小規模組織向けサイバーセキュリティ

CISO 向けチェックリスト：顧客を守る

個人レベルのデータ保護に関する顧客および従業員への助言

☐ **従業員と顧客が各自のデータ保護をより強化できるよう、以下の個人向けガイドラインを案内する:**

- 全ての個人および業務用デバイスで強力なパスワードを利用し、パスワードマネージャーの利用を検討する。
- 全てのコンピューターおよびモバイルデバイスにおけるオペレーティングシステムならびにその他のソフトウェアおよびアプリケーションを最新状態に保つ。
- 不正プログラムを防止、検出、そして削除するアンチウイルス、アンチマルウェア、そしてアンチランサムウェアソフトウェアをインストールする。
- ファイアウォールプログラムを利用して、コンピューターへの不正アクセスを防止する。
- 信頼できる会社のセキュリティ製品のみを利用する。コンピューターおよび消費者向け出版物のレビューを読み、コンピューターまたはオペレーティングシステムのメーカーに相談することを検討する。
- 機密情報の取扱いには注意する。 銀行口座のパスワードまたはその他の金融口座に関する機密データを暗号化されていないメールで送信しない。
- 銀行または機密の個人情報が関係するその他の通信のためにインターネット接続を行う場合、いつ、どのようにして利用するのかよく考える。
- 一方的に送られてきたか、疑わしいメールの添付物またはリンクを直ちにクリックしない。Stop. Think. Click.
- 予期せぬ形で誰かがインターネットまたは電話で連絡してきて、個人情報を求めた場合は警戒する。既知のアドレスと通信している場合でも、メール上での個人情報の共有は最小限に留める。
- 金融機関は既にあなたに関する個人情報を保持しているため、機密情報を求めてメールまたは電話で連絡してくることはない点に留意する。
- 一度も口座を開いたことのない銀行から情報を要求された場合は、詐欺であるものと仮定する。
- 個人情報を提供する前に、疑わしいメールまたはポップアップボックスの妥当性を検証する。メールアドレスに注意を払う。

アカウントの管理

☐ **顧客が貴組織のサービスにログインする際は、強力なIDとパスワードを使用するよう義務付ける。他のアカウントと同じパスワードを使うことのないよう助言する。**

☐ **インスタント認証、リアルタイム認証、テストデポジット認証、ID認証、および／またはアウトオブウォレット質問を用いて本物の顧客を確認し、詐欺の機会を減らす。**

☐ **顧客が貴組織のサービスにログインする際は、二要素認証の利用を提案するか義務付ける。**

☐ **ユーザーアカウントに詐欺の痕跡がないか、定期的に確認する。**

データの保護

- ☐ 貴組織がサービスを遂行するにあたって、どの顧客データを収集する必要があるのか検討し、その用途以外の顧客データを収集する際は警戒する。
- ☐ データ保持ポリシーを設定して配布する。不要になった顧客データは破棄する。
- ☐ 転送および保存中のデータを暗号化する。
- ☐ データセキュリティポリシーを配備して、どのデータ転送手段が承認または禁止されているのか明確にして、従業員が顧客データを取扱う際に容認される手段を特定する。こうしたポリシーが全ての職員を対象に文書化、連絡、施行され、定期的に審査 ・ 更新されるよう万全を期する。

公開 WEB アプリケーションのセキュア化

- ☐ 組織の顧客対応 Web アプリケーション上で HTTPS を実装し、全ての HTTP トラフィックを HTTPS にリダイレクトする。
- ☐ Web サイトでコンテンツセキュリティポリシーを採用する。
- ☐ Web サイトで公開キーピニングを有効にする。
- ☐ 顧客対応 Web アプリケーションが、極秘または重要な顧客情報（パスワードなど）の保管にクッキーを一切利用せず、クッキーに関して控えめな有効期限（後ではなく近い将来）を設けるよう万全を期する。
- ☐ 使用するクッキーに保存した情報の暗号化を検討する。
- ☐ 最低年に一度、顧客対応 Web アプリケーションのセキュリティアセスメントとしてペネトレーションテストサービスの利用を検討する。

従業員の訓練

- ☐ 従業員に説明責任と戦略を教えて、顧客データの漏洩につながる人的エラーを最小限に留める。つまり、以下の点について助言すること:
  - 顧客データへのアクセスおよびその転送は、各職務権限の遂行のみに必要となるよう最小限に留める。
  - 顧客データを取扱う全てのデバイスおよびアカウントにおいて、強力なパスワード、二要素認証の有効化、ソフトウェアの最新状態の維持、そして疑わしいリンクのクリック回避による強力なセキュリティ慣行を維持する。
  - 潜在的な内部／外部セキュリティインシデント、脅威、または顧客データの取扱いミスについて、組織の技術職員および／または上級管理職に通報する。
- ☐ 必ず、従業員が組織のデータ保護およびセキュリティポリシーを理解し、これを遵守する書類に署名するよう万全を期する。

顧客への通達

☐ **組織の規制環境に対するアウェアネスを築き、顧客のデータ漏洩を取扱うインシデントが発生した場合も確実に遵守できるようにする。**

☐ **貴組織が顧客の機密情報への不正アクセスによるインシデントを把握した場合、調査を進めて当該情報が悪用されたか、今後悪用される可能性を速やかに判断する。通達に関するベストプラクティスに従い、影響を受けた顧客にできる限り早急に以下の点を伝える:**

- インシデントの基本的な情報および漏洩した情報
- 更なる情報および支援を提供するための電話番号
- 今後 12〜24 カ月間にわたって「引き続き警戒する」必要があることの確認
- なりすまし犯罪が疑われるインシデントが発生した場合の迅速な通報の奨励
- 当該情報を更なる不正アクセスまたは使用から保護するために金融機関が取っているステップの基本的な情報
- 信用調査機関の連絡先情報
- 貴組織が遵守するべき規制に基づき義務付けられているその他の情報

CARNEGIE
ENDOWMENT FOR
INTERNATIONAL PEACE

CarnegieEndowment.org