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：組織を守る

リスクベースの情報セキュリティプログラムの策定

- ☐ 貴組織の事業が保管および利用する、あらゆる種類の情報を特定 ・ 一覧化する（例: 顧客の氏名およびメールアドレス）。
- ☐ 次の情報の種類に関して質問し、回答を記録する:
  - この情報が公開された場合はどうなるだろうか？
  - この情報が不正確であった場合、私の事業はどうなるだろうか？
  - 私／顧客がこの情報にアクセスできなかった場合、私の事業はどうなるだろうか？
- ☐ 特定した情報に触れるテクノロジーは何か記録する。これには、ハードウェア（例：コンピューター）およびソフトウェアアプリケーション（例：ブラウザメール）が含まれる。
  - 該当する場合は、貴組織の事業以外のテクノロジー（例：クラウド）ならびにファイアウォールなどの保護テクノロジーなどが含まれる。
  - 在宅勤務用の展開に利用するかもしれないテクノロジーも含める。
  - メーカー、モデル、シリアル番号、またその他の識別子も含める。
  - 各製品がどこにあるのか追跡する。ソフトウェアに関しては、そのソフトウェアがどのマシンに搭載されているのか特定する。
- ☐ 金融セクターが直面し得る脅威と脆弱性について、全国的な CERT、FS-ISAC 、自身の地域の InfraGard 支部、またその他から得る情報を定期的に見直し、貴組織が影響を受ける可能性を推察する。
- ☐ 最低でも月に1回、脆弱性のスキャンまたは分析を実施する。
- ☐ 「在宅勤務」プロトコルを含む、貴組織のためのサイバーセキュリティポリシーを作成する。
- ☐ ポリシーの詳細について全ての従業員を訓練し、ポリシーを遵守して組織のサイバーセキュリティの継続的な維持に同意する書類への署名を要求する。
- ☐ エンタープライズリスクアセスメントおよびアクセス制御管理を含む内部脅威に対して保護計画を策定する。

マルウェアによる被害の防止

- ☐ ファイアウォールを起動してアクセス制御リスト（ACL）を設定する。ホワイトリスト設定を利用してアクセスを制限する。
- ☐ 全てのコンピューターおよびノートパソコンにおいて、アンチウイルスソフトウェアおよびアンチスパイウェアを利用する。
  - ☐ セキュリティツールを「在宅勤務」環境において効果的に運用できるよう万全を期する。
- ☐ メーカーおよびベンダーが提供する最新のソフトウェアアップデートを適用する。可能な限り「自動的にアップデート」を利用する。
- ☐ 新しいプログラムのインストールは管理者権限を持ったIT職員に制限する。
- ☐ 保護／検出ハードウェアまたはソフトウェアによって生成されたアクティビティログを保守 ・ 監視する。パスワード保護と暗号化によってログを保護する。

- ☐ 必ず、全てのホストの内部クロックを同期する。
- ☐ SD カードおよび USB スティックなどのリムーバブルメディアに対するアクセスを制御する。職員には、代わりにメールまたはクラウドストレージ経由でのファイル転送を推奨する。外部ソースから得た USB の利用、または他者への USB の引き渡しがもたらすリスクについて職員を教育する。
- ☐ 自身のメールサービスにおいて、メールセキュリティとスパムフィルタをセットアップする。
- ☐ 顧客対応 Web サイト上の全てのページを暗号化およびその他に利用可能なツールで保護する。
- ☐ 組織のアセットおよびシステムのセキュリティを評価するため、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

- ☐ 全ての新入社員にはオンボーディングの際に、また既存社員には最低でも年に一度、定期的な間隔を空けて、必須のサイバーセキュリティトレーニングの実施を計画する。従業員には以下を義務付けること：
  - 全ての業務デバイスおよびアカウントにおいて強力なパスワードを利用し、プライベートのデバイスでも同様の措置を取ってパスワードマネージャーの利用を奨励する。
  - 在宅勤務用のITインフラストラクチャーを含め、全てのデバイスをまたいだオペレーティングシステム、ソフトウェア、そしてアプリケーションを最新の状態に保つ。
  - 全てのアカウントで二要素認証を用いる。
  - アカウント情報とアクセスカードを安全に保ち、デバイスを離れる際はロックをかける。
  - アカウント情報またはその他の機密データを、暗号化されていないメールまたはその他のオープンな通信経由で共有することを控える。
  - 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開かないようにする。
  - 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して、メールアドレスに細心の注意を払う。
  - 潜在的な内外部のセキュリティインシデント、脅威、データもしくはデバイスの取扱いミスについて、技術職員および／または上級管理職に通報する。
- ☐ 偽アカウントからフィッシング形式のメールを送信するシミュレーションなどを通じて、従業員アウェアネスの定期的なテストを計画 ・ 実施する。従業員が正しく対処できなかった状況を評価し、学習と改善の機会に活かす。

