ネットワークのセキュリティに関するガイドライン

アクシスコミュニケーションズ株式会社

はじめに

本文書は、ハッカーにより悪用されやすい、起こり得る監視脆弱性に関連した質問を想定したガイドラインと、そのような脆弱性を最小化するための専門家によるアドバイスを提供します。

背景

すべてのネットワーク機器は、ネットワークカメラも含め脅威にさらされることを前提としています。カメラが攻撃される理由は様々です。ほとんどのケースでは、システムの破壊とそのサービスを妨害することです(DoS 攻撃)。時には内部ネットワークへのアクセスを入手する、という目的もあります。

ネットワークカメラは常にネットワークが屋台骨となる、より大きなシステムの一部として組み込まれます。それがシステムであれ個々の機器であれ、すべてのシステム構成要素は攻撃を受けやすく、保護が必要です。保護レベルは、その攻撃や破壊行為が引き起こすであろう影響や損害を基に定義されます。

アクシスは、カメラ一台の小さなモニタリングから大規模な企業向けソリューションまで、幅広いソリューションに対する要求を満たすべく奮闘しています。小規模システムにおいては、ソフトウェアが適切なセキュリティレベルをセットアップするようオーナーより求められます。中規模ソリューションでは販売業者、インテグレータ、もしくは設置業者が十分な保護を提供するように、大規模においてはしばしば専任の担当者がシステムの保護を構成しメンテナンスするよう、それぞれ求められます。システムの保護を増強させると、アクセシビリティに影響を及ぼします。ほとんどの場合、それが保護の目的そのものとなります。また、アクセシビリティがシステム保護の低減によるコスト削減より重要になることもあります。

テーマ： 一般的なセキュリティの脆弱性

Q: ネットワーク機器におけるリスクにはどんなことがありますか？

A: 適切に保護されたシステムを破壊するには、時間、リソース、および知識が必要になります。カメラもしくは監視システムが攻撃にさらされるリスクは、攻撃する側にとってどのくらいの価値があるのかによります。多くの場合、システムへのアクセスや権限をソーシャルエンジニアリングにより手に入れ

るのが容易であるといえます。監視システムは破壊行為の対象になる可能性がより高いです。アクシスは改竄やいたずらを検知し通知する、いたずら防止製品を提供しています。

Q: アクシスはセキュリティの問題に対し、どのように取り組んできたのですか？

A: アクシスの R&D は“安全第一”で、堅牢で回復力のあるファームウェアとそのインターフェースを開発します。アクシスの品質管理部門はよくある脆弱性をすべて検知する、最上級のスキャンツールを使用しています。アクシスは、システム周辺の脅威および脆弱性に対する品質と知識を常に向上させるべく、外部のコンサルタントや独立調査会社と協働しています。

アクシス製品に使用されているファームウェアは Linux をベースにしています。オープンソースのコミュニティは常にモニターされ、欠陥があれば基幹部分とサービスの両方がアップデートされます。アクシスは独自のサービスや機能を持つ製品と共に、最新の利用可能なオープンソースパッケージをベースにファームウェアを構築します。

Q: アクシスの製品やソフトウェアにはトラブルシューティングのための仕様書に書かれていない“抜け道”があり、それがハッカーにより悪用されてしまうということはありますか？

A: アクシス製品には抜け道になるサービスは存在していません。

Q: ハッキングが起きた場合、被害に遭ったユーザーをどのようにサポートしますか？

A: カメラが攻撃されたのか破壊されたのかを判別するのは難しいものです。これはカメラのアクセスログやネットワーク管理モニタリングログに現れるものです。アクシスのサポートチームは、お客様がシステム攻撃を受けた際に脆弱性があるかどうかを判別すべく、常にスタンバイしています。アクシスはカメラのファームウェアを通じて新しい機能、バグの修正、およびセキュリティパッチを継続的にアップデートし、お客様を積極的にサポートしています。脆弱性が発見された過去の例では、アクシスは速やかにファームウェアのアップデートを提供して参りました。脆弱性が深刻なものであるとみなされた場合には、生産終了品に対してもアップデートを提供します。修正されたファームウェアはアクシスのサポートページ(http://www.axis.com/techsup/index.htm)より、無償にて、追加の情報と共に提供されます。深刻な脆弱性が発見された場合、アクシスは登録ユーザーやパートナーの皆様にコンタクトを取ることもあります。

