ホワイトペーパー

物理アクセスコントロールのデジタル化とサイバーセキュリティ

企業がアクセスコントロールの可能性を最大限に引き出し、よりスマートで安全な世界を実現できるようにするためのシステムとプロトコルの検証

7月 2021

AXIS COMMUNICATIONS

目次

1 まとめ

クラウド接続の発展は、物理セキュリティ業界の様相を変え、設置担当者はビジネスを維持するために適応することを余儀なくされています。アクセスシステムの管理は、グローバルテクノロジー企業の領域に移行すると考えられ、システムのインテリジェント化やエッジベース化が進み、拡張性が高くなるにつれて、システムがもたらす価値が大幅に上がると期待されます。

また、この進化、そして他の企業システムとの統合の可能性は、特に既存のインフラ上にシステムを構築する場合、システムの開発と展開においてサイバーセキュリティがさらに大きな役割を果たすことが必要となることを意味します。シリアルアーキテクチャやMACアドレスの欠如などの技術的な障壁を克服することは、現在と今後の要件を満たすことができるデジタルアクセスコントロールシステムへの移行における重要なステップです。

アクセスコントロール向けのデジタルシステムを展開して保護することは、最高水準のセキュリティを確保するためのベストプラクティスに従うことでもあります。デバイス、サプライヤー、プロトコルなど、システムに関連するあらゆる要素の評価とテストを行い、すべての信頼性を実証する必要があります。また、脅威の状況と、新たに発見された脆弱性や欠陥によってもたらされるリスクを軽減する方法を、常に把握することも必要です。

ベンダーのデバイスがネットワークに接続することを許可するため、特にベンダーについては特別な考慮が必要です。プロフェッショナルなベンダーは、強化ガイドの公開や、ネットワークデバイスの管理と保護を容易にする専用の管理ツールの提供などにより、製品を保護するための独自のプロセスを提供しています。また、発見された脆弱性や欠陥を管理するための戦略について、オープンで正直なベンダーが望ましいと言えます。

2 はじめに:アクセスコントロールの今後

クラウド接続は、物理セキュリティ業界に、システムをどのように展開して利用すべきかという新しいビジョンを提示しました。エンドユーザーと購入者は、従来のテクノロジーが提供するものをはるかに超える、監視機能とアクセスコントロール機能を備えた、よりスマートで統合され、よりビジネスに焦点を合わせたソリューションを求めています。

多くのサプライヤーは、物理セキュリティに関する専門知識、サービス、知識を中心として、強力なビジネスモデルを構築してきました。しかし、ネットワーク接続とIoTは、絶えず変化する状況をもたらし、物理セキュリティの従来のベンダーや設置担当者は、ITの言語、つまりオープンプラットフォーム、IP接続、ソフトウェア統合などを学び、市場の変化に適応して現状に即した存在であり続ける必要があります。

支配力は、電子アクセスシステムのサプライヤーから、その従来の運用の正当性に問題を投げかける方向へとセキュリティを形成する力を持つ、グローバルテクノロジー企業に急速に移行しているようです。スマートビルディングやスマートシティには大きな機会があり、導入の容易さと今日のテクノロジーの高度化がスマート環境に多くのメリットをもたらすため、多くの人が現代のアクセスコントロール市場の急速な成長を予測しています。

ビッグ・テックの影響により、世界的に新型コロナウイルス感染症が大流行している間、非常に大きく依存されていたクラウドテクノロジーの成功が実証されているため、ホスト型アクセスコントロールの採用に向けた動きが生まれるのは当然のことです。このような企業には、根本的な変化をもたらす思考力、規模、想像力があり、物理セキュリティもビジネスとして変換され、クラウドの価値を実現し、セキュリティ要件とビジネス要件のすべてを処理するホスト型ソリューションに目を向けます。

