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。

●冬期の長期休暇へ向け備えを･･･JPCERT/CC

http://news.mynavi.jp/news/2015/12/19/090/
https://www.jpcert.or.jp/pr/2015/pr150006.html

このニュースをザックリ言うと･･･

- 12月17日（日本時間）、セキュリティ専門機関JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center、JPCERT/CC）より、「冬期の長期休暇に備えて 2015/12」と題し、年末年始の休暇期間へ向けた情報セキュリティインシデント発生の予防や発生時の対応などの要点が公開されました。

- 記事では、年末年始の休暇期間中はインシデント発生に気がつきにくく、発見が遅れる可能性があることから、休暇明けにサーバのログから不審なアクセスや侵入の痕跡を確認する手順や、休暇期間中に発生したインシデントへの対応体制、関係者への連絡方法などを事前に調整しておくこと等が推奨されています。その中でも具体的に次の点（下記参照）に関して注意を呼びかけています。

AUS便りからの所感等

- 年末年始はもちろん、ゴールデンウィークや夏期休暇といった長期休暇で発生し得るインシデントへの対応体制は、その直前に準備を始めるのではなく、普段から文書化や各社員での意識合わせ等をしておくことが肝要です。

- クライアントPCの各ソフトウェアを最新に保つことは言うまでもありませんが、意識が及びにくい可能性もあるサーバ、さらにはUTMをはじめとするネットワークアプライアンス等においても、ソフトウェア・ファームウェアが古いものから更新されていないままになっていないか、適宜確認しておくべきでしょう。

マイナビニュース

冬期の長期休暇へ向け備えを － JPCERT/CC

後藤大地　[2015/12/19]

JPCERTコーディネーションセンター(Japan Computer Emergency Response Team Coordination Center、JPCERT/CC)は12月17日、「冬期の長期休暇に備えて 2015/12」において、年末年始の休暇期間へ向けた情報セキュリティインシデント発生の予防や発生時の対応などの要点を公開した。年末年始の休暇期間は情報セキュリティインシデントが発生したとしても気づきにくく、対応が遅れやすくなる。休暇に入る前の準備や、休暇明けの作業手順などを確認しておくことが推奨されている。

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center

JPCERT CC®

トップページ
情報提供
・注意喚起
・早期警戒
・脆弱性対策情報
・Weekly Report
・インターネット定点観測
インシデントの報告
各種登録
制御システムセキュリティ
ラーニング
公開資料
イベント
プレスリリース
JPCERT/CC
公募・入札情報

冬期の長期休暇に備えて 2015/12

各位

<<< 冬期の長期休暇に備えて 2015/12 >>>

JPCERT/CC
2015-12-17

冬期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がつきにくく、発見が遅れる可能性があります。休暇明けにサーバのログから不審なアクセスや侵入の痕跡を確認する手順や、休暇期間中に発生したインシデントへの対応体制、関係者への連絡方法などを事前に調整しておくことをお勧めします。

JPCERTコーディネーションセンターでは、具体的に次の点に関して注意を呼びかけています。

◆SNSやクラウドサービスなどのアカウント連携機能による情報漏洩への対策
（メール内容の確認について）
覚えのない友達紹介などのメールには注意し、送信元、メールアドレス、本文等を確認することを推奨します。また、安易にファイル内のリンクや添付ファイルを開かないことが大切です。不審に思った場合は、メール以外の方法でも確認することをお勧めします。

◆利用しているソフトウェアを最新のバージョンへアップデート
（特に以下のものに注意）
Adobe Acrobat/Reader
Adobe Flash Player
Microsoft Office
Microsoft Windows

◆情報セキュリティインシデント発生時の連絡網の整備と確認

◆年末年始の休暇中に動作させる必要のない機器の電源を落とす

◆重要なデータのバックアップの実施

◆推測されやすい安易なパスワードを変更
（特に以下の点に注意）
容易に推測できる文字列（名前、生年月日、電話番号、アカウントと同一のものなど）や安易な文字列（12345、abcde、qwert、passwordなど）を設定していないか確認する

●セキュアなパスワードの作り方とは？

http://news.mynavi.jp/news/2015/12/25/243/

このニュースをザックリ言うと・・・

- 12月24日（米国時間）、ITニュースサイトfossBytesにおいて、安全度の高いパスワードを作成する方法および注意点に関する記事が掲載されました。

- 記事では、「小文字だけを使っている」「自分やペットの名前、自分の誕生日、一般的な名詞を使っている」「長さが6文字以下」「辞書に掲載されている単語を結合しただけ」「以前使っていたパスワードを使い回している」等を弱いパスワードの例として挙げています。

- これに対する強いパスワードの作り方として、「大文字・小文字・数字・記号を組み合わせる」「8文字以上の可能な限り長いパスワードを使用する」「単語、スラング、名前、電子メールアドレスなどをパスワードとして使用しない」「文章をベースにしてパスワードを作成する」等を、この他の推奨事項や注意点として「LastPass・KeePass・1Password等のパスワードマネージャを使用する」ことや「付箋紙にパスワードを書き留めてディスプレイに貼るといったことはしない」等を挙げています。

AUS便りからの所感等

- 不正ログインに関しては、旧来から「簡単なパスワードを総当りで試す」もしくは「IDと同じパスワードを試す」といった方法が行われている他、2014年頃から目立ってきたトレンドとして「あるサイトで奪取したIDとパスワードを他のサイトでも試行する」ことが挙げられ、これらに対抗するためにも、アカウントに強いパスワードを設定することが求められます。

- 外部の大手サービスのみならず、自社ネットワーク上のメールサーバ等への不正ログインにも注意を怠るべきではなく、不正ログインを狙うアクセスを検知し遮断するためには、UTMによるセキュリティ機能が有効活用できるでしょう。

●サンリオ海外サイト330万件のアカウント情報が一時外部からアクセス可能な状態に

http://internet.watch.impress.co.jp/docs/news/20151224_736803.html

このニュースをザックリ言うと・・・

- 12月22日（米国時間）、サンリオの海外ファン向けサイト「サンリオタウン」を運営するSanrio Digital社は、同サイトの会員情報330万件が外部からアクセス可能な状態にあったことを発表しました。

- この問題は、同19日に米国セキュリティニュースサイトCSO Onlineが個人情報漏洩の可能性を指摘していたもので、会員の氏名・生年月日・性別・メールアドレス・ハッシュ化されたパスワード等にアクセス可能だったとされています（クレジットカード情報やその他の支払い情報は含まれていなかった模様です）。

- Sanrio Digital社の発表では、会員情報のデータベースサーバの設定ミスが問題の原因としており、会員情報が悪意ある第三者に盗まれた形跡は一切ないとのことですが、サンリオタウンのパスワードおよび同様のパスワードを設定している他のオンラインサービスのパスワードを変更するよう呼び掛けています。

AUS便りからの所感等

- 「サーバの設定ミス」に関してより厳密に言うと、データベースソフトウェア「MongoDB」が使用するサービスポートに外部からアクセス可能であった模様です。

- 内部のデータベースを含め、不特定多数への公開を意図していないサービスへのアクセスをサーバ自身もしくはルータ・UTMのファイアウォール機能により遮断・制限することは、サーバを堅牢なものとするために不可欠なものです。

- また、外部からのあらゆるアクセスについてログを取得することも、不正アクセスの有無やアクセス元の分析を確実かつ迅速に行うために重要となるでしょう。