テーマ：セキュリティシステムインテグレーション

どのようなシステムソリューションのタイプであっても、アクシスの製品やサービスが安全に運用されるようにインターフェースや機能を提供します。

アクシスはスタンダードソリューションを利用し、マルチレベルのユーザー認証/権限、パスワードの保護、SSL/TLS 暗号化、802.1X、IP フィルタリング、および証明書管理を含む、数々のインターフェースと機能を提供します。これによりアクシスの製品は様々なタイプのセキュリティソリューションに統合され利用可能となります。

テーマ：システム設定とメンテナンス

Q:システムにおける一番の弱点は？

A: 適切に設定されメンテナンスされていないシステムが、期待されるセキュリティレベルまで到達することはまずありません。残念なことに、そのようなことがシステムにおいて一番の弱点となることがしばしばあります。システムの保護がおざなりになってしまう理由として、知識がない、不便になる、アクセシビリティと保護において利害が対立する、オーナー、役割、責任の範疇が明確でない、プロセスやツールの不足、などがあります。セキュリティプロセスの欠如はソーシャルエンジニアリングのリスクを増加させ、ハッカーが機密情報の所有者をだまして情報を漏えいさせてしまうことにつながります。

Q: アクシスはどのように弱点を克服できるようサポートしているのですか？

A: アクシスはセキュリティ効率を最大化しメンテナンスすべく、機能やおすすめツールを提供しています。たとえば、直感的なインターフェース、システム/アクセスログ、および情報文書の提供など、システム管理者の皆様の運営にかかる負荷を減らす支援をしています。

Q: 最も安全な方法でカメラをセットアップできるように、アクシスではどのようなトレーニングを提供していますか？

A: アクシスコミュニケーションズアカデミー(アカデミー)では、素早く簡単に、お客様がどのような環境にあっても監視システムを最善な形で設置し、セッティングを最適化させられるよう、ツールやトレーニングを提供しています。アカデミーでは設置や設定のための特別なラーニングプログラムを開催しています。

Q: システム保護を強化する、共通の奨励事項はありますか？

A: 以下の事項をすべて徹底することが重要です。

1. システム保護と脅威の可能性についての知識を得ることです。リセラー、システムインテグレータ、コンサルタント、製品ベンダーとよく連携しましょう。

2.脅威となること、および攻撃を受けた際のダメージや損害の可能性に対するリスクを分析しましょう。これにより、リスクを減らすための予防策とどのくらいの保護レベルが必要とされているのかが示されます。

3.ネットワークを保護しましょう。ネットワークプロテクションが破壊されると、機密情報が詮索され、個々のサーバーやネットワーク機器が攻撃されるリスクが増加します。

4.機器の出荷状態のデフォルト設定に頼ってはいけません。

a. デフォルトのパスワードを変更する。

b. デバイス保護サービスを作動させる。

c. 利用していないサービスをストップさせる。

5.強力でユニークなパスワードを利用し、定期的に変更する。

6.システムに要求されるのでなければ、カメラが直接インターネットにアクセスできるようにするのはやめましょう。クライアントによるビデオへのアクセスが求められるのであれば、メディアプロキシを利用しましょう。

7.できれば、ローカルネットワークにおいても暗号化された接続を使いましょう。

8.アクセスログを定期的にチェックし、承認されていないアクセスの試みを検知しましょう。

9.定期的に機器をモニターしましょう。システム通知がサポートされていれば作動させましょう。

10.利用可能な最新のファームウェアを利用しましょう。セキュリティパッチが含まれることがあります。

テーマ：コンテンツの保護

Q: メーカーは「どこからでも映像が見える」と宣伝しています。どのようにしてシステムが安全であると確証できるのですか？

A: 多くのシステムにおいて、コンテンツには機密情報が含まれます。アクシス製品はコンテンツを守り、暗号化、サービスの停止、プライバシーマスキングなどのプライバシーやデータ規制に準拠する機能を提供します。

以上