しかし現在、多くのメーカーはこの変化する市場に対応する準備ができておらず、今なお、厳格な独自の設計に基づくビジネスモデルを採用しています。スマートな物理セキュリティソリューションへの移行は、今後、真価を大きく問われるであろうこの従来のアプローチとは真逆の位置に存在します。変化は一夜にして起こるものではなく、新しいクラウドホスティングソリューションはまだ主流にはなっていませんが、この明るい新たな世界は、現在私たちの業界に参入する新しいエンジニアの領域となっています。

したがって、アクセスコントロールの今後、そして物理セキュリティ全体は、より大きな価値に対する期待にもとづいています。アクセスコントロールシステムはデータ収集ポイントとなり、ドアコントローラーはインテリジェントなI/Oデバイスとなります。訪問者管理用QRコードと、摩擦のないアクセスコントロールを実現する生体認証顔認識は、カメラやセンサー内の分析機能として、ますますエッジで管理されるようになります。アクセスコントロールの今後は、それを受け入れて具現化する、つまり、よりスマートで安全な世界のために革新する真の機会に対する準備ができている人々にとって、刺激的でやりがいのある時をもたらします。

本書では、アクセスコントロールシステムの多数の基本的な機能を含め、アクセスコントロールに特に関連する側面について説明します。また、プロバイダーに説明を求め、より賢明な購入決定を行うためのエンドユーザー向けの情報や提案とともに、サプライヤー向けのベストプラクティスに関する考慮事項についても説明します。

3 進化するアクセスコントロール市場における課題

物理アクセスコントロール (PACS) に焦点を当てる場合、物理的入室の許可または阻止に関する考察の観点からリスク要因に対処する傾向があります。物物理アクセスコントロールシステムの設計にバランスの取れたアプローチを取ることは、潜在的な脅威の評価に基づく重要な考慮事項です。

今日、施設はますます高度な電子アクセスコントロールソリューションによって保護されているため、これらのシステムは、企業全体のアクセスを管理するための迅速かつ効率的な方法を提供し、必要に応じて調査したり監視したりできるデジタルフットプリントを残します。また、HRや訪問者管理などの他のシステムと完全に統合されています。

ビジネスとセキュリティに関する意思決定に加え、アクセスコントロールを支援する強力な洞察が得られるこのシステム統合では、システムのサイバー成熟度を徹底的に評価することが重要になります。犯罪者がますます巧妙になり、脅威の状況が進化し続ける中、課題は、アクセス認証情報の複製、内部脅威、またはリモートによるサイバー攻撃のリスクを軽減することにあります。

しかし、アーキテクチャ自体が問題を生じさせます。従来のアクセスコントロールシステムの多くは、古いインフラ上に構築されています。このインフラを一般的に利用するセキュリティテクノロジーの統合において、ベンダーにとっての課題は、ハードウェアをこれらの企業ネットワークに接続できるよう適応させることと、ITセキュリティの重要性と、企業にもたらされる多くのリスクを徹底的に評価して防御する必要性を促進する、セキュリティ環境の変化を認識することです。

サイバーセキュリティに関する考察は、新しいセキュリティシステムの開発における重要な要素となります。アクセスコントロールテクノロジーは、物理セキュリティソリューションにおいて不可欠な役割を果たすため、認識されているサイバーセキュリティの原則、インシデントレポート、およびベストプラクティスに従って作られる必要があります。システムの完全性は、その最も脆弱な部分と同程度の強度であることを認識することが重要です。**それを受け入れる準備ができていないシステム**は、暴露の潜在的なリスクとなります。公的に認識された復旧対応を受け入れ、通知し、実施する準備ができているこ

とを実証できない場合、これは最終的に、展開された物理セキュリティの必要なレベルを提供する能力に悪影響を及ぼします。

3.1 サイバーセキュリティ実績 (サイバー成熟度)

