サイバーセキュリティチェックリスト

サイバー犯罪者は、新たな脆弱性を突いて攻撃するための巧妙な手段を日々見つけ出しています。リモートワーク、IoTデバイスやデータの増加は、サイバーセキュリティリスクの増大につながり、2021 年のフィジカルセキュリティ業界状況レポートにおいて、回答者の 52% が組織が直面する最大の課題はサイバーセキュリティの脆弱性であるとしています。

そのため、包括的なサイバーセキュリティ戦略はフィジカルセキュリティの導入プロセスにおいて、あらゆる段階で非常に重要となります。ここでは、導入前、導入中、導入後のサイバーセキュリティ体制を強化するのに役立つ 3 つのチェックリストを示します。

Genetec™

導入前のチェックリスト

既存のフィジカル セキュリティ基盤に新しいシステムを導入または追加しますか？必ず成功するように準備しましょう。このチェックリストは自社とベンダーを評価し、導入設置計画の最適化、潜在的なリスクの低減に役立ちます。

ベストプラクティス

- ☐ 適切なサイバーセキュリティ戦略計画は自社に存在していますか？
- ☐ 保有するセキュリティシステムを対象にサイバーセキュリティ評価を実施しましたか？
- ☐ 保有するフィジカルおよびサイバーセキュリティの両方に対して脆弱性評価を行い、問題点を把握していますか？
- ☐ 自社内で接続されているすべてのフィジカルセキュリティデバイスの完全な脆弱性評価を実行し、懸念点があるモデルとメーカーを特定できていますか？
- ☐ 自社内で使用されている機器は、模造品や不正ライセンス製品ではなく正規の製品だけですか？
- ☐ 技術的な側面の他に、リスク低減のために考慮すべきことは他に存在しますか？

リスク管理

- ☐ 包括的なリスク管理戦略は自社に存在しますか？
- ☐ セキュリティ運用やインシデント管理をガイドするための新しい基準を設けましたか？
- ☐ 社内の IT チームとフィジカルセキュリティチームは、包括的なセキュリティプログラムに互いに協力していますか？
- ☐ フィジカル セキュリティデバイスやシステムにアクセス可能なユーザーを特定していますか？
- ☐ 信頼できるメーカーのエッジデバイスを使用していますか？
- ☐ 違反・漏洩管理ポリシーとその対応手順は存在しますか？
- ☐ サイバー保険を必要としていますか？
- ☐ 重要なデータのバックアップや災害復旧計画は存在しますか？
- ☐ どのようにシステムの可用性を確認していますか？

認証と規制

- ☐ 検討されたソリューションには必要な認証が含まれていますか？
- ☐ 自社の特定の状況に適用されるデータ保護規制やフレームワークはどういったものですか？
- ☐ GDPR に準拠するために何をすべきかを評価しましたか？
- ☐ PIPEDA に準拠するために何をすべきかを評価しましたか？

ベンダー査定

- ☐ ベンダーは、サイバーセキュリティの実装を支援するドキュメントやツールを保有していますか？
- ☐ システムをオフラインにする必要があるときに、ベンダーに通知機能がありますか？
- ☐ サイバーセキュリティの脆弱性に関してベンダーの透明性はどの程度ですか？
- ☐ ベンダーは、セキュリティ上の問題点や脆弱性を解消するための包括的な戦略を備えていますか？
- ☐ ベンダーは製品開発においてサイバーセキュリティを優先していますか？
- ☐ 社内の機器が個人情報へのアクセスに使用される場合、誰が責任を負いますか？
- ☐ ソフトウェアとハードウェアを構築する製造会社を所有しているのは誰ですか？

アプライアンスとクラウドサービス

- ☐ 保有するセキュリティアプライアンスが安全に設定されていることを確認するにはどうすればよいですか？
- ☐ セキュリティシステムを保護する特殊なアンチウイルスは存在しますか？
- ☐ 安全なクラウドソリューションを選択していますか？
- ☐ 利用しているクラウドプロバイダーは、データセキュリティや保存性を確保していますか？
- ☐ クラウド上でのデータの入れ替えや保存は完全に保護されていますか？

導入時チェックリスト

新しいフィジカル セキュリティシステムを導入する準備はできましたか？
このチェックリストに従って、アップグレードまたはインストール作業をフォローし、リスクの低減、円滑な導入を進めてください。

ベストプラクティス

- ☐ IT に関するベストプラクティスについて従業員に適切なトレーニングを実施しましたか？
- ☐ 現在のサイバー脅威に関するインテリジェンスや脅威のトレンドを監視・共有し、予防措置やその対応に関する協力を奨励していますか？
- ☐ すべての保有機器のリストを保持していますか？
- ☐ データ保護
- ☐ システムに保存されているマルチメディアデータは保護されていますか？
- ☐ マルチメディアデータは、保有システム内で交換されたときに保護されますか？
- ☐ 指揮統制のデータは保護されていますか？
- ☐ エンドツーエンドの暗号化は実装されましたか？
- ☐ 暗号化キーはどのように管理されますか？

