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。

●Webサイトへの「SQLインジェクション攻撃」、メールアドレス約128,000件流出

https://scan.netsecurity.ne.jp/article/2021/09/29/46361.html
https://www.logovista.co.jp/Iverp/information/information/emergency.html

このニュースをザックリ言うと･･･

- 9月24日(日本時間)、翻訳ソフト等の開発・販売を行うロゴヴィスタ社より、同社Webサイトが不正アクセスを受け、ユーザーのメールアドレスが流出したと発表されました。

- 被害を受けたとされるのは、同社へのユーザー登録・問合せフォームの利用および直販サイトからの購入を行ったユーザーのメールアドレス約128,000件とされています(名前・住所およびクレジットカード情報等は影響を受けていないとのことです)。

- 同24日にユーザー宛に迷惑メールが届いたとの問合せを受けて調査を行ったところ、Webサイトに対するSQLインジェクション攻撃により、メールアドレスが奪取されたとされています。

AUS便りからの所感等

- WebアプリケーションにSQLインジェクション攻撃が可能になる脆弱性が存在する場合、内部のデータベースサーバーにアクセスされ、データを奪取されるのみならず、改ざん・消去・破壊等も行われる恐れがあります。

- Webサイト・ECサイトの構築を容易にする著名なCMS(コンテンツ管理システム)等においても、SQLインジェクションあるいはクロスサイトスクリプティングといった、いわば古典的な脆弱性が確認され、悪用による実害が発生するケースは近年においても珍しくなく、利用においては常に最新バージョンに保つ管理体制を確実にとることが重要です。

- 加えて、脆弱性を狙った攻撃と推測されるアクセスパターンを検知・遮断するWAF(Webアプリケーションファイアウォール)や、外部へのデータの流出を検知する出口対策のためのソリューションを設置することにより、万が一未修正・未発見のいわゆる「ゼロデイ脆弱性」を突かれた場合にも攻撃や情報漏洩の成功率を抑制することに繋がるでしょう。

LOGOVISTA

■弊社ホームページへの不正アクセスによる被害発生のお詫びとお知らせ

2021.09.24 掲載
2021.09.30 更新

平素はロゴヴィスタに格別のお引き立てを賜り、誠にありがとうございます。

この度、ロゴヴィスタ株式会社(代表取締役社長:小宮善維)は、弊社ホームページに対し第三者による不正アクセスがあり、結果として、お客様のメールアドレス情報が不正に取得されていた事実を確認致しました。
お客様および関係者の皆様に多大なるご迷惑とご心配をおかけする事態となりましたこと、心よりお詫び申し上げます

被害の対象は、お客様が弊社ホームページ(弊社直販サイトを含みます)で、ご入力を頂きましたメールアドレスとなり、お名前・ご住所・クレジットカード情報等のメールアドレス以外の情報は被害の対象には含まれておりません。

お客様および関係者の皆様に多大なご迷惑とご不安、ご心配を生じさせる事態となりましたことを深くお詫び申し上げますとともに、本被害をお知らせさせていただきます。

●ドコモ騙るSMSフィッシングで約1,200人が不正決済被害…総額1億円に

https://www.jiji.com/jc/article?k=2021100200476&g=eco
https://www.nttdocomo.co.jp/info/notice/page/211002_00.html

このニュースをザックリ言うと・・・

- 10月2日(日本時間)、NTTドコモより、同社を騙るSMSによるフィッシング詐欺による不正な決済が発生しているとして注意喚起が出されています。

- 注意喚起によれば、「ドコモお客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です」といった文面のSMSから「NTTセキュリティ」「NTT DOCOMOセキュリティセンター」を装う不正なアプリのインストールおよびネットワーク暗証番号の入力を促すことにより、ユーザーが意図しない不正な決済を行うとしています。

- ドコモオンラインショップからApp Store & iTunesギフトカード等が不正に購入され、被害は約1,200人・約1億円に上っているとされていますが、これに対し同社では被害全額を補償するとしています。

AUS便りからの所感

- NTTドコモを騙るフィッシングは、9月14日にもフィッシング対策協議会より、dアカウントの奪取が目的とされるものについて注意喚起が出されています(https://www.antiphishing.jp/news/alert/nttdocomo_20210914.html)。