IT業界の関与の高まりにより、テクノロジーの評価、展開、保守の方法に変化が起き始めています。IT利害関係者にとって重要な考慮事項は、ベンダーのサイバーセキュリティの知識に重点を置いた、企業のサイバーセキュリティ実績の評価です。この知識は、サイバー成熟度とも呼ばれます。この成熟度が高いということは、脅威の状況とリスクの軽減について十分に理解していることを示唆します。ネットワークカメラ用にすでに作成されている広範なサイバーセキュリティのドキュメントとガイダンスは、物理アクセスコントロールにも適用できます。サイバーリスクと攻撃の可能性に関する課題、評価、説明は、これらの製品にも同様に関連するためです。

3.2 セキュリティシステムアーキテクチャの今後

最新のアクセスコントロールデバイスは、ネットワークケーブルとRJ45コネクターを介して接続されます。ネットワークは、アクセスコントローラー、およびデバイスと中央管理システム間の通信に電力を供給します。アクセスコントロールの推進力は、TCP/IPベースのシステムへの移行です。2013年に初のIP対応ドアコントローラー (AXIS A1001) が発表されて以来、PACSは進化を続け、現在では、レガシーテクノロジーだけでは不可能であった、幅広い高度な機能を提供しています。

このような革新の例としては、タッチフリーアクセスコントロールを促進するQRコードリーダー、ネットワークカメラとの統合による顔認識、ナンバープレートの読み取りなどがあります。これらはすべてPACSデータベースと連動して、入場の許可または拒否についてエッジベースの決定を行います。IPシステムの主な利点には、シンプルな設定とデバイス管理による低設置コストが含まれます。他のデバイスとの容易な統合は、新しいセキュリティテクノロジーと拡張機能が利用可能になったときに、それらのシンプルなプラグアンドプレイ接続を可能にする、将来性に優れたソリューションを実現します。

3.3 IP 対 従来のアクセスコントロール

IPの利点は、最新のアクセスコントロール設計、特にエンドユーザーが標準として期待する非接触システムで実現されます。また、ユーザーは、アクセスコントロールがモバイル認証だけでなく、スマートフォンやタブレットの使用に適応することを望んでいます。業界はどのようにして、より優れた、より便利で時間とコストを節約するアクセスコントロールシステムを提供するのでしょうか？また、大手テクノロジー企業が推進するイノベーションサイクルに対応できるのでしょうか？これらは、業界のサプライヤー側の課題です。

これまで、こういった機会は活用されていませんでした。レガシーアクセスコントロールシステムは、シリアルアーキテクチャに設置され、RS-485ケーブルで中央ユニットまたはサーバーに接続された、ドアコントローラーに依存しているためと考えられます。また、ほとんどのシステムは独自仕様です。つまり、ドアコントローラーは「ロック」されており、サプライヤーが指定したソフトウェアでのみ管理できます。これにより、エンドユーザーは単一のハードウェアサプライヤーとソフトウェアサプライヤーに制限されるだけでなく、システムが複雑なため、設置や設定に専門家が必要になる場合が少なくありません。

従来のアクセスシステムを拡張する場合、一般的な中央コントローラーは特定の数のドアに対応するよう設計されているため、プロセスが複雑になり、非標準の構成によってシス

テムの柔軟性が制限されるため、コストが高くなります。たとえば、ドアを1つ追加するだけで膨大なコストがかかり、不当に高額になる可能性があります。

IPネットワークにより、はるかに優れた柔軟性とカスタマイズを実現する、非常にシンプルで設置が容易なPACSアーキテクチャの導入が可能になりました。ITプロフェッショナルは、真のIPデバイスと、そのネットワークベースのアクセスコントロールシステムでの使用に、強くこだわっています。こういった人々を将来の設計プロセスに含めることが重要です。彼らは拡張のコストを削減する上でも重要であり、将来のアクセスコントロール設計の要件となる、IPデバイスの使用を保証するためです。

