AXIS Camera Station Pro

システム強化ガイド

はじめに

はじめに

はじめに

どのようなセキュリティシステムやサイトも100%サイバーセキュアにすることができる、万能で間違いのない機能です。この言葉は魅力的に聞こえますが、そのような機能は存在しません。あるいは、すぐにでも存在するかもしれません。代わりに、組織特有の脅威や脆弱性がもたらすリスクを検証し、リスクが許容できないと判断された場合は、そのリスクを軽減するためのコントロールを導入する必要があります。明確に定義されたポリシーと手順は、組織全体における一貫したコミュニケーションと統制の適用を保証し、成熟したサイバーセキュリティプログラムの基礎を形成します。

推奨されるアプローチは、ISO 27001、NIST CSFなど、標準化されたITセキュリティリスク管理フレームワークに従って作業をすることです。小規模な組織にとって、この作業は大変なことかもしれませんが、情報セキュリティポリシーの基本セットとそれを支えるプロセスを定義することは、何もないよりははるかにましです。組織がサイバー成熟への旅を始めようとしていて、自由に使えるリソースが限られている場合は、*Center for Internet Safety (CIS) Critical Security Controls Version 8*を調査することを推奨します。CISは、組織のサイバーセキュリティプログラムの開発と成熟を支援するために、3つの実施グループに分類された18のセキュリティコントロール活動のリストを提供しています。

セキュリティ侵害が多くの組織で発生しているのは、企業が従業員の使用方法やアクセス権を管理するための明確なポリシー、ルール、手順を確立していないためです。あなたの組織は、ビデオ管理運用のポリシーやプロセスに取り組んでいますか? そうでない場合は、定義づけを始める時期です。

目的

本書では、システムの安全な展開と保守を支援するために有用な、多くのサイバーセキュリティポリシーと手順を概説します。サイバーセキュリティフレームワークに直接マッピングされているわけではありませんが、当社は主にCIS Security Controls v8を参考にして、以下のコントロール活動に重点的に取り組んでいます。

- *コントロール1: 企業資産のインベントリとコントロール*
- *コントロール2: ソフトウェア資産のインベントリと管理*
- *コントロール3: データ保護*
- *コントロール4: 企業の資産とソフトウェアのセキュアな設定*
- *コントロール5: アカウントの管理*
- *コントロール6: アクセスコントロールの管理*
- *コントロール7: 継続的な脆弱性の管理*
- *コントロール10: マルウェアの防御*

当社の推奨事項は、システムを導入および管理する際の一般的なリスクを軽減するために、設置業者、インテグレーター、およびエンドユーザーを支援することに重点を置いています。

前提条件

*AXIS OS強化ガイド*で定義および説明している推奨事項と手順を理解し、それに従うことを前提としています。また、本書では、ビデオシステムとやり取りする複数の一般的なユーザーの役割についても言及しています。これらのユーザーの役割を、お客様のユーザーおよび役割の分類に合わせてマッピングしてください。個々のユーザーは、組織に応じて複数の役割を持つ場合があります。

定義済みの役割:

- **システムインストーラー**: システムのインストール、設定、リペア、アップグレード、ダウングレード
- **ネットワーク管理者**: ネットワークインフラストラクチャー、エンドノード接続、ネットワークサーバーとリソース、ネットワーク保護を維持します

はじめに

- **ビデオシステム管理者**: ビデオシステムを定義および管理して、使用、パフォーマンス、およびユーザー権限を保護します
- **ビデオシステムメンテナンス**: ビデオシステム管理者に代わって、コンポーネントの監視、調整、トラブルシューティングを行い、システムのパフォーマンスを保護します
- **ユーザー**: クライアントを使用して、ライブビデオや録画ビデオにアクセスし、通常は組織の物理的な保護に責任を負う個人。