認証と承認

- ☐ 自社内でパスワードを適切に管理していますか？
- ☐ クレデンシャルの有効期間管理についてのポリシーとプロセスを確立していますか？
- ☐ デバイス等のデフォルトのユーザー名とパスワードをすべて変更しましたか？
- ☐ セキュリティシステムと接続されているすべてのデバイスへのアクセス時に充分な強度のパスワードを使用していますか？
- ☐ 不正アクセスを防ぐために単一認証よりも堅牢なものを必要としていますか？
- ☐ ユーザーのシステムへのアクセス時のセキュリティを強化するために、多要素認証やユーザー承認定義を含む多層的な戦略を実装しましたか？
- ☐ 保有するすべてのセキュリティシステムの ID 管理を可能な限り一元化していますか？
- ☐ パスワードへのブルートフォース攻撃に対する保護はありますか？
- ☐ ユーザーグループを正しく設定し、適切なユーザーに権限を割り当てていますか？
- ☐ 長時間ログインがないユーザーからのアクセスを制限する保護機能は存在しますか？
- ☐ 許可されたユーザーは、必要なものにのみにアクセスを制限されていますか？

デバイスのセキュリティ

- ☐ 既存のカメラはセキュアな状態ですか？
- ☐ 各デバイスの製造元やファームウェアのバージョンなど、各フィジカルセキュリティデバイスの詳細情報を把握していますか？
- ☐ ネットワークに接続されているすべてのカメラや管理システムに関する最新の保有設備リストは存在しますか？
- ☐ セキュリティで保護されていないデバイスの交換を計画していますか？
- ☐ サポートされる暗号化機能やサイバーセキュリティ機能の種類や各デバイスのファームウェアのバージョンを把握できる仕組みがあり、利用できる状態ですか？
- ☐ 入退室管理ハードウェアはセキュアに保護されていますか？
- ☐ VMS と ACS ソフトウェアが、データ保存や監視コンソールとして稼働するデバイスやサーバーとともに最新版であることを確認しましたか？
- ☐ 自動ナンバープレート認識デイバスはセキュアな状態ですか？
- ☐ デバイスのファームウェアに迅速にパッチを当てるための手順は決められていますか？

導入・設置後

導入や設置が完了しても必要な作業はそこで終わりではありません。このチェックリストは、システムの正常稼働性の監視、サイバーセキュリティ対応状態の確認を行い、システムの円滑な稼働を実現するための予防処置の立案を支援します。

メンテナンスとアップデート

- ☐ 導入したデバイスを最新の状態に保つためのツールは存在しますか？
- ☐ 絶えず重要なセキュリティアップデートに注意を払っていますか？
- ☐ インストール前に、各ソフトウェアアップデートの取得先の正当性を確認しましたか？
- ☐ セキュリティリスクの存在が公開されている製造元やモデルの情報をもとに、保有するデバイスリスト上に該当するものが存在しないかチェックしましたか？
- ☐ 必要に応じてネットワーク設計を変更して古いデバイスを別セグメント化するなど、クロスオーバー攻撃を低減する措置を行っていますか？
- ☐ 適切なソフトウェアパッチやホットフィックスを適用していますか？
- ☐ 保有する Windows のエコシステムを適切に管理していますか？
- ☐ すべてを最新の状態に保ち、サイバーセキュアな状態に保つための適切なツールを保有していますか？
- ☐ どうやってユーザーリストを最新の状態に保ちますか？
- ☐ メンテナンス作業を自動化するためのツールは存在していますか？
- ☐ どのようにセキュリティアプライアンスのオペレーティングシステムを最新の状態に保ちますか？
- ☐ すべてのユーザー権限を確認および更新するためのツールはありますか？

正常動作監視とリスク管理

- ☐ システムやデバイスの状態を監視するための適切なツールは存在しますか？
- ☐ 多数の導入・設置時の状況と正常動作性を監視する機能はありますか？
- ☐ 保護・管理の連携を維持していますか？
- ☐ 新しい脅威や脆弱性に注意を払っていますか？
- ☐ サイバーインシデントが発生した場合に、調査のためのログ分析技術を備えていますか？

Genetec システムの正常稼働性を確実に監視

Genetec プロフェッショナルサービスチームは、御社のサイバーセキュリティ対応状況を精査し、システムを効率的に運用し続けるために求められる予防措置についての知見の共有を支援いたします。

弊社のセキュリティスペシャリストがどのように支援できるかをご覧ください。

Genetec は、セキュリティ、インテリジェンス、オペレーションを含むオンプレミスおよびクラウドベースのソリューションを提供するテクノロジー企業です。弊社の主力製品である Genetec™ Security Center は、IP ベースのビデオ監視、入退室管理、自動ナンバープレート認識 (ALPR)、通信および分析が統合化されたフィジカル セキュリティプラットフォームです。さらに、Genetec は、地域やコミュニティのセキュリティを向上させるために設計されたクラウドベースのソリューションとサービスを開発しています。

UDPT: 23-09-2022

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

Genetec™