滋賀県警察サイバーセキュリティ情報
サイバーコネクトSHIG@
R５年度 No. 2
今、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。

大規模国際会議開催前のサイバー攻撃に御注意ください！！

Ｇ７(主要国首脳会議)広島サミットが本年５月19日(金)から３日間の日程で開催されます。
一方で、こういった大規模で世界から注目を浴びる催しの前は、サイバー空間での脅威が大きくなる傾向にあります。
先日、滋賀県議会や大津市議会のホームページ等が閲覧できなくなったほか、その他の地方議会のホームページでも同様のトラブルが発生している模様です。これらとＧ７広島サミットとの関連は不明ですが、過去の大規模で国際的な催しの前には、様々なサイバー攻撃が実行されてきたことを考えると、現在、サイバー空間の脅威が増しているものと思われます。
県内の各事業者の皆様には、今一度、自社のセキュリティ体制を見直していただき、必要な対策を取っていただきますようお願いします。

事例1

2016(平成28)年に開催されたＧ７伊勢志摩サミットでは、国際ハッカー集団「アノニマス」による日本の企業や政府機関等を狙ったサイバー攻撃がありました。
このサイバー攻撃は、大量のデータをＷｅｂサーバに送り付け、政府機関、地方自治体、空港、水族館などのＷｅｂサイトを閲覧不能にさせるものでした。

事例2

2021(令和３)年夏に開催された東京2020オリンピックでは、大会組織委員会に対するサイバー攻撃があっただけではなく、聖火リレーの偽サイトが次々と作成され、継続視聴のための有料サイトや個人情報の入力を促すサイトへ誘引する攻撃が仕掛けられました。
世界中の方が注目するオリンピックを利用して金銭的な利益を得るための偽サイトと思われます。

必要な対策

過去の事例では、ファームウェアのバージョンアップがされずに脆弱性を狙われたり、不審なメールの添付ファイルを開封していたり、誤ったサーバ設定であった結果、サイバー攻撃を受けて被害が拡大しています。したがって、いつも紹介している基本的なセキュリティ対策を着実に実行していただくことが、サイバー攻撃を受けないための王道です。

！！確認ポイント！！

Ｗｅｂサーバの保守やＷｅｂサイトの作成、通信機器の保守などを外部に委託されている事業者の方は、Ｇ７開催前のこの機会を捉えて、業務委託先にも基本的なセキュリティ対策ができているかの確認をお願いします。
業務委託されていても、直接、業務の影響を受けるのは自社です。攻撃を受けても被害を最小限に留めるために、業務委託先にもセキュリティ対策の確認をしていただき、対策が十分ではない場合は、必要な措置をお願いします。

«CS情報SHIG@» 家庭用ルーターの不正利用に注意！

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表） 詳細は県警webページで →