システムセキュリティのポリシー

物理的なセキュリティ

物理的な保護のポリシー

サーバー、装置、ネットワーク機器、ケーブルは、干渉されたり、妨害されたり、盗まれたりする可能性のある物理的物体です。ルーターやスイッチなどの重要なネットワーク機器や、サーバーソフトウェアを実行しているホストは、物理的および論理的にアクセスが制限された環境に設置する必要があります。カメラやその他の接続された装置は、手の届きにくい場所に取り付け、耐衝撃モデルやケーシングを採用する必要があります。壁やコンジットにケーブルがあると、いたずらや妨害行為の危険が高まるため、ケーブルの保護には注意が必要です。

推奨ポリシーと手順
決まった間隔でVMSサーバー、ネットワークハードウェア、接続された装置、およびケーブルの物理的な保護を視覚的に監査する責任を負う個人または組織単位を定義します。場所を含め、すべてのサーバーおよび装置の正確なインベントリを維持することが不可欠です。

ソフトウェア管理

サードパーティ製アプリケーションソフトウェアポリシー

は標準的なWindows環境にインストールされるため、ビデオ管理とは関係のないソフトウェアアプリケーションにその環境を利用しようとすることがあります。他のサードパーティ製アプリケーションをインストールすると、環境にマルウェアを持ち込む可能性があり、システムのダウンタイムにつながったり、攻撃者が組織のネットワークに侵入するためのバックドアを提供したりする可能性があります。

推奨ポリシーと手順
ホストハードウェアでは、サーバーソフトウェアと信頼できるサードパーティの統合ソフトウェア以外は実行しないでください。物理ハードウェアを他の目的で使用する必要がある場合は、複数の仮想サーバーインスタンスを使用し、1台の仮想マシンでサーバーソフトウェアを実行し、サードパーティ製の非VMS関連ソフトウェアを別の仮想マシンで実行してください。仮想環境でを実行するための情報については、*こちら*を参照してください。

さらに、サーバーに接続するすべてのサーバーとコンピューターにウイルス対策ソフトウェアを導入することをお勧めします。モバイルデバイスを展開する場合は、その装置に (ウイルス対策ソフトウェアを直接にインストールするのではなく) 最新のオペレーティングシステムとパッチがインストールされていることを確認することも含まれます。ウイルススキャンを行う場合、録画データベースを含むディレクトリやサブディレクトリはスキャンしないでください。これらのディレクトリでウイルススキャンを実行すると、システムのパフォーマンスに影響を与える可能性があります。

アカウントの管理

一般アカウントポリシー

管理者レベルの権限は、利便性のために通常のユーザーに付与される場合があります。多くの組織では、アカウント権限の確認やシステムへの従業員のアクセスの監視を誰が行うのかが不明確です。

推奨ポリシーと手順
システムアカウントを定義する際には、最小権限の原則に従うことをお勧めします。つまり、ユーザーアクセス権限は、特定の作業タスクを実行するために必要なリソースのみに制限されます。また、「特権クリープ」を防ぐため、システムユーザーのアカウント権限を定期的に監査することもお勧めします。

の管理者アカウントポリシー

Windows環境でを展開する際によくある間違いは、Windowsホストに1つの管理者アカウントが定義される点です。時間の経過とともに、パスワードが組織内で共有され、権限のない個人がWindows環境の管理者権限を取

得する危険性があります。その結果、サーバーに多数の不要なユーザーアプリケーションやマルウェアがインストールされる可能性があります。

推奨ポリシーと手順
サーバーをホストしているWindowsには、少なくとも1つの管理者権限アカウントと1つのユーザー権限アカウントが必要です。どちらのアカウントも、Windowsのデフォルトの管理者アカウントと同じであってはなりません。デフォルトの管理者アカウントは、管理者とユーザーの特権アカウントを作成した後に無効にしてください。展開後、管理者アカウントのパスワードは、**ネットワーク管理者**のみが知っていて、使用する必要があります。ユーザー特権アカウントは、**ビデオシステム管理者**がサーバーにログインする必要がある場合に使用します。さらに、上記の2つの役割が同じ個人によって実行される場合でも、監査目的のために、ネットワーク管理者アカウントとビデオシステム管理者アカウントを別々に持つことを推奨します。先に定義したような他の役割をサポートするために、システムにログインする個人**ユーザー**ごとに非特権ユーザーアカウントをさらに作成する必要があります。

