protiviti®
Face the Future with Confidence

リモートワークや在宅勤務における サイバーセキュリティの取り組み

リモートワークや在宅勤務（Work From Home : WFH）への移行が加速する中、企業は、WFHを行う従業員（リモートワーカー）が意識すべきセキュリティ対策や、企業が行うWFHに対するサイバーセキュリティ対策を検討する必要があります。以下のセキュリティ対策と活動は、WFHへの移行におけるいくつかの前提事項を踏まえ、個人および企業の双方で対処すべき項目を示しています。

個人のサイバーセキュリティ対策

在宅で働く人が日々意識して実践しなければならない活動

- フィッシングメールや詐欺を警戒する
  - 新型コロナウイルス/COVID-19関連のキャンペーン
  - なりすましのパスワードリセット要求
  - 見覚えのない添付ファイル
  - ソーシャルメディア関連の要求（例：LinkedIn接続要求）
- フィッシングの脅威に関する認識を向上する（WFHセキュリティトレーニングの実施）
- 自宅ネットワーク機器のセキュリティを更新し維持する
- すべての機密データは、個人の電子メールではなく安全で暗号化されたソリューション（ShareFileやMicrosoft Teams等）を介して送信する
- 他者に業務用のデバイスを使われないようにする（例：画面のロック）
- 利用出来るデバイスが自宅の私物に限定されている場合の
  - OSやアプリケーション等に全てのセキュリティパッチをインストール
  - アンチウイルスやパーソナルファイアウォール、および一般的なインターネット保護ソフトウェア（例：URLフィルタリング）を導入
  - インターネットを閲覧するブラウザを最新版に更新
  - ブラウザのパスワード保存機能を無効化
  - 業務関連のファイルをローカルのハードドライブにダウンロードしない、もしくはソフトウェアを活用し、ローカルに保存されたファイルを安全に速やかに削除
- シュレッダーがない、または使用不可の場合は、機密データを印刷しない

企業のサイバーセキュリティ対策

企業が考慮して実施しなければならない活動と管理

- 一般的なコンシューマー向けのWi-Fiを利用するにあたってのセキュリティチェックリストを配布する
- 上記の「個人のサイバーセキュリティ対策」を用いてWFHのセキュリティに関する考慮事項と要件のチェックリストを配布し、従業員に確認とサインを求める
- 従業員全体に対するコミュニケーションを高める
  - 「どうやるの（How do I）」ではなく「WFHセキュリティのコツや注意点」を通知し意識向上を図る
  - フィッシングに関する注意喚起の通知を実施する
  - 従業員がリアルタイムのフィードバックや質問を行える仕組を提供する

リモートワークや在宅勤務におけるサイバーセキュリティの取り組み

企業のサイバーセキュリティ対策（続き）

ネットワーク

- WFHに必須の技術（VPN、VDI、コラボレーションツールなど）の帯域幅と制限を確認する
- VPNアクセスが利用可能であることを確認し、（可能であれば）登録されたデバイスのみを許可する
- VPNにセキュリティパッチが適用され、適切にアクセス設定されていることを確認し、許可された個人のみがVPNにアクセス可能とする
- 企業ネットワーク環境への全てのリモート接続ポイントにおいて多要素認証（MFA）を適用し、MFAを省略する古い認証プロトコルは停止する
- 最新の脅威に対応するため、スパムフィルタを見直し継続的に更新する
- ウェブフィルタリング／プロキシの設定を見直し継続的に更新して、必要なビジネス活動のみに制限する
- データ損失防止（DLP）ソフトウェアを導入し、構成やデジタル署名が最新であることを確認する

コラボレーション・ソリューション

- すべてのコラボレーションプラットフォーム（電子メール、チャット、ビデオ会議、ファイル共有など）のセキュリティをレビューし、ベストプラクティスを実施する
- 権限のある個人のみがアクセス可能とする
- ファイル共有が安全な方法で行われる仕組を整備し、安全なファイル共有の実践法を周知する
- データ損失防止対策を実施する（可能な場合）
- ビデオ会議において不特定多数が参加できないようパスワード入力を要求する
- 可能な場合、すべてのデバイスに対し重要なパッチを更新するためのプッシュ機能の導入を検討する

セキュリティ・オペレーション

- WFHの実現において新たに指定されたミッションクリティカルな資産にセキュリティ監視と運用を集中する
- インシデント対応計画を見直し、WFHのシナリオに適用可能であることを確認する
- セキュリティイベント報告手順を従業員および請負業者に周知し、改めて認識させる
- サポートデスクのストレスを軽減するために、パスワード変更期限を一時的に緩和することを検討する

PC端末（エンドポイント）

- エンドポイントファイアウォールのソフトウェアを導入し、ローカルネットワークの可用性を制限し、インターネットからの脅威から保護する
- アンチウイルス／マルウェア検出ソフトウェアを導入し、設定やシグネチャを最新の状態に保つ
- EDR（エンドポイント検出対応）ソフトウェアを導入し、構成やデジタル署名が最新であることを確認する
- データ損失防止（DLP）ソフトウェアを導入し、構成やデジタル署名が最新であることを確認する
- デバイスやデータのバックアップを有効にする
- デバイスの暗号化を有効にする

他の留意点

- 調達部門と連携し、新たに購入したハードウェアが資産管理ソフトウェアによって棚卸され、従業員に配布される前に適切に構成および保護されていることを確認する
- 従業員がオフィスに戻る前に、新たに導入されたすべてのハードウェアを収集および一覧管理するプロセスを整備する
- 廃棄される予定のハードウェアを、不要なデータや設定が残存していないことを確認のうえで活用する
- インターネットに接続できない従業員のために、スマートフォンのテザリング機能を活用する
- 全体的なIT／サイバーの意思決定を小規模且つアジャイルなプロセスとする（スピードやコラボレーションを優先し、形式主義を排除するため）
- 安定性が達成されるまで、すべてのシステムの開発を凍結する
- WFHが生み出す新たなビジネスリスクや、リスクを軽減するために行なった措置、また、リスク軽減のためのオペレーションの変更や維持の方法等について、役員や取締役会メンバーから質問に答えられるよう準備する

Protiviti.com/TechnologyConsulting
TechnologyConsulting@Protiviti.com
TCblog.Protiviti.com

protiviti®