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。

●大手レコードチェーン店のECサイトが不正アクセス、個人情報70万件流出か…平文パスワードも

https://www3.nhk.or.jp/news/html/20220629/k10013694311000.html
https://diskunion.net/

このニュースをザックリ言うと･･･

- 6月29日(日本時間)、CD・レコードチェーン店を運営するディスクユニオン社より、同社運営のECサイトが不正アクセスを受け、利用者の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、「diskunion.net」「audiounion.jp」に登録した利用者最大約701,000件分の個人情報(氏名・住所・電話/FAX番号・Eメールアドレス・ログインパスワードおよび会員番号)とされています(クレジットカード情報は保有しておらず、流出の対象ではないとのことです)。
- 6月24日に外部からの情報提供によって情報漏洩の可能性を確認しており、同日のうちに各サイトを停止、同28日までに個人情報保護委員会および警察に被害を報告したとしています。

AUS便りからの所感等

- 流出した情報にログインパスワードが含まれていますが、ハッシュ化した状態ではなく平文で保存されていたとのことで、いわゆる「リスト型攻撃」のターゲットとなるのは確実とみられ、万が一同じパスワードを他のサイトで使い回していた場合は、より速やかに推測されにくいパスワードへの変更が必要となります。
- 各サイトは7月5日現在も休止中で、情報流出の経路も現時点では明らかになっておりませんが、その原因の判明と再発防止策が適用され次第再開予定とされています。
- ECサイトを運営する各組織においては、今後発表されるであろうより詳細な報告をもとに、自サイトにおいて適切な対策をとっているかの点検とさらなる対策の適用を行うことを推奨致します。

NHK

「ディスクユニオン」 70万人余の会員の個人情報 漏えいか

2022年6月29日 18時25分

CDやレコードなどの専門店を展開する「ディスクユニオン」は、運営する2つのオンラインショップに登録している70万人余りの会員のメールアドレスとパスワード、それに名前や住所などの個人情報が漏えいしたおそれがあると発表しました。

東京 千代田区に本社がある「ディスクユニオン」によりますと、漏えいしたおそれがあるのは、CDなどを販売する「diskunion.net」と、オーディオ機器などを販売する「audiounion.jp」の2つのオンラインショップのおよそ70万1000人分の会員情報です。

この会員情報には、名前や住所、電話番号のほか、メールアドレスや暗号化されていないパスワードなどが含まれていて、今月24日までに登録したすべての会員のものが対象だということです。

●6月度フィッシング報告件数88,250件、フィッシングサイトURL件数は過去最高の27,217件

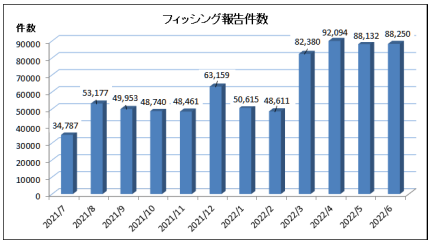
https://www.antiphishing.jp/report/monthly/202206.html

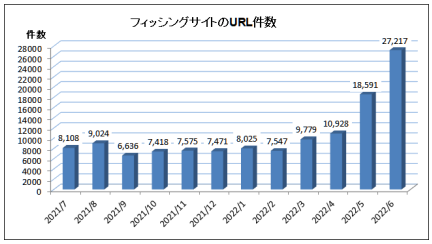
このニュースをザックリ言うと・・・

- 7月5日(日本時間)、フィッシング対策協議会より、6月に寄せられたフィッシング報告状況が発表されました。
- 6月度の報告件数は88,250件で、5月度(https://www.antiphishing.jp/report/monthly/202205.html)の88,132件から微増し、4か月連続で8万件以上を記録しています。
- フィッシングサイトのURL件数は27,217件で、5月度の18,591件から8,626件の急増となり、過去最高を引き続き更新しています(ただしIPアドレスが同一のものが多いとされています)。
- 悪用されたブランド件数は100件(5月度 110件)でこちらも4か月連続で100件以上となり、報告全体に対するブランドの割合についてはAmazonが18.3%と最も多く、これとイオンカード、えきねっと(JR東日本)、auおよびau PAY、の4ブランドで併せて約40.2%を占めているとのことです。