を実行しているホストがWindows Active Directoryドメイン環境に配置されている場合は、管理者アカウントとユーザーアカウントをドメインのコンテキストで作成することも、従業員の既存のドメインアカウントをホストへの認証に使用することもできます。これにより、追加のアカウントを作成して管理する必要がなくなり、アカウント管理が簡素化されます。また、これにより、グループポリシー管理を使用して、パスワードの複雑さ、証明書の展開、ドメイン環境で利用可能なその他のセキュリティ機能を強制する可能性も開けます。

のユーザーアカウントポリシー

ユーザーアカウントは 内で特定の役割に割り当てられます。これにより、各ユーザーがシステム内で持つ特定の権限 (アクセスできるビューやビデオなど) が決まります。複数の個人が1つのユーザーアカウントを共有する場合、パスワードが組織内の他の人と共有されるリスクが高まります。また、アカウントを共有することで、誰が、いつ、どのカメラやビデオにアクセスしたかを監査することも事実上不可能になります。

推奨ポリシーと手順

クライアントユーザーの認証には、**Kerberos** を使用することをお勧めします (*5 ページKerberosを使用した認証* を参照)。

可能であれば、Microsoft Active Directoryを使用すると、ユーザーとグループの管理が容易になります。また、システムを設定する前に、すべてのユーザーの役割に関連するセキュリティグループが定義されていることを確認することもお勧めします。

Active Directoryは、以下の機能も提供します。

- ユーザーがパスワードを定期的に変更する必要があるパスワードポリシー
- 認証に何度か失敗すると、組織のパスワードポリシーに従ってWindows ADアカウントがブロックされる、総当たり攻撃に対する保護機能
- 役割ベースの権限、つまり、ドメイン全体にアクセスコントロールを適用可能

ローカルのWindowsアカウントを使用しなければならない場合は、システムの各ユーザーに固有のアカウントを作成し、各自の責任を果たすために必要なシステム内のエンティティのみにアクセスできるようにすることを推奨します。同じ権限を持つユーザーが複数いる場合、ユーザーにグループを活用することで、権限の割り当てを簡素化することができます。

Kerberosを使用した認証

は統合Windows認証を使用してクライアントのユーザーを認証します。はMicrosoft Negotiateプロトコル (SPNEGO) を使用します。つまり、Kerberosが優先およびデフォルトの認証プロトコルです。ネゴシエーションプロトコルは、Kerberosの使用を試み、代替としてNTLMを使用します。

Kerberosを使用するには、以下のコマンドを使用してActive Directoryにサービスプリンシパル名 (SPN) を登録する必要があります。

```
setspn -s ACSService/{HOST} {ACCOUNT_NAME}
```

HOST - 実行中のサーバーのホスト名です。

ACCOUNT_NAME - サーバーを実行するコンピューターの名前 (コンピューターアカウント) です。

Kerberosが正しく動作するために、ターゲットサーバーの短いホスト名とFQDNの両方を登録することをお勧めします。

例::

```
setspn -s ACSService/CompanyServer CompanyServerAccount setspn -s
ACSService/CompanyServer.domain.local CompanyServerAccount
```

詳細については、*microsoft.comのSetspn*を参照してください。

装置アカウントポリシー

Axis装置のアカウントは、主にコンピューター/クライアントのアカウントです。**ユーザー** には、Axis装置への直接アクセスを絶対に許可しないでください。通常の運用中に装置にアクセスする必要があるクライアントはサーバーのみです。一般的な戦略として、すべての装置に同じパスワードが使用されています。これは新たなリスクをもたらしますが、パスワード管理を簡易化することもできるため、装置自体のリスク許容度を評価する必要があります。は、管理インターフェースを通じて各デバイスに一意のパスワードを割り当てる機能をサポートしています。

