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。

●年末年始における情報セキュリティに関する注意喚起、JPCERT・IPA呼びかけ

https://www.jpcert.or.jp/pr/2017/pr170003.html
https://www.ipa.go.jp/security/topics/alert291221.html

このニュースをザックリ言うと・・・

- 多くの企業が長期休暇となる年末年始を迎えるにあたり、12月18日（日本時間）にJPCERT/CC、同21日にはIPAより、情報セキュリティに関する注意喚起が出されています。

- システム管理者が長期間不在になることにより、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまう可能性、および従業員等が友人や家族と旅行に出かけた際の、SNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- 両組織とも、今回特に注意すべき攻撃として、実在の企業の業務メール等をかたり「URSNIF(Gozi)」等の情報詐取型マルウェアをばらまく攻撃を挙げており、特に休暇明けにおいては大量のメールがたまっている可能性があることから、不審なメールから添付ファイルを開いたり、書かれたURLにアクセスしないよう注意することを呼び掛けています。

- またJPCERT/CCでは、もう一つのトピックとして「リスト型攻撃」を挙げており、Webサービス等のユーザに対しパスワードの使い回しを行っていないか注意を促す他、管理者に対しても「緊急時の対応体制の確認」「不正ログイン等の異常検知・自動遮断の設定」「管理しているアカウントの確認」「システム管理部門以外で管理しているWebサービスの確認」を行うよう呼び掛けています。

AUS便りからの所感等

- セキュリティ機関の呼びかけにおいては、組織内のシステム管理者やユーザに対し、休暇前・休暇中および休暇明けにとるべき対策のポイントが挙げられており、情報システムとインターネットを組織内外で利用する者として、「普段から」セキュリティを意識した慎重な行動をとることを改めて示す以外にも、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。

- UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有がそういった攻撃による被害を最小限に抑えられるために大切なことと言えます。

- もしこのAUS便りを連休明けにご覧になったとしても、その時点で点検すべきことは多く存在し、以後もゴールデンウィークや夏季といった長期休暇に備えて、準備・点検を行うよう意識して頂ければ幸いです。


長期休暇に備えて 2017/12
最終更新: 2017-12-18
ツイート　メール
2017年12月18日
一般社団法人 JPCERTコーディネーションセンター (JPCERT/CC)
<< 長期休暇に備えて 2017/12 >>
冬の長期休暇期間におけるコンピュータセキュリティインシデント発生の予防および緊急時の対応に関して、要点をまとめましたので、以下を参考に対策をご検討ください。
年末年始の休暇期間中は、インシデント発生に気づきにくく、発見が遅れる可能性があります
者への連絡方法などを事前に調整し、休暇明けには、不審なアクセスや侵入の痕跡がないか、

図 1：情報窃取を目的とした不審なメールを用いた攻撃例
図 2：パスワードリスト型攻撃例


IPA Better Life with IT 情報処理推進機構
年末年始における情報セキュリティに関する注意喚起
最終更新日：2017年12月21日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

多くの人が年末年始の長期休暇を迎えるにあたり、IPAが公開している長期休暇における情報セキュリティ対策をご案内します。

長期休暇の時期は、「システム管理者が長期間不在になる」、「友人や家族と旅行に出かける」等、いつもとは違う状況になりやすく、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまったり、SNSへの書き込み内容から思わぬ被害が発生したり、場合によっては関係者に対して被害が及ぶ可能性があります。

また、ここ数ヶ月の間、実在の企業を騙った不審なメールに関する相談が多く寄せられています。長期休暇明けはメールが溜まっていることが想定されますので、誤って不審なメールの添付ファイルを開いたり、本文中のURLにアクセスしたりしないように注意してください。

これらのような事態とならないよう、「長期休暇における情報セキュリティ対策」に、(1)組織のシステム管理者、(2)組織の利用者、(3)家庭の利用者、のそれぞれの対象者に対して実施すべき対策をまとめています。また、長期休暇に限らず、日常的に実施すべき情報セキュリティ対策も「日常における情報セキュリティ対策」として公開しています。被害に遭わないためにもこれらの対策の実施をお願いします。

