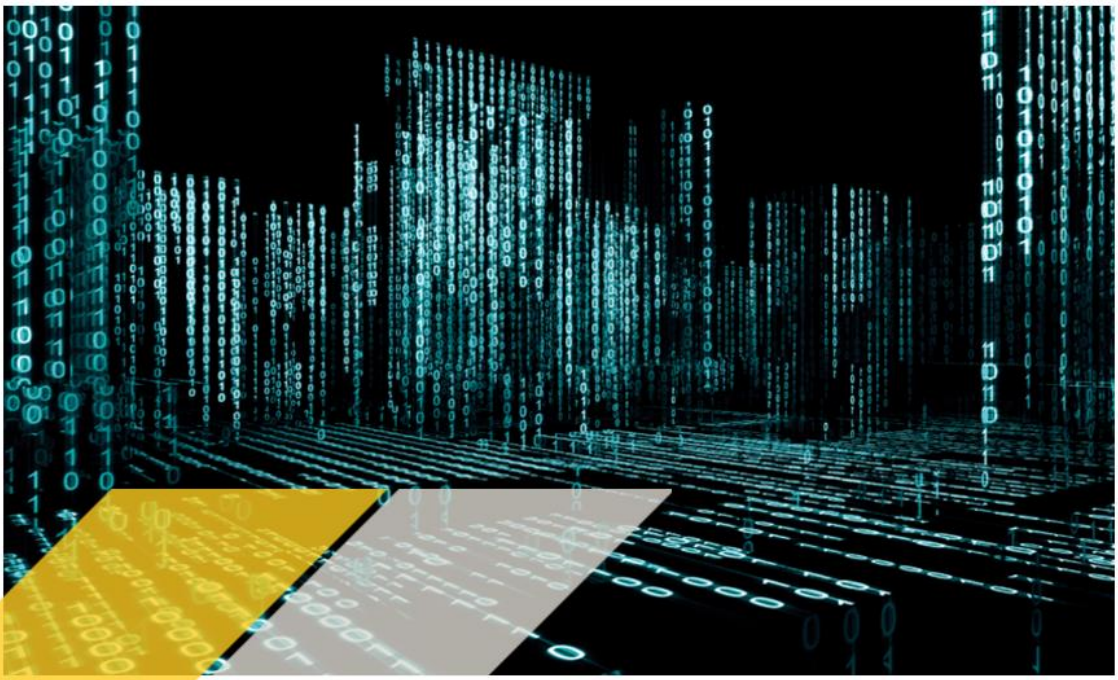

IPカメラ - ネットワークのドアを開けたままにしない

IoTのビジョンは、接続されたデバイスによる広範なネットワークが提供する利便性、機能、柔軟性によって魅力的に見えますが、ネットワークへの入り口が劇的に増えるため、セキュリティの脅威や侵害に対するリスクも増大します。Ciscoの最近の調査では、73%のビジネス意思決定者たちが、「今後2年間でIoTによってセキュリティの脅威がより深刻になる」と回答しています。さらに心配なのは、78%のITセキュリティ専門家たちが、ネットワークに接続された新たな種類のデバイスのセキュリティを保護することについて、「その能力に不安があるか、可視性と管理が欠如している」と考えています。

ネットワークへのアクセスの可用性を高めると、侵害に対するリスクも高まります。システムを設計する際には、念入りなシステム脅威/リスク分析を行う必要があります。システムに追加するどのアプリケーションについてもそうですが、新しいコンポーネントを追加するたびに攻撃露出エリアが増えます。Microsoft Office Suiteをすべてのコンピューターにインストールすると新たなサイバーリ

スクが増えることと同じように、映像システムを追加すると新たな露出エリアが増えます。映像システムのコンポーネントは他のネットワークリソースにリスクをもたらす可能性があり、逆にネットワークに他のリソースを追加すれば、映像システムにリスクが生じる可能性があります。攻撃対象エリアを最小化するというのは、一般的なサイバー保護対策です。**デバイス、サービス、アプリケーションが相互に作用する必要がないのであれば、相互間の接続を制限することを検討できます。**映像システムを残りのネットワークから分離させるのは、総合的に優れた保護対策となります。これにより、映像リソースとビジネスリソースが互いにマイナスまたは危険な影響を及ぼし合うリスクを減らせます。

ネットワークカメラは、ノートパソコン、デスクトップコンピューター、モバイルデバイスなどネットワーク上の他のデバイスとは異なり、ユーザーが潜在的に危険なWebサイトを訪問する、悪意のあるメール添付ファイルを開く、不審なアプリケーションをインストールするなどの脅威には晒されません。しかし、インターフェースのあるネットワークデバイスである以上、カメラや接続された他の物理セキュリティデバイスもリスクを表面化する可能性があります。ですから、これらのリスクの露出エリアを減らすことが重要です。

映像セキュリティシステムのセキュリティを確保する、つまり強化するプロセスについて理解することは、設置者およびIT担当者にとってますます重要になっています。優れた強化ガイドは、進化する脅威の環境に対処できるよう特定のユーザー要件にかなった設定戦略を提供します。Axisは、強化ガイドのベースラインとして、『SANS Top 20 Critical Security Controls』を使用しています。その最初のステップは、業界標準のセキュリティプロトコルを理解および使用することです。これには、マルチレベルユーザー認証/許可、パスワード保護、SSL/TLS暗号化、802.1X、IPフィルタリング、証明書管理が含まれます。

また、Axisのようなカメラメーカーは、常に新しい機能、バグ修正、セキュリティパッチを含む形でカメラのファームウェアを更新しています。セキュリティリスクの危険度、種類、量が増えるなか、セキュリティシステムのユーザーは、メーカーが提供する最新のアップデートを活用し、ネットワークカメラをベースにしたシステムを対象にする攻撃を防ぐためのベストプラクティスに留意する必要があります。