よくある間違いは、複数の役割が共有している1つのアカウントを使って、に装置を追加することです。ある時点で、**ビデオシステムメンテナンス**が何かを調整するためにブラウザーを使用する必要がある場合、装置のマスターアカウント (root) パスワードが開示されます。数か月もすれば、組織内のほとんどの人がすべての装置のパスワードを知り、システムの管理者権限を持ちます。

推奨ポリシーと手順
装置には、少なくとも2つの管理者アカウントが必要です。装置管理者用に作成された固有のアカウントと、サーバーに装置を追加するためのデフォルトのrootアカウントです。**ビデオシステムメンテナンス**がWebブラウザーを使用して装置にアクセスする場合など、一時的なアクセスは、一時的なアカウントを使用して管理する必要があります。

AXIS Device Managerは、装置のアカウントとパスワードを管理するための主要なツールとして使用する必要があります。AXIS Device Managerのバージョンはに直接組み込まれており、[Management (管理)] タブで利用できます。装置のrootパスワードは、AXIS Device Managerとによってのみ使用され、装置を管理するツールとしてAXIS Device Managerまたはを使用する人だけが知っている必要があります。

メンテナンスの役割の人が、トラブルシューティングやメンテナンスのために、Webブラウザーで (複数の) 装置にアクセスする必要がある場合は、を使用して、一時的なアカウントを用意します。装置を選択し、メンテナンスが使用できる新しいアカウント (できればオペレーター権限付き) を作成します。作業が完了したら、一時アカウントを削除します。

システムメンテナンス

のWindowsホストパッチ適用ポリシー

サーバーおよびクライアントはWindows環境上で実行されます。ソフトウェアをホストするシステムに、ビデオ管理システムへの不正アクセスに悪用されるオープンな脆弱性がないように、これらのシステムを常に最新の状態に保つことが重要です。

推奨ポリシーと手順
Axis NVRまたはカスタムハードウェアのいずれで実行されているかにかかわらず、すべてのシステムで、自動更新をオフにすることをお勧めします。このため、を実行しているすべてのホストシステムに配布する前に、一部のマシンで利用可能な更新プログラムをテストし、システムの安定性を確認することをお勧めします。ただ し、Windowsシステムのパッチ未適用の状態が長く続くと、環境全体にリスクが生じる可能性があるため、セキュリティと安定性のバランスを取る必要があります。外部の脅威に対するお客様のシステムの露出レベルに基づいて、システムが最新の更新を受けるための期間をパッチ適用ポリシーに記載する必要があります。

ソフトウェア更新ポリシー

ほとんどの場合、の最新のソフトウェアリリースを使用すると、新しく発見されたすべての脆弱性に対するセキュリティパッチを確実に利用できます。システムにパッチを適用しないまま長期間放置すると、攻撃者が脆弱性を悪用し、システムが危険にさらされるリスクが高まります。

推奨ポリシーと手順
が最新であることを保証するために、展開されたソフトウェアのバージョンを定期的に評価し、パッチ適用ポリシーを定義することが重要です。また、パッチ適用ポリシーでは、サーバーとクライアントの両ソフトウェアの更新に関連する作業の管理責任者を明確にする必要があります。の場合、最新のリリースは*www.axis.com*にあります。は最新の.NETライブラリを必要とするため、Windowsのパッチ適用ポリシーをのポリシーに合わせるように注意する必要があります。

装置ファームウェア更新ポリシー

最新のファームウェアバージョンには、攻撃者が悪用しようとする可能性のある既知の脆弱性に対するパッチが含まれています。したがって、最新のファームウェアバージョンで装置を稼動させると、装置のほとんどの一般的なリスクが軽減されます。Axisは、セキュリティパッチやバグ修正を含む装置ファームウェアの長期サポート (LTS) リリースを提供していますが、プラットフォームの長期的な安定性を確保するため、機能追加は制限されています。ファームウェア開発に関するAxisの戦略の詳細については、*Axisファームウェア管理*ホワイトペーパーを参照してください。

