滋賀県警察からのお知らせ

サイバーセキュリティ情報 CSI

事業者の皆さまに、注目のサイバーセキュリティに関する情報をお届けします。

R３年度No.４

サイバー攻撃による情報流出の事例紹介

サイバー攻撃によって個人情報等の重要な情報が流出する事案が発生しています。
個人情報の流出は、事業活動に大きな影響を及ぼすため、それぞれ厳格に管理されていますが、最近のサイバー攻撃は、高度化しており警戒する必要があります。

最近のサイバー攻撃事例

今年上半期に、公表された主なサイバー攻撃による情報漏えい事案（インターネットで公表された情報を元に作成）

業種	種別	概要等
通販	不正アクセス	オンラインショップシステムの脆弱性を突かれ、決済に関するプログラムが改ざんされた。クレジットカードに関する情報数千件が漏えいしたおそれあり。
教育	不正アクセス	予約システムの脆弱性をつかれ、予約者の個人情報約数千件が漏えいしていたおそれあり。
アプリ	不正アクセス	アプリを管理するサーバに不正アクセスの痕跡があり、調査したところ顧客の画像データ等が100万件以上漏えいしたおそれあり。
金融	不正アクセス	オンライン相談サービスのシステムの不備を悪用され、氏名、電話番号等数千件が漏えいしたおそれあり。
ゲーム	不正アクセス	ランサムウェアに感染した上、約39万人の個人情報が流出したおそれあり。

システムの脆弱性対策

- システムの脆弱性が悪用されて、不正にアクセスされるケースが発生しています。
- 脆弱性は、プログラム上の不備であり通常使用には影響を及ぼさないものが多いですが、第三者が悪意を持って不備を利用することで、システムから情報を抜き取ることができる場合があります。
- 特に、オンラインショップや予約サイト等利用者が文字を入力する仕組みを持つWebサービス（システム）は、攻撃の入り口となる側面がありますので、このようなサービスを提供している場合は注意が必要です。

◆ **脆弱性の対策は、脆弱性が発見された場合に「パッチ」と呼ばれる修復プログラムを適用することです。**
◆ **システム提供者が公開する脆弱性情報に注意して、脆弱性が発見された場合は、早急にパッチを適用するようにしましょう。**

スミッシングにご注意

スミッシングは、SMSを利用したフィッシングです。
攻撃者は、金融機関、宅配サービス、通信事業者等を装って偽サイトに誘導して、アカウントを窃取したり、不正アプリをダウンロードさせたりします。
メッセージを受信した場合は、必ず無視してください。
万が一、アプリをダウンロードしてしまった場合は、必ずアンインストールしてください。
アンインストールしないと、通信料を請求され続ける可能性があります。

お客様宛にお荷物をお届けにあがりましたが不在の為持ち帰りました。
配送物は下記よりご確認ください。
http://OOO-■■.com/

（スミッシングの例：URLをクリックすると偽サイトに誘導されます）

«注意»巧妙化する標的型メール攻撃にご注意願います。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）