3.4 オープンプロトコル

アクセスコントロールの今後は、オープンプロトコルフォーラムでスキルと能力を共有する、メーカーの積極性と結びついています。このオープン性に対し抵抗があるのは明白です。多くのアクセスシステム開発者は、エンドユーザーを独自のソリューションに結び付け、将来の収益を保証するプロセスを好む傾向にあるからです。ただし、このアプローチには長期的な価値はありません。ユーザーはソリューションから、より多くのことを求めており、そのためには喜んでデータを共有します。

システム設計者とアクセスハードウェアのサプライヤーが、総合的な物理セキュリティシステムの一部としてユーザーが要求する、すべてのソリューションを提供するためのリソースやITのノウハウを持っていることは、めったにありません。多くの企業は、それぞれのビジネスモデルとアクセスコントロール市場での地位を脅かす革新的な新しいソリューションによって、自社の製品やサービスの価値が急速に失われていることを、真に理解していないようです。このような最新システムの能力と最新イノベーションの速度によって、アクセスコントローラーをまったく必要とせず、インテリジェントI/Oユニットが代替品となるときは、すぐそこに近づいています。

オープン性により、ベンダーは、シンプルさを鍵とし、購入と設置のコストが競争力を必要とする、小規模アクセスシステムに適したデバイスを構築することができます。これらの同じデバイスは、必要に応じて、より大規模で、より技術的に複雑な運用に適応させることができます。この柔軟性は、最新のセキュリティの特徴であり、ユーザーのビジネスが成長し、要件が変化しても、現在購入したシステムが将来にわたって有用であることを保証します。

オープン性とオープンテクノロジーの詳細については、オープンな標準規格に向けた開発を推進するために設立された業界フォーラム、ONVIFのWebサイト (*www.onvif.org*) をご覧ください。

4 採用に対する技術的障壁

デジタルアクセスコントロールを可能にする技術的な接続、インターフェース、およびデバイスに関しては、考慮すべきことが多くあります。従来のシステムからクラウド対応システムへの移行の結果として、予期しない影響が生じる可能性があります。次のセクションでは、既存のテクノロジーを支援するために考慮しなければならないポイントと、それに関連するプロセスについて詳しく説明し、新しいソリューションのアップグレードと採用の障壁になるのを防ぎます。

4.1 RS-485コントローラー

1つの考慮事項は、RS-485コントローラーの展開と、メディアアクセスコントロール (MAC) アドレスをほとんど持たないために識別が困難な、セミインテリジェントデバイスを設置する潜在的なリスクです。RS-485 (TIA-485 (-A) またはEIA-485とも呼ばれる) は、シリアル通信システムで使用するドライバーとレシーバーの電気的特性を定義する規格です。電気信号は平衡であり、マルチポイントシステムがサポートされています。ただし、RS-485はジェネレーターとレシーバー、つまり物理層のみを指定します。重要な通信層は管理しません。

MACアドレスがないことやシリアルアーキテクチャの採用は、それ自体が信頼性の問題となったり、アクセスコントロールシステムの運用に悪影響を与えたりすることを意味するものではありません。このような設計は、30年以上にわたりアクセスコントロールの主力となっています。ただし、アクセスコントロールシステム内のすべての制御デバイスがインテリジェントであり、個別に対処できない限り、セキュリティに対する期待値の進歩を視覚化することは困難です。私たちは、完全にインテリジェントなシステムと完全にアクセス可能なデバイスだけが、期待される将来の価値を提供できると考えています。「完全にアクセス可能」とは、サイバーセキュリティが不十分なデバイスを意味するわけではありません。その逆です。

4.1.1 オープン監視デバイスプロトコル (OSDP)

