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。

●AWS設定ミスで25万件の個人情報がGoogle検索に掲載される

https://www.itmedia.co.jp/news/articles/2207/04/news155.html
https://www.itmedia.co.jp/news/articles/2207/07/news098.html
https://www.cybaxuniv.jp/news/2022/20220701

このニュースをザックリ言うと･･･

- 7月1日(日本時間)、リスクモンスター社より、同社運営の企業向け研修サービス「サイバックスUniv.」のサーバーに保存されていた個人情報が誤って公開状態となり、Googleの検索結果に掲載されていたと発表されました。

- 対象とされるのは、当該サービス登録者約25万件の会社名・部署名および氏名で、住所・生年月日・電話番号等は含まれていないとのことです。

- 6月29日に利用者からの問合せを受けて発覚し、同日中に情報が保存されていたサーバーの停止により対策を行っています。

- 2020年2月16日にサーバーの設定変更を行って以降、当該情報が公開状態にあったとしていましたが、その後7月5日の続報において、サーバーをAWSに移行した際のネットワーク誤設定が原因と発表されています。

AUS便りからの所感等

- 設定の誤りで公開を意図しない情報に第三者がアクセス可能な状態となる事案は過去枚挙にいとまがなく、ディレクトリ名を指定してアクセスできる極めて古典的でシンプルなケース、データベースサーバーのサービスポートが外部にオープン状態になっていたケース等様々です。

- サービスの全てのサーバーを丸ごとではなく、一部のサブシステム(サーバー)のみをAWSに移行する形をとっていたことにより、他のサーバーからのみアクセスを許可するようなアクセス制限設定の漏れが発生したものと推測されます。

- 続報では同社が実施する再発防止策としてパブリッククラウドの設定診断サービス等を定期的に受けること等が挙げられており、オンプレミス上・クラウド上に拘わらず、外部からサーバーやネットワークにアクセス可能な設定になっていないか、第三者視点さらには攻撃者視点によるネットワーク診断の実施は重要と言えます。

ITmedia NEWS

個人情報25万件が"Google検索で丸見え"のリスクモンスター、原因はAWS移行時の設定ミス

2022年07月07日 11時07分 公開　[ITmedia]

印刷　366　Share　B!　48

企業向け研修サービス「サイバックスUniv.」のサーバに保存していた約25万人分の個人情報がGoogleで検索できる状態になっていた件を巡り、提供元のリスクモンスターは7月5日、原因はネットワークの設定ミスだったと発表した。過去にサーバをAWS移行した際、設定変更があったところ、チェック体制に不備がありミスにつながったという。

6. 原因
・直接の原因は、本件サーバーの環境変更時のネットワーク誤設定によるものでございます。
・本件サーバーは、サイバックス Univ.のサブシステムであり、サブシステム単位での個人情報の洗い出しが不十分であったうえ、セキュリティ対応の見直しもされていませんでした。
・本件サーバーが外部からアクセス可能となったきっかけとなるサーバー設定変更とは、サーバーの AWS 移行に伴う設定変更ですが、当社が初めて独自で AWS へ移行したサーバーにも関わらず、チェック体制が不十分でした。

トラブルの原因（リスクモンスターの発表から引用）

情報がGoogleで検索可能になっていたサーバは、サイバックスUniv.のサブシステム（システムの一部を構成する小規模なシステム、または予備や代替のシステム）の運用に使っていたもの。リスクモンスターによれば、サブシステムが抱える個人情報の洗い出しが不十分だった他、当時のサーバ移行が同社にとって初めて、

●ドラッグストアECサイト等に「リスト型攻撃」…個人情報19,057件流出か

https://www.itmedia.co.jp/news/articles/2207/12/news115.html
https://www.sundrug.co.jp/news/news_20220711_01.pdf

このニュースをザックリ言うと･･･

- 7月11日(日本時間)、ドラッグストア大手のサンドラッグ社より、同社が運営するECサイト等において不正ログインが発生し、個人情報等が流出した可能性があると発表されました。