- 同社でも、これまでに度々発生しているフィッシングへの注意喚起等をまとめたページを用意しています(https://www.nttdocomo.co.jp/info/anti-phishing/)ので、特に同社ユーザーにおいては随時参照することを強く推奨致します。

- この他にも、不審なメール・SMSの受信時には、携帯電話キャリア各社や大手サービスあるいはフィッシング対策協議会をはじめ啓発を行っている団体の情報を速やかに参照し、フィッシングの可能性を確認できるようにし、普段利用する各サービスの正規のWebサイトをブックマークに登録し、そこからアクセスするような体制を整えることが肝要です。

JIJI.COM

ドコモ、利用者が１億円詐欺被害　フィッシングで１２００人

2021年10月02日22時44分

ＮＴＴドコモの看板

ＮＴＴドコモは２日、同社をかたるショートメッセージが利用者のスマートフォンに届き、暗証番号の入力を求められギフトカードなどを不正に購入される「フィッシング詐欺」の被害が発生したと発表した。被害は約１２００人、合計で約１億円に上り、同社が全額を補償する。

「密」避け特殊詐欺　自宅で活動、容疑で６人逮捕一警視庁

ドコモによると、「ドコモお客様センターです。ご利用料金のお支払い確認が取れておりません。ご確認が必要です」などと書かれたショートメッセージが届いた。

●パスワードに関する意識調査、回答者の65%が依然複数アカウントで使い回し

https://japan.zdnet.com/article/35177142/
https://blog.lastpass.com/2021/09/new-report-2021-psychology-of-passwords/

このニュースをザックリ言うと・・・

- 9月22日(現地時間)、パスワード管理ツールを提供する米LastPass社より、米・英・ドイツ・フランス・インド等7ヶ国の3,750人のITプロフェッショナルに対し行った、パスワードに関する意識調査の結果をまとめたレポートが発表されました。

- 同じパスワードを複数のWebサービス等のアカウントで使い回す行為について、回答者のうち92%はリスクがあることを承知しているものの、65%は依然使い回しを行っているとの結果が出ています。

- この他、金融機関に関するアカウントに強力なパスワードを設定するとした回答者は68%に上った一方で、仕事関係のアカウントについて実施しているのは32%に留まった、等の結果も出ています。

AUS便りからの所感

- いわゆる「リスト型攻撃」による複数のサイトでの不正ログインが国内外で話題となって数年が経過し、「推測されにくいパスワードを設定する」「複数サイトでの使い回しはしない」よう啓発が進んだり、「定期的にパスワードを変更する」ことの安全性へ疑問が呈されたりといった動きがありましたが、2020年以降はコロナ禍でユーザーが社内外でオンラインサービスを使用する頻度が上昇したことが、再び同じパスワードを使い回す傾向への回帰に影響した可能性も考えられます。

- レポートでは、「より長く、強力で、覚えやすく、かつ攻撃者に解読されにくいパスワードを設定する」ヒントとして「一つの単語ではなく、数字や記号を含む無意味なフレーズを活用する」ことを挙げており、もしそのようなパスワードを思いつくのが難しいとしても、使い回しを行うのではなく、LastPassをはじめとした各種パスワード管理ツールにより、ランダムなパスワードを生成して使用することを強く推奨致します。

ZDNet Japan

調査

不適切なパスワード、リスクの認識高まるも使い回しなど依然多く

Liam Tung (ZDNet.com) 翻訳校正：編集部　2021-09-27 12:25

多くの人は依然として不適切なパスワードを選んでいるようだ。おそらく、人々がより一層ウェブサービスに依存するようになっているためだろう。

パスワード管理ソフトウェアを提供するLastPassが実施した、パスワードに関する行動の心理に関する調査で、多くの人が依然として複数のアカウントでパスワードを使い回していることが分かった。1つのアカウントの認証情報がハッカーに侵害されると、同じパスワードではかのアカウントも侵害されてしまう恐れがあるため、パスワードの使い回しは問題となる。そして、このことはオンラインアカウントで貧弱なパスワードを選択することに伴う多くのリスクの1つにすぎない。