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@
R４年度 No.１２
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。

サイバーセキュリティ対策の再確認を！

報道等でもご承知のとおり、今月６日夕方から、複数の我が国政府機関及び企業等のサイトにおいて閲覧障害の発生が確認されています。

こうしたインシデントが様々な機関、企業等（以下各事業者等）に対して、今後も発生する可能性が否定できないことから、各事業者等におかれましては、提供サービスの重要性などを踏まえ、適切なサイバーセキュリティ対策を確保するよう再確認をお願いいたします。

KILLNETとは

KILLNET（キルネット）は、親ロシア派のハッカー集団。ロシアによるウクライナ侵攻の際に、ウクライナを支援している国の政府機関や民間企業に対するサイバー攻撃を展開している。主な攻撃は、ウェブサイトやサーバーなどに大量のデータを送りつけ、機能停止に追い込む『DDos攻撃』。

主な対策について

今回、展開されているサイバー攻撃は、決して新しい技術ではありませんが、今後、どのような攻撃が展開されるかわかりません。各事業者等において、サイバーセキュリティ対策が適切に講じられているか、下記の対策事項を参考にこの機会に改めて確認をお願いします。

１．システム障害等を認知した際の対処手順及び情報共有体制の確認
- 対応手順及び情報共有体制の再確認
- 連絡体制の確認及び更新
- 保守業者等のサポート窓口の営業状況及び連絡先の再確認
- インシデントを認知した場合の組織内報告窓口の周知

２．監視の強化
- 今後もサイバー攻撃が行われる可能性があるため、必要に応じた体制等を含めた監視の強化
- 自社のなりすましサイト等を発見した場合は、JPCERT/CCなどの専門機関へ連絡

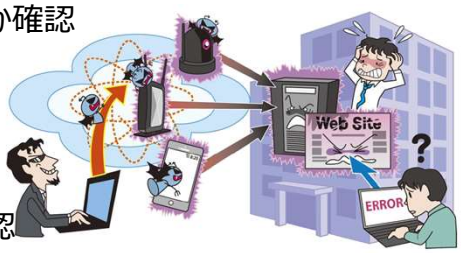
３．バックアップ対策の実施
- 最新のバックアップが確実に取得されていることを確認
- バックアップデータから実際に復旧できることの確認
- バックアップデータをネットワークから切り離し、変更不可とする対策の検討

４．サービス不能攻撃への対応
- サービス不能攻撃に対抗するための機能設置
- サービス不能攻撃に係る通信遮断等の対策の導入を検討
- サービス不能攻撃の影響を排除又は低減するための専用対策装置の導入を検討
- コンテンツデリバリーネットワーク(CDN）サービスの利用を検討
- 閲覧障害時の告知ページに最低限のテキストデータを掲載する
- 複数の情報発信手段を活用して情報発信を行う

５．アクセス制御に関する対策
- 不必要な管理機能、ポート及びプロトコルが解放されていないか確認
- パスワードが単純でないかの確認
- アクセス権限の確認、多要素認証の利用等

６．ソフトウェアに関する脆弱性対策の実施
- ソフトウェアに関する脆弱性対策の状況を確認

７．利用機器に関する対策
- 機器のファームウェアが最新のものにアップデートされているか確認



«CS情報SHIG@»OSやアプリを最新のものに更新し、定期的にウイルスチェックしましょう。

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　→