IECによって承認され、アクセス通信のセキュリティを強化する可能性を提供する新しい通信方法が、Open Supervised Device Protocol (OSDP)、アクセスコントロール製品とセキュリティ製品間の相互運用性を向上させるためにセキュリティ産業協会 (SIA) によって開発されたアクセスコントロール通信規格です。OSDPは、128ビット暗号化を使用するとともに、マルチドロップ接続に対応し、接続を監視してリーダーの問題を報告します。さらに注目すべき点は、OSDPはカードリーダー、ドアストライク、アラーム接点、および以前はドアごとに必要であった複数の接続ではなく、2本のワイヤーを使用して機能を終了するリクエストをサポートすることです。SIA Webサイトでは、次のように報告されています。「OSDPは、2020年5月に国際電気標準会議によって国際規格として承認され、2020年7月、IEC 60839-11-5として公開されます。SIA OSDPは、業界をリードする地位を維持するため、継続的に改良されています。」

4.2 MACアドレスを持つデバイスの価値

MACアドレスは、単一のネットワークアダプターまたはデバイスの、世界的に一意のハードウェアアドレスです。ITネットワークにおいて、MACアドレスはIPアドレスと同じくらい重要です。MACアドレスは、LAN上のコンピューターを一意に識別し、TCP/IPなどのネットワークプロトコルが機能するために必要です。MACアドレスはデバイスにハードコードされており、オペレーティングシステムを介してスプーフィングすることは可能ですが、もちろんこれは非推奨であり、アドレスはセキュリティソリューションで保護する必要があります。

TCP/IPおよびその他の主流のネットワークアーキテクチャは一般的に、ネットワーク機能が層に分割される開放型システム間相互接続 (OSI) モデルを採用しています。MACアドレスはデータリンク層 (OSIモデルの第2層) で機能し、コンピューターがネットワーク上でコンピューター自体を一意に識別できるようにします。MACアドレスフィルタリングは、セキュリティの層を追加します。デバイスがネットワークに接続することを許可する前に、ルーターはデバイスのMACアドレスを承認済みアドレスのリストと照合します。クライアントのアドレスがルーターのリストにある場合はアクセスが許可され、そうでない場合はアクセスが拒否されます。

4.2.1 Power over Ethernet (PoE)

PoEは、アプリケーションにわたり一貫した2つの利点、コスト削減とデバイス配置の柔軟性を提供します。PoEは一本のケーブルでデータと電力を送るため、従来の設計よりもデバイスアーキテクチャを簡素化することができます。多くのアクセスコントロールシステムが、IP接続として宣伝されていることは注目に値します

5 ベストプラクティスの特徴

アクセスコントロール管理は、人の流れを効果的に処理し、アクセスを管理するための重要な要素です。企業は、ドアをロックしたりバリアを設置したりするだけでなく、顧客サービス関係を強化し、常に高レベルなセキュリティと安全性を実現するための、より優れた管理オプションを必要としています。包括的なアクセスコントロールに対するベストプラクティスアプローチの採用は、適切なツールの選択にとどまりません。適切なアーキテクチャを導入すること、高品質の技術を取り入れること、適切な手順とプロトコルに従うこと、そしてスタッフと利害関係者が正しい態度と行動をとるよう奨励することが必要です。

5.1 利害関係者の管理と集中型セキュリティアプローチ

サイトがシームレスに機能するために必要な運用テクノロジーを提供するために、テクノロジーが同じインフラストラクチャーに集中するにつれ、統合された意思決定プロセスも必要になります。集中型セキュリティアプローチが壁を打ち破り、さまざまなビジネスチームが連携できるようになった成功例はすでに見てきました。この集中性は、従来の電子セキュリティ製品と物理セキュリティ製品が企業ネットワーク上に並んで存在する今日ほどは、重要ではありませんでした。

物理セキュリティチームは、運用要件をサポートし、関連するリスクに対処すると同時に、ITセキュリティポリシーをサポートし、物理デバイスが企業ネットワークへのバックドアにならないようにするテクノロジーに依存できることが重要です。すべての利害関係者が連携することで、安全なサイバー環境と物理環境を構築することができます。

5.2 パートナー、ベンダー、サプライヤーに期待されること

サードパーティが