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。

●札幌市の財団法人、メールアカウントに不正アクセス…スパムメール送信でブラックリスト登録の事態に

https://scan.netsecurity.ne.jp/article/2025/09/08/53576.html
https://www.kankyou-sapporo.jp/info/6877
https://imakiire.jp/urgent_notice/20250822/

このニュースをザックリ言うと･･･

- 8月25日(日本時間)、一般財団法人・札幌市環境事業公社より、同社のメールアカウントが不正アクセスにより、スパムメール送信の踏み台とされていたと発表されました。

- 発表によれば、不正アクセスは同18日頃に発生、またスパムメール送信により、同社のドメイン名が複数の迷惑メールブラックリストに登録される事態になったとしています。

- 現在メールアドレスの設定の一部変更、ブラックリストの解除申請を進めている一方、同社職員を装った不審なメールや心当たりのないメールを受信した場合にも、メールの開封・添付ファイルの参照・メール本文中のURLのクリック等を行わないよう注意を呼び掛けています。

AUS便りからの所感等

- 8月22日には鹿児島県のいまきいれ総合病院からも、19日に同院のメールアカウントが不正アクセスにより、スパムメール送信の踏み台とされていたと発表されています。

- 「外部からの不正ログイン」以外で不審なメール送信の踏み台に悪用する手口としては、他にも「PCへのマルウェアの感染」や「第三者に偽装した送信元へエラーメールが送信されるよう仕向ける」あるいは「SMTP認証なしでメールの中継が可能な設定(オープンリレー)のサーバーを悪用する」等が挙げられます。

- 踏み台にされたサーバーからなりすましメールが送信された場合、SPF・DKIM・DMARCによる偽メールの検知が困難となる可能性があり、踏み台にされた側でも今回のようにブラックリストへの登録に繋がることにより、通常の運用に支障をきたす恐れが考えられます。

- メールを受信するPC側では添付ファイルのウイルスチェックや、アンチフィッシング機構による不審なサイトへの誘導の遮断等が重要であり、またサーバー側でもメール送受信アカウントに強力なパスワードを設定する等の厳密な管理の他にも、PCのアンチウイルスやUTMによる保護、またサーバー側で不審なログイン試行の監視・遮断、不自然な大量のメール送信に対する送信量の制限、送信メールのスキャン・チェック、といった各種対策の実施を検討すべきでしょう。

ScanNetSecurity by iid

2025.9.8 Mon 8:05

迷惑メール送信元として悪用された一般財団法人に起こったこと

一般財団法人札幌市環境事業公社は8月25日、第三者による同社の一部のメールアドレスの乗っ取りについて発表した。

一般財団法人札幌市環境事業公社は8月25日、第三者による同社の一部のメールアドレスの乗っ取りについて発表した。

これは8月18日頃に、同社の一部のメールアドレスが第三者によって不正に乗っ取られ、迷惑メールの送信元として悪用され、不特定多数に不審なメールが送信された可能性が判明したというもの。その結果、同社のドメイン名が複数の迷惑メールブラックリストサイトに登録されたため、メール送受信が正常に行えない状況となっているという。

●ノルウェーのダムがハッキングにより不正に放流される

https://gigazine.net/news/20250906-norway-dam-hacked-russia/
https://rocket-boys.co.jp/security-measures-lab/norway-dam-forced-valve-opening-cyberattack-authorities-suggest-russian-involvement/
https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/
https://cyberriskleaders.com/hackers-open-dam-valves-in-norway/

このニュースをザックリ言うと・・・

- 8月13日(現地時間)、ロイター通信等のメディア各社より、ノルウェー南西部ブレマンゲルのダムを制御するシステムがハッキングを受け、不正に放流される事態が発生していたと報じられています。
- ハッキングは4月7日に発生していたもので、4時間にわたり毎秒約500リットルの水が不正に放流されていたとしています。
- ノルウェー当局は、親ロシア派のサイバー犯罪グループが関与していると主張しています。

AUS便りからの所感

- 2021年には米フロリダ州で水処理システムが不正アクセスを受け、ごく短時間ながら飲料水内の水酸化ナトリウム濃度が100倍以上に上昇する攻撃が行われています(AUS便り 2021/02/15号参照)。
- 今回の不正アクセスについては、制御パネルに外部からアクセス可能、かつ脆弱なパスワードが設定されていたとする情報もあります。
- 基本的にこのような社会的インフラの制御システムへは、くれぐれも不特定多数からWebアクセスできるような設定は行うべきでなく、外部に公開しない、ないしアクセス元IPアドレスの制限あるいはVPN・SSH等によるアクセスとすること、かつ内部ネットワーク等からのみアクセス可能であってもパスワードは強力なものを設定することが重要であり、可能であれば多要素認証等を導入することも検討に値します。

●証券口座乗っ取り、2か月連続で被害額増加…金融庁発表

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html
https://news.jp/i/1337732040535196594

このニュースをザックリ言うと・・・

- 9月8日(日本時間)、金融庁より、8月における「インターネット取引サービスへの不正アクセス・不正取引の発生状況」が発表されました。
- 不正アクセスの件数は4月の5,424件をピークに5月3,342件→6月1,794件→7月1,055件と減少していましたが、8月に1,248件と増加しています。
- また不正取引件数も4月の2,986件から5月2,383件→6月879件→7月894件→8月562件と推移している一方、被害額(売却・買付の合計)は4月約2,924億→5月約2,132億→6月約399億→7月約473億→8月約514億と、2か月連続で増加しています。

AUS便りからの所感

- 不正取引1件あたりの被害額も8月は約9,100万円となり、4月の約9,800万→5月約9,000万あたりに近い水準となっています。
- 同庁でもフィッシング対策やアカウント保護のため各種注意喚起を行っていますが、例えば認証に関しては「知識要素（PW、秘密の質問等）・所持要素（SMSでの受信や専用トークンで生成するワンタイムコード等）・生体要素（指紋、静脈等）のうち二以上の要素を組み合わせる」多要素認証を、「同一要素を複数回用いる多段階認証よりもセキュリティが強いとされる」として推奨しており、特に生体認証は近年スマートフォンを中心に利用環境が整っていることから、可能な限り認証のための要素に組み入れることが望ましいでしょう。