラウドサービスの導入が予定されていたところ、SBT社によるメールシステムの移行作業中、アクセス制御設定に不備があり、サーバーが任意のアドレスからメール送信に使用可能な状態(オープンリレー)になっていたとのことで、19日未明に対策が行われたとしています。

- サーバーが攻撃者に侵入されたり、マルウェアに感染したというものではないようですが、スパムメールの発信元となったことにより、メールサーバーのIPアドレスが「メール受信拒否リスト」に登録され、正当なメールの相手方での受信が阻害されるといった事態にもなっていた模様です。

- なりすましメールの受信を防いでもらうための機構であるSPF・DMARC等では、このようなケースで正当な発信元から発信される不審なメールを遮断することは困難であり、別の機構による対策、加えてクライアントPC～サーバーの乗っ取り等の発生時に外部へメール送信も含めた不審な通信を行われないようにする対策等を事前にとるようにすることが肝要です。

JIJI.COM

不正メール８０万件送信か　４県システムに不正アクセス

2022年03月20日21時02分

秋田県庁舎＝２０２０年８月２０日

秋田県は２０日、運営するメールシステムに不正アクセスがあり、秋田市を装った不正メールが約４２万件、外部に送信されたと発表した。委託業者の設定ミスが原因という。

最恐ウイルス「エモテット」猛威◆再燃の裏側とロシアの影

県によると、青森、福島、新潟各県でも同様の手口で計約３８万件の不正送信が確認された。東北６県と新潟県は来年度に向け、同一のクラウドサービスを導入する準備をしていた。

不正送信があったのは１８日午後５～７時ごろ。秋田県によると、委託先のＳＢテクノロジー（東京）によるメールシステムの移行作業中、アクセス制御設定に不備があり、外部から侵入可能になっていた。１９日未明に対策を施し、現時点で情報漏えいや被害の報告はない。

ITmedia NEWS

自治体から迷惑メール91万件　SBテクノロジーのセキュリティクラウド、設定ミス突かれ踏み台に

2022年03月22日 11時49分 公開　[岡田有花，ITmedia]

印刷　156　Share　B!　13　2

SBテクノロジーは3月21日、同社が提供する自治体向け情報セキュリティクラウドが、メール中継システムの設定ミスにより、迷惑メールの踏み台になったと発表した。

不正送信されたメールは91万2299件（.jpドメイン向け2467件、それ以外のドメイン向け90万9832件）。メール中継システムが受信拒否リストに登録され、自治体の一部メールが送信できない問題も発生していた。

システムを利用している秋田県などが被害を公表した。個人情報など自治体内の情報漏えいは確認していないという。

3月18日（金）	14：43	メール中継システムにおいて送信障害が発生。
	14：50	送信障害の原因特定のための調査を開始。

● 「APC Smart-UPS」に不正アクセスの脆弱性、物理的破壊に至る恐れも

https://news.mynavi.jp/techplus/article/20220310-2289919/
https://www.armis.com/research/tlstorm/

このニュースをザックリ言うと・・・

- 3月8日(現地時間)、セキュリティベンダーの米Armis社より、Schneider Electric社の無停電電源装置「APC Smart-UPS」に複数の脆弱性が存在すると発表されました。

- 発表ではこれらの脆弱性を「TLStorm」と呼称しており、UPSにリモートからアクセス可能な場合、脆弱性を悪用し、UPS上での不正なコードの実行やファームウェアの改ざん等を行うことにより、UPSが乗っ取られ、最悪の場合、機器の加熱やコンデンサの破壊等の物理的な不正行為も可能とされています。

- 影響を受けるとみられるUPSは合計2,000万台以上に上るとされる一方、脆弱性に対するセキュリティアップデートや回避策は既に公開済みとされているとのことです。

AUS便りからの所感

- 脆弱性は、ファームウェア更新ファイルの署名・暗号化用鍵の問題(CVE-2022-0715)と、TLS暗号化処理の問題(CVE-2022-22805, CVE-2022-22806)によるものとされています。

- Schneider社のセキュリティ情報ページ(https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp)においても3月8日付で当該脆弱性に関する情報(SEVD-2022-067-02)が公開されています(現時点で日本語の情報はまだ出てはいない模様です)。

- IoT機器や複合機等と同様、UPSについてもファームウェアの随時アップデートを行うよう管理の目が届きにくい傾向があるとみられますが、ネットワーク機能の有無に拘わらず可能な限り全ての機器について存在を把握し、LANやWi-Fiへの接続機能が有効になっているか、実際に接続されているか、あるいはそういった設定が適切かを含め確認する体制、そしてファームウェアの更新情報を常時確認して速やかにアップデートが実施できる体制を整えるよう心掛けるべきです。

● Apache・OpenSSL・BIND、相次いで脆弱性発表

https://news.mynavi.jp/techplus/article/20220316-2294660/
https://news.mynavi.jp/techplus/article/20220317-2294730/
https://news.mynavi.jp/techplus/article/20220318-2296590/

このニュースをザックリ言うと・・・

- 3月15日(日本時間)、Webサーバーソフトウェア「Apache」において、サーバーのダウン等が可能になる脆弱性4件が発表され、修正バージョン2.4.53がリリースされています。

- 同日、暗号化通信ライブラリ「OpenSSL」においてもセキュリティアップデート3.0.2・1.1.1nがリリースされ、OpenSSLを利用するサーバーやクライアントにおいて無限ループを発生させられる脆弱性1件が修正されています。

- 3月17日には、DNSサーバー「BIND」においても、サーバーのダウンや不正なホストへの誘導等の可能性がある脆弱性4件が発表され、こちらもバージョン9.18.1・9.16.27・9.11.31で修正されています。

AUS便りからの所感

- JPCERT/CC等各種機関からもこれらの発表を受け、各ソフトウェアのアップデートを行うよう注意喚起が出されています。

- 一方で、例えばApacheの脆弱性は特定の設定やモジュールの利用時にのみ影響するものが、BINDの脆弱性は比較的新しいバージョンや特定の用途での使用時に発生するものが含まれており、また主なLinuxディストリビューションのパッケージでも対応状況はまちまちで、CentOSでは3月22日時点でパッチがリリースされたものはない模様です。

- ソフトウェアをディストリビューションのパッケージからインストールしている状況で、脆弱性対応の名目で新しいバージョンをソースコードからインストールするのは、以後の管理が煩雑になる等の可能性があるため安易に行わないよう注意し、常日頃からパッケージのアップデートを定期的に行う設定としていることが望ましいでしょう。