AUS便りからの所感

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





- 月々のフィッシング報告件数の水準は1年以内のスパンで増加をみせており、今後も9万件以前後の水準で推移し続けるとみられます。
- 同協議会の調査用メールアドレス宛に届いたフィッシングメールについては、メール差出人として正規のメールアドレスを不正に使用する「なりすまし」メールが約69.5%となっている一方、受信検知・防止機構のうちSPF(送信ドメイン認証)において「hardfail(認証失敗により廃棄)」と検出できたメールは約23.4%(5月度 約7.1%、4月度 約37.1%)と再上昇、ただし「softfail(認証は失敗したがメールは受信する)」と検出したメールは約25.0%(5月度 約49.7%、4月度約31.7%)と減少しており、また同じく受信検知・防止機構であるDMARCに関しては、対応しているメールサービスの利用者からの報告が増えていることから、ポリシー設定が「none(検証に失敗してもメールは受信する)」のまま運用され続けているドメイン名(ブランド)が悪用されている可能性が示されています。
- 既にSPFを採用・設定している組織において、自社ドメイン名のなりすましメールによる被害をさらに防ぐことを考慮するならば、より厳密なSPFポリシーの設定や、加えてDMARCの採用も検討に値しますが、一方で正規のメールサーバーを介して外部にEmotetをはじめとしたマルウェアメールが送信される恐れにも注意し、PC・UTMあるいはメールサーバー側におけるメール送受信時のウイルススキャンやその他のソリューションの導入も怠りなく行うべきでしょう。

●大学Q＆Aシステムに「ブラインドSQLインジェクション」による不正アクセス…メールアドレス2,086件漏えいか

https://www.itmedia.co.jp/news/articles/2206/28/news190.html
https://www.nagoya-u.ac.jp/info/20220628_icts.html

このニュースをザックリ言うと・・・

- 6月28日(日本時間)、名古屋大学より、同大学が運営するQ&Aシステム(情報システムに関する問い合わせシステム)が不正アクセスを受け、メールアドレスが漏洩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、質問時に連絡先として記載され、システムに保存されていたメールアドレス2,086件とされています。
- 5月10日・14日および15日に、「ブラインドSQLインジェクション」の脆弱性を突いた不正アクセスが発生していたことが同16日にシステムのログから確認されており、同日中に脆弱性の修正を行ったとしています。

AUS便りからの所感

ITmedia NEWS

- ブラインドSQLインジェクションは、SQLインジェクションの中でも特に「不正な入力によるWebサーバー側の微細な応答・動作の変化から、不正なSQLコマンドの実行が可能なパターンを推測する」ものを指し、データベースへの不正なアクセスが可能かの確認まで比較的手間がかかるものとなります。
- SQLインジェクション全般に対する根本的対策として、Webアプリケーション内でのSQLコマンド実行の際にプリペアードステートメント(プレースホルダー)の利用ないし入力内容の確実なエスケープが重要であり、脆弱性を入れ込んでしまった後から発覚・修正するのが困難とならないよう全ての場面においてこの対策を確実に実行すること、加えて可能な限り脆弱性を悪用せんとする不正なアクセスパターンを遮断できるようWAFの設置等を行うことが重要です。

名古屋大学に不正アクセス　「ブラインドSQLインジェクション」攻撃でメアド2086件漏えいか

2022年06月28日 18時00分 公開　[ITmedia]

印刷　435　Share　B!　30

名古屋大学は6月28日、情報システムに関する質問を受け付けるシステムが不正アクセスを受け、メールアドレス2086件が漏えいした可能性があると明らかにした。攻撃対象サーバの挙動を分析して内部情報を探る「ブラインドSQLインジェクション」を受けたとしている。

令和4年5月16日（月）、Q＆Aシステムのログを確認したところ、第三者から攻撃を受けていたことが判明しました。この攻撃は5月10日（火）4時27分から10時35分の間、及び5月14日（土）11時14分から5月15日（日）8時45分の間であり、アクセスログ解析の結果、当該システムに保存されていた、質問時に連絡先として記載されたメールアドレスが2,086件漏洩した可能性があります。

不審なアクセスの報告を受けた日に、プログラムを修正することにより当該システムの脆弱性を解消いたしました。現時点では、閲覧されたメールアドレスが悪用された事実は認められておりません。

漏洩した可能性のある方々には、登録されていたメールアドレスにメールにて事実関係をご説明するとともに、対応窓口の設置及びその連絡先をお伝えし、お詫び申し上げたところです。

被害の経緯と詳細