- 被害を受けたとされるのは、「サンドラッグe-shop本店」および「サンドラッグお客様サイト」の会員19,057件の個人情報(氏名・住所・電話番号・メールアドレス・生年月日・購入履歴・保有ポイントおよびクレジットカード番号の一部とのことです。

- 7月9日から同11日にかけて、外部のサービスから流出したメールアドレス・パスワードによる、いわゆる「リスト型攻撃」が海外のIPアドレスから行われており、対象となる会員全員にパスワードを変更するようメールで連絡を行ったとしています。

AUS便りからの所感

- 不正ログインを行っていたとする海外からのアクセスは既に遮断されており、第三者機関を踏まえたセキュリティ対策を講じたとしています。

- サイト自体の脆弱性等を突かれなかったとしても、リスト型攻撃が既に効率的で大規模な情報奪取の手段として定着している今日において、単にIDとパスワードだけでログインが可能な状態というのは見方によっては危険なものとも言え、登録されたメールアドレスや携帯電話番号へのワンタイムパスワード送信から、スマホアプリ等を用いた二段階認証ないし多要素認証まで、何らかの本人確認手段を提供すること、またユーザー側でも推測されにくいパスワードの使用・複数のサービスでパスワードを使い回さないといった鉄則とともに先に挙げた多要素認証を可能な限り活用することにより、アカウントの確実な保護を心掛けるべきでしょう。

ITmedia NEWS

サンドラッグにリスト型攻撃　個人情報・クレカ情報など1万9000件流出の可能性

2022年07月12日 12時05分 公開　[ITmedia]

印刷　329　Share　B!　9

サンドラッグは7月11日、ECサイト「サンドラッグ e-shop 本店」やクーポンなどを配信する「サンドラッグお客様サイト」が不正ログインを受け、個人情報やクレジットカード情報の一部など計1万9057件が流出した可能性があると発表した。他のサービスで不正に入手したIDやパスワードの組み合わせを使ってログインを試みる「リスト型攻撃」を受けた可能性があるという。

●業務委託元の3割がUSBメモリー等での情報持ち出し認める…IPA「テレワークのセキュリティ実態調査」発表

https://news.mynavi.jp/techplus/article/20220704-2385532/
https://www.ipa.go.jp/security/fy2021/reports/scrm/index-telework.html

このニュースをザックリ言うと･･･

- 6月30日(日本時間)、IPAより、「企業・組織におけるテレワークのセキュリティ実態調査」の2021年度版の調査結果が発表されました。

- 「緊急事態宣言中またはコロナ禍により特例や例外を認めなければならないセキュリティ対策の社内規定・規定・手順等はありましたか」という設問に対し、書類あるいはUSBメモリー等電子記録媒体による機密情報の社外持ち出しを社員に認めていたと回答した企業は、委託先(ITベンダー)企業が17.2%(2020年度12.4%)に対し、委託元(ITユーザー)企業が29.0%(2020年度20.2%)となっており、特に後者については19.4%が現在もこれを認めているとしています。

- また機密情報を保存することができる会社支給PCの持ち出しについても、委託先企業の24.1%(2020年度17.8%)、委託元企業の33.5%(2020年度26.9%)が認めていたとする結果が出ています。

AUS便りからの所感

- 6月23日に兵庫県尼崎市から委託されたITベンダー企業が市民の個人情報を記録したUSBメモリーを一時紛失する事案が発生しており(AUS便り 2022/06/28号参照)、IPAの発表は奇しくもそれから一週間というタイミングになりました。

- それまでに定められたセキュリティポリシーにより、オンラインでの情報の転送ができず、USBメモリーでの情報の移動を行わざるを得ないケースも多々あるとみられますが、いずれにしろこれが常態化している限り情報漏洩のリスクが増大し得ることをIPAでは指摘しており、より安全な情報へのアクセスのためのシステム構築と、それを実現するためのルールの見直しは今後重要となってくるでしょう。

マイナビニュース

IPA、テレワークセキュリティの調査結果公開 - 特例や例外でリスク増

2022/07/04 11:18　著者：後藤大地