2017年に起きたサイバー攻撃の中から、標的型サイバー攻撃に関わる活動の概要とそのトピックを下記にご紹介します。

●JALが「振り込め詐欺」被害…詐欺メールに3.8億円送金

http://itpro.nikkeibp.co.jp/atcl/column/14/346926/122001256/

このニュースをザックリ言うと・・・

- 12月20日（日本時間）、日本航空（JAL）より、8～9月に取引先を装った2件の詐欺メールによって、同社が3.8億円を騙し取られる被害を受けたと発表されました。

- 発表によれば、8月24日と9月7日に米国の貨物事業所における地上業務委託料計21.6万ドル（約2400万円）、9月27日に海外の金融会社からリースしている旅客機のリース料約325.5万ドル（約3億6000万円）をそれぞれ香港の銀行にある偽の口座に送金したとしています。

- いずれも取引先の担当者になりすましたメールで「偽の口座」への変更が指定されたものとされています。

AUS便りからの所感等

- 発表では、前述のうち1件目は「正規の取引先とは別のメールアドレスから詐欺メールが来た」上に「口座変更について確認したところ、正規の取引先から『変更は事実』と返事が来た」こと、2件目については「送信元が通常やり取りしている取引先の名前・メールアドレスだった」「正規の請求書の『訂正版』として振込先を変更したPDFファイルが送られてきた」ことから、それぞれ信じ込んだものとされています。

- いわゆる「ビジネスメール詐欺」は今年に入り国内でも問題とされ、IPAや大手銀行等が注意喚起を行っており、今回のような大企業が億単位の被害を受けたという衝撃の大きさの一方で、小企業であっても、普段のメールのやりとりを盗み見るなど綿密な準備のもと詐欺が行われる可能性は決して皆無ではありません。

- ビジネスメール詐欺への対応にあたり、UTM等のIT面での防御のみで根本的な対策が行えるものではありませんが、侵入の防止やメールにおける詐称の検出等、あくまで詐欺の各段階での攻撃を遮断できる可能性はあり、送金判断時あるいは送金後においても、詐欺と感知した場合に即座に連絡する等の対策マニュアルを用意しておくべきでしょう。

●大学で不正アクセス相次ぐ…大阪大から個人情報約8万件流出、放送大学から迷惑メール14万件以上送信

http://www.itmedia.co.jp/news/articles/1712/13/news113.html
http://itpro.nikkeibp.co.jp/atcl/news/17/121402867/

このニュースをザックリ言うと・・・

- 12月13日（日本時間）、大阪大学と放送大学がそれぞれ不正アクセスを受けたことを相次いで発表しています。

- 大阪大学については、5月～7月にかけて教育用計算機システムが不正アクセスを受け、職員・学生計69549件のユーザ情報が流出、また学内グループウェアのメールに含まれる学内外関係者11558件の個人情報が流出した可能性があるとされています。

- 放送大学については、10月27日～11月8日の間にメールサーバのアカウントが不正利用され、学外へ迷惑メールが14万3000回送信されたとされています（他のサーバへの侵入や個人情報の流出はないとされています）。

AUS便りからの所感等

- 大阪大学の件では、ある教職員アカウントが不正ログインされ、システムに不正プログラムを仕掛けられ、管理者IDが盗まれたとされており、一方の放送大学でもパスワードが脆弱なアカウントが悪用されたものとなっています。

- また放送大学では6月にも同様の事件が発生しており、そのときは使わなくなり削除されないまま残っていたアカウントが悪用されたことが原因でした。

- いずれも、権限を持たない一般のアカウントが悪意を持つ攻撃者に乗っ取られたことがきっかけで発生したものとされますが、こういった不正ログインを防止すること、および不正ログイン後の不正行為によって内外に脅威をもたらされることを食い止めること、いずれの観点においても適切なセキュリティ対策をとることがシステムをより強固なものとするでしょう。