データの保護

- ☐ 重要なデータ（例：文書、メール、カレンダー）を定期的にバックアップして、復元可能であることをテストする。クラウドへのバックアップを検討する。
- ☐ バックアップを含んだデバイスが、オリジナルのデータを抱えたデバイスに物理的またはローカルネットワーク経由で永続的に接続していないことを確認する。
- ☐ サージプロテクターをインストールして発電機を使い、全てのコンピューターおよび重大なネットワークデバイスが無停電電源装置に差し込まれていることを確認する。
- ☐ モバイル端末管理（MDM）ソリューションを利用する。

デバイスを安全に保つ

- ☐ モバイル端末の PIN またはパスワード保護をオンにする。デバイスが紛失するか盗難に遭った場合、追跡、遠隔ワイプ、または遠隔ロックが可能となるようデバイスを構成する。
- ☐ 可能な場合は「自動的にアップデート」オプションを利用して、デバイス（および全てのインストール済みアプリ）を最新状態に保つ。
- ☐ 機密データを送信する際は、公共の Wi-Fi ホットスポットに接続せず、セルラー接続（テザリングおよび Wi-Fi ドングルを含む）または VPN 接続を利用する。
- ☐ メーカーサポートが終了したデバイスは、最新の代替品と置き換える。
- ☐ 紛失したか盗難にあった機器の通報手順を設定する。

パスワードの利用

- ☐ 必ず、全てのコンピューターが、再起動後にパスワード入力を必要とする暗号化製品を利用すること。モバイル端末の PIN またはパスワード保護をオンにする。
- ☐ 強力なパスワードを利用すると共に、予測しやすいパスワード（例：passw0rd）や個人を特定可能な情報（家族またはペットの名前）を回避する。同じ対策を全ての従業員に求める。
- ☐ 可能な限り二要素認証（2FA）を利用する。
- ☐ 職員に配布する前に、ネットワークおよびIoTデバイスを含む、メーカー発行のデフォルトパスワードを全てのデバイスで変更する。
- ☐ 職員が容易に各自のパスワードをリセットできるように万全を期する。また、職員が定期的な間隔でパスワードを変更するよう義務付けることも可（例：四半期ごと、半年ごと、または毎年）。
- ☐ パスワードマネージャーの利用を検討する。パスワードマネージャーを利用する場合は、「マスター」パスワード（その他全てのパスワードへのアクセスを提供）が強力であることを確認する。

許可の制御

- ☐ 必ず、全ての従業員が一意的に識別可能なアカウントを持ち、貴組織のシステムにアクセスする度に認証されるよう万全を期する。
- ☐ 管理上の特権は信頼できるIT職員および主要職員のみに付与し、標準ユーザー向けワークステーションにおける管理者特権を破棄する。
- ☐ 従業員には職務に必要となる具体的なデータシステムへのアクセス権限のみを付与し、いかなるソフトウェアも許可なくインストールすることのないよう万全を期する。
- ☐ 組織のコンピューターで各従業員のユーザーアカウントを作成する。
- ☐ 在宅勤務している職員および管理者向けのアクセスオプションを明確に定義する。

WI-FI のセキュア化

- ☐ 職場の Wi-Fi がセキュアであり、WPA2 方式で暗号化されていることを確認する。一般的にルーターの暗号化はオフの状態で届くため、必ずこれをオンにする。ルーターへのアクセスをパスワード保護して、必ず事前設定されたデフォルトパスワードを更新する。あらゆる「遠隔管理」機能をオフにする。
- ☐ Wi-Fi ネットワークへのアクセスは、一定の MAC アドレスを備えたデバイスのみに制限する。顧客が Wi-Fi を必要とする場合は、別途の公衆ネットワークをセットアップする。
- ☐ ネットワークにアクセスした全てのデバイスを容易に追跡できるよう、ネットワークデバイスで DHCP（動的ホスト構成プロトコル）ロギングを有効にする。
- ☐ ルーターのセットアップ後、管理者としてログアウトする。
- ☐ ルーターのソフトウェアを最新状態に保つ。ルーターのメーカー登録を行い、最新情報にサインアップする。

フィッシング攻撃の回避

- ☐ 必ず、職員が管理者権限を持ったサーバーまたはアカウントから、Web のブラウジングやメール確認を行うことのないよう万全を期する。
- ☐ Web およびメールフィルタをセットアップする。一般的にサイバーセキュリティ脅威と関連付けられている Web サイトに従業員がアクセスする際は、これをブロックすることを検討する。
- ☐ 綴りや文法の明らかな誤りや、見覚えのあるロゴの低品質なバージョンなど、フィッシングの分かりやすい痕跡について従業員を指導する。送信元のメールアドレスは正当なアドレスに見えるだろうか?
- ☐ フィッシング攻撃を受けたことが疑われる場合は、できる限り早急にマルウェアスキャンを行い、パスワードを変更する。職員がフィッシング攻撃に遭ったとしても、懲罰を与えてはいけない（将来的に通報する気を削ぐことになるため）。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org