推奨ポリシーと手順
ハードウェア装置については、すべてのファームウェアを最新の状態に保つことをポリシーに明記する必要があります。プロセスでは、の内蔵ファームウェア更新機能またはAXIS Device Manager Extendを活用して、Axis装置の新しいファームウェアバージョンが利用可能かどうかを確認できます。通常、営業時間外に、すべてのカメラのファームウェアアップグレードを展開するスケジュールを設定する必要があります。/AXIS Device Manager Extendでは、ファームウェアの更新が受け入れられたかどうかも確認できます。更新によって影響を受ける可能性のある特定の統合がシステムにある場合、LTSファームウェアトラックを標準化することを検討してください。

ネットワークセキュリティ

リモートアクセスポリシー:

インターネットにさらされている装置やサービスは、外部の敵が既知の脆弱性を探ったり悪用したりするリスクを高めます。たとえば、リモートビデオアクセスが必要な小規模な組織でインターネットにさらされるカメラは、脆弱なパスワードが使用されたり、新しい致命的な脆弱性が発見されたりすると、簡単に被害者となります。Windows環境へのリモートアクセスは、厳重にコントロールするか、可能であれば避ける必要があります。Windows環境では、システムを更新するための利便性の問題としてインターネット接続が装備されている可能性がありますが、Windows Remote Desktop、TeamViewer、AnyDeskなどのリモートデスクトップサービスを利用すると、正しく管理されていない場合、システムにアクセスできる経路が発生します。

推奨ポリシーと手順
絶対に、インターネットから直接アクセスできるような方法でカメラのIPアドレス/ポートを公開しないでください リモートビデオアクセスが必要な場合は、Axis Secure Remote Accessを使用してください。は、クラウドベースのリモートアクセスサーバーを使用し、クライアントまたはAXIS Camera Stationモバイルアプリケーションを経由したシステムへの暗号化リモートアクセスを容易にします。リモートアクセスサーバーは、リモートユーザーやモバイルユーザーの接続管理を行うだけでなく、リモートユーザーが使用する際の整合性を保護するという重要な役割を果たします。Axis Secure Remote Accessの詳細については、*こちら*を参照してください。Axisは、AndroidとApple iOSの両方に公式ブランドのモバイルアプリケーションを提供しています。AXIS Camera Stationモバイルアプリは、Google PlayストアとApple App Storeのそれぞれ公式ソースからのみダウンロードしてください。

Windows環境へのリモートデスクトップアクセスに関しては、を実行しているシステムにこの種のアクセスを提供することはお勧めしていません。ただし、必要な場合は、選択したリモートデスクトップアプリケーションがセキュリティで保護され、アクセスが必要な個人にのみ提供されるように細心の注意を払う必要があります。多要素認証 (MFA) のような追加的な管理レイヤーの導入をお勧めします。誰が、どのような時間にWindows環境にリモートアクセスしたかを追跡するために、リモート接続試行のログとその後の監査を強くお勧めします。

ローカルネットワーク露出ポリシー

ローカルネットワークの露出を減らすことで、攻撃対象領域を縮小し、多くの一般的な脅威を軽減することができます。ネットワークの露出を減らすには、物理的なネットワークセグメンテーション (ネットワークハードウェアとケーブルの分離)、仮想LAN (VLAN) による論理的なネットワークセグメンテーション、IPフィルタリングなど、さまざまな方法があります。AxisのカメラはIPフィルター (IPテーブル) をサポートしているため、装置は明示的に許可されたIPアドレスからの接続要求のみに応答します。

推奨ポリシーと手順
AXIS Camera Station S22 NVRsは、デュアルネットワークポートを持つハードウェアサーバーです。ポートの1つはカメラ用にセグメント化されたネットワークを構築し、もう1つはプライマリネットワーク (ドメイン) に接続してビデオクライアントにサービスを提供します。サーバーはカメラネットワークのブリッジおよびファイアウォールとして機能し、クライアントがカメラに直接アクセスすることを防ぎます。これにより、プライマリネットワーク上の敵からの脅威の可能性が低くなります。

