COVID-19 に乗じたオンライン詐欺と脅威への注意

PCI SSC は コロナウィルス（COVID-19）感染拡大 に乗じたオンライン詐欺と脅威 に対するガイダンスを共有しています。

質問: COVID-19 危機に関連してどのような脅威が潜在しているのですか？

回答: 不確定な状況下で増加するオンラインによる活動が進む中、サイバー犯罪者は現在のコロナウィルス（COVID-19）感染拡大問題に突け込み、混乱の状況を利用した攻撃で活発に活動しています。犯罪者はその規模と手口を向上させておりオンライン詐欺と脅威に今まで以上の注意が重要です。

社会が公衆の健康問題に情報と関心が向いている間、サイバー犯罪者は人々を欺き普通のサイバー攻撃を施します。US シークレットサービスによると、この時期に最も一般的なオンライン攻撃のひとつはフィッシング・ソーシャルエンジニアリング攻撃です。 サイバー犯罪者はコロナウィルスについての重要情報を合法的な医療・保険機関になりすまし広範囲に大量のメールを送るなど消費者の混乱に突け込みます。 ハッカーはフィッシングと他のソーシャルエンジニアリング手法使い合法的に見えるメールとソーシャルメディアメッセージで秘密情報、例えばクレジットカード番号、ソーシャルセキュリティ番号やパスワードなどを提供するように欺き組織を標的にします。

これらの攻撃はしばらくの間、各地で発生しサイバー攻撃の中心をなし、ビジネスと顧客をリスクに晒すことになります。 メールやソーシャルメデイアの取り扱いの際に防御を向上させることが重要です。コロナウィルスの状況によりリモートワーク人口が増えれば増えるほどフィッシングやソーシャルエンジニアリング攻撃に対するベストプラクティスへの啓蒙が必要となります。

https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_Coronavirus_Phishing_Alert.pdf

質問: フィッシング・ソーシャルエンジニアリング攻撃からどのように防御したらよいですか？

回答: フィッシング・ソーシャルエンジニアリング攻撃は過去何年もの間報告されています。このタイプの攻撃から防御するために下記を含む多くの手法があります。

欲しないメールトラフィックの削減:

- ✓ 基本的なセキュリティ保護策の導入と維持、これにはファイアウォール、アンチマルウェアソフトウェア、知られた悪意のIPアドレスやドメインなどを避けるEメールフィルターなどを含む

Eメールとブラウザのセキュリティ、ベストプラクティスに関する従業員とユーザー教育、この中には下記の項目を含む:

- ✓ 不審なメール内にあるウェブサイトへのリンクにクリックを促すような内容に応じない
- ✓ 未知のソースからのメールの添付物には警戒する。また、多くのウイルスはリターンアドレスを偽造できる、そのためたとえそれが一見既知の人物からのように見えても添付物の開封には慎重な対応が必要

定期的な更新:

- ✓ 悪意の侵入をブロックし不審な行為をアラートする基本的なセキュリティツールを使用する。この中にはファイアウォール、アンチウィルス、マルウエア・スパイウェア検知ソフトを含む
- ✓ ウェブブラウザとセキュリティソフトウェアが常に最新のセキュリティパッチと更新を実行しているか定期的にチェック

私用デバイスと業務用デバイスは分離:

- ✓ ソーシャルメディアサイト、Eメール、一般的なインターネット用のコンピューターと金融取引用に使われるコンピューターを分離する

従業員とユーザーに対してウェブサイトとブラウザセキュリティベストプラクティスを教育、これには下記の項目が含まれる:

- ✓ 承認されたアプリケーションのみをインストールする
- ✓ ソフトウェアをダウンロードしたりアップグレードする時に正しいウェブサイトであることを確認、信頼できるサイトを使うときでも異なるサイトに誘導されていないことを確認するためダウンロードの前にURLを再チェックする
- ✓ あなたのコンピューターが影響を受けている兆候が認識された場合はIT担当に連絡する

良いパスワードを健全に使うプラクティス:

- ✓ コンピューターとPOSシステム(OS,セキュリティソフトウェア、ペイメントソフトウェア、サーバー、モデム、ルーターを含む)のパスワードをデフォルト値から推測が難しい個人に属するものに変更(例えば、大文字、数字、特殊文字またはパスフレーズなどを含む)
- ✓ システムパスワードを定期的に更新、特に外部コントラクターがハードウェア、ソフトウェア、POSシステムのインストールやアップグレードを行った場合
- ✓ 従業員とユーザーに強力なパスワードの使用と頻繁な変更を教育

2要素認証の使用:

- ✓ 攻撃の多くはどうにかしてパスワードを取得することに依存している。そのため、例えばセキュリティトークンのように他のIDも求めればハッカーがアカウントにアクセスするのをさらに難しくする

質問: COVID-19 不正アラートやフィッシング・ソーシャルエンジニアリング攻撃についての情報はどこから取得したらよいですか？

回答:下記リソースから増大する脅威と対抗するためのガイダンスについて最新情報をご確認ださい。

関連する脅威に関して:

https://www.secretservice.gov/data/press/releases/2020/20-MAR/Secret_Service_Coronavirus_Phishing_Alert.pdf

https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing

https://www.justice.gov/usao-wdpa/covid-19-fraud-page
https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/make-your-home-cyber-safe-stronghold

支援するためのリソース:
https://blog.pcisecuritystandards.org/resource-guide-defending-against-phishing-attacks
https://blog.pcisecuritystandards.org/resource-guide-defending-against-phishing-attacks
https://blog.pcisecuritystandards.org/topic/phishing
https://blog.pcisecuritystandards.org/infographic-protecting-your-payment-data-from-malware

2020年 3 月