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。

●川崎重工、不正アクセスにより情報流出…2019年9月以降海外から

https://www.itmedia.co.jp/news/articles/2012/28/news075.html
https://www.jiji.com/jc/article?k=2020122800631&g=eco
https://www.khi.co.jp/pressrelease/news_201228-1j.pdf

このニュースをザックリ言うと･･･

- 12月28日(日本時間)、川崎重工業より、国内拠点が社外からの不正アクセスを受け、一部情報が流出した可能性があると発表されました。

- 発表によれば、6月11日に国内拠点のシステム監査を実施した際、タイの海外拠点から国内拠点へのアクセスが発覚したのがきっかけとしており、その後インドネシア・フィリピン・米国の海外拠点からも不正アクセスが確認されたことから、各拠点との通信制限や端末の検査等を実施したとしています。

- 不正アクセスは2019年9月から発生しており、国内のシステムの管理者アカウントが奪取されていたとも報じられていますが、各種セキュリティ対策により、2020年8月以降は国内への不正アクセスが発生していないことを確認、同11月30日以降海外拠点の接続を再開し、通信に異常がないことを確認したとしています。

AUS便りからの所感等

- 同社では、不正アクセスは「痕跡を残さない高度な手口による」もので、発表の時点では「内容不明の情報が外部に流出した可能性」が確認された段階であり、個人情報を含め、社内からの情報流出に関して特定できた事実はないとしており、詳細・全容については今後の続報が待たれるところです。

- 今回の事例は異なるでしょうが、拠点間のアクセス、特にVPN経由でのアクセスについて、利便性をとって同一LANからのアクセス並みに制限を緩めている、ないし行っていないケースは依然多いとみられ、この場合一つの拠点への侵入がたちどころに他の全拠点への攻撃に繋がる恐れがあります。

- 拠点間の通信のみならず、拠点内の複数のLAN間の通信においても、不必要な接続を制限するよう設定が行われているか、随時確認することが重要です。

ITmedia NEWS

川崎重工に不正アクセス、一部情報流出の恐れ　「痕跡がなく、高度な手口によるもの」

2020年12月28日 15時47分 公開　[ITmedia]

川崎重工業は12月28日、同社の海外拠点から日本国内のデータセンターへ不正アクセスがあり、一部の情報が外部に流出した可能性があると発表した。

同社は6月、社内で実施したシステム監査で、本来は発生しないタイ拠点から日本国内のデータセンターへのアクセスを発見。同日中に不正アクセスと判断して通信を遮断した。その後、インドネシア、フィリピン、米国の各拠点からも不正アクセスがあったと判明したため、各拠点との接続を遮断、または通信を制限したという。

●年末年始を狙った不正アクセスも…個人情報流出、不正メール送信相次ぐ

https://www.itmedia.co.jp/news/articles/2101/05/news051.html
https://www.itmedia.co.jp/news/articles/2101/05/news057.html
https://www.itmedia.co.jp/news/articles/2101/06/news082.html

このニュースをザックリ言うと･･･

- 2021年初頭、国内の複数の組織等におけるメールシステムへの不正アクセス事案が相次いで発表されています。

- 1月4日(日本時間)、愛知県で開催される国際芸術祭「あいちトリエンナーレ」実行委員会より、同委員会が管理運営するメール配信システムが同3日午前に不正アクセスを受け、登録されていた約3,500件分のメールアドレス・氏名等の流出および外部へのなりすましメール送信が発生したと発表されました。

- 同日には愛媛大学より、学生2名のメールアカウントが昨年11月末に不正アクセスを受け、外部へ約35,000件の迷惑メールが送信されたと発表されました。

- 1月5日には、「リラックマ」の会員制ファンサイト「いつでもリラックマ」の運営元より、2020年12月30日に同サイトが不正アクセスを受け、105,180件分のメールアドレスが流出したと発表されています。

AUS便りからの所感

- 前述のうち2件は年末年始に不正アクセスが発生しており、監視が薄くなっていたところを狙った攻撃であった可能性が高いです。

- Webメールも提供するメールサービスの場合、内外への迷惑メール送信のみならず、保存されている送受信メールやアドレス帳のメールアドレスが閲覧されるリスクがあることを意識し、多くのサービスで提供している多要素認証を可能な限り有効にすることを推奨致します。

- 愛媛大学の事案は、学生が利用する外部サービスから不正アクセスで奪取されたメールアドレス・パスワードの悪用による、いわゆる「リスト型攻撃」の一環とみられますが、アカウントの保護に際しては、「複数のサービス間でパスワードを使い回していないか」だけでなく、「推測しやすい安易なパスワードを使用していないか」についても注意が必要です。

ITmedia NEWS

あいちトリエンナーレに不正アクセス　個人情報漏えいの恐れ

2021年01月05日 12時11分 公開　[ITmedia]

愛知県の芸術祭「あいちトリエンナーレ」の実行委員会は1月4日、同組織が管理、運営するメール配信システムへ不正アクセスがあったと発表した。なりすましメールが送信された他、システムに登録されていた約3500件分のメールアドレス、氏名などが流出した可能性があるという。

●12月のフィッシング報告件数、対策協議会より発表…1年で約4倍に

https://www.antiphishing.jp/report/monthly/202012.html

このニュースをザックリ言うと･･･

- 1月6日(日本時間)、フィッシング対策協議会より、2020年12月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 11月度の報告件数は32,171件で、11月度(https://www.antiphishing.jp/report/monthly/202011.html)の30,967件より1,204件増加、また2019年12月度(https://www.antiphishing.jp/report/monthly/201912.html)の8,208件から4倍近くへの増加となっています。

- Amazonを騙ったフィッシングの報告が全体の50.0%と最も多く、三井住友カード・楽天・アプラス(新生銀行カード)・MyJCBを加えたものが報告全体の約86.0%を占めていたとのことです。

- フィッシングに悪用されたブランド件数63件(11月度も同様)のうち、クレジット・信販系が16、金融機関系が18となっており、特に信販系・地方銀行を騙るフィッシングが増加しているとのことです。

AUS便りからの所感

- 11月度に比べ、報告全体におけるAmazon(11月度62.3%)および上位5ブランド(同90.1%)の割合が下がっており、また同協議会からのフィッシング注意喚起においてもこれまで悪用されていなかったブランドのクレジットカードに関するものが目立ってきています(AUS便り 2020/12/21号参照)。

- 今月は緊急事態宣言の再発令への便乗、あるいは10月にも確認された「特別定額給付金の第二弾」を騙るフィッシング等が発生することが考えられ、政府機関の公式サイトやSNS等から随時の情報収集を行い、また利用しているサービスの公式サイトへはブックマークからアクセスする等の防御策をとっていくことを引き続き心がけてください。

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