サーバーとカメラがすべてプライマリネットワークに配置されている場合は、カメラのIPフィルターを設定し、をホストするサーバー、AXIS Device Manager、および追加のメンテナンスクライアントにのみアクセスを制限することを推奨します。

ネットワーク暗号化ポリシー

安全でないネットワークを通して転送されるネットワークトラフィックは、常に暗号化する必要があります。インターネットは安全でないネットワークに分類されます。ローカルネットワークも安全でないネットワークに分類される場合があります。そのため、ネットワークトラフィックも暗号化する必要があります。ネットワーク上のビデオトラフィックにどのようなポリシーを適用するかは、ビデオがどのように分類されるか、また、敵対者がビデオシステムにネットワークアクセスするリスクによって決まります。当社の推奨事項として、ネットワークはすでに侵害されていると想定してください。大規模な組織では通常、ネットワークの分類方法を定義するポリシーがあります。

推奨ポリシーと手順

ビデオクライアントとサーバー間のトラフィックは暗号化を使用する必要があります。サーバーとカメラ間のトラフィックは、インフラストラクチャに応じて暗号化する必要があります。Axisカメラは自己署名証明書を備えており、HTTPSがデフォルトで有効になっています。悪意のあるコンピューターがカメラになりすまそうとする場合など、ネットワークスプーフィングのリスクがある場合は、CA署名証明書を使用した秘密鍵インフラストラクチャー (PKI) を使用する必要があります。には、Axis装置のサーバー証明書の署名と配布をコスト効率よく管理できるローカル認証局 (CA) が組み込まれています。

TLSバージョン

TLSバージョン1.1および1.0を無効にすることをお勧めします。AXIS Camera Stationのインストーラーが、インストールやアップグレード中にサポートを提供します。

HTTPS暗号

はTLS暗号スイートをサポートし、HTTPS接続を安全に暗号化します。具体的な暗号スイートは、に接続するクライアント、あるいは接続されたサービスに依存し、がTLSプロトコルに従ってネゴシエーションを行います。*RFC 7540*に記載されているTLS 1.2暗号スイートを使用しないようにWindowsを設定することをお勧めします。暗号スイートを無効にする機能は、と一緒に使用する装置とカメラによって異なります 。装置やカメラが特定の暗号スイートを必要とする場合、弱い暗号スイートを無効にできないことがあります。

データ管理

ビデオ分類

ライブビデオや録画ビデオは分類する必要があります。ビデオは、パブリック、プライベート、制限付き、または組織のポリシーによって定義されたその他のクラスに分類されることがあります。多くの場合、ビデオは法律や地域の規制、社内のITポリシーによって規制されているため、ビデオデータに適用される法律や規制を把握しておくことはシステム所有者の責任です。

推奨ポリシーと手順
組織のデータ分類ポリシーに従って、ライブビデオ、録画ビデオ、音声を分類します。ビデオや音声データの機密性に応じて、ユーザーのアクセス権限やシステムの強化を設定します。必要ではない場合、装置レベルで音声を無効にすることができます。

追加のセキュリティコントロール

追加のセキュリティコントロール

組織の成熟度レベルやリスク許容度にもよりますが、日常運用におけるサイバーセキュリティリスクを低減するために、CIS Controls v8からさらにいくつかのセキュリティコントロールを導入することをお勧めします。

追加のCISコントロール:

コントロール8: 監査ログ管理
攻撃の検知、理解、回復に役立つ可能性のあるイベントの監査ログ、アラートを収集し、レビューおよび保持します。

コントロール14: セキュリティ意識およびトレーニングプログラムの実施
従業員のスキルと行動を理解します。さまざまな形態の攻撃を識別する方法について従業員を訓練します。

コントロール17: インシデント対応と管理
インシデント対応/管理のフェーズや担当者の役割、セキュリティインシデントを関係当局や第三者に報告する方法などが明確に定義された、文書化されたインシデント対応計画を活用すること。

システム強化ガイド
AXIS Camera Station Pro

バージョン M1.7
日付: 2024年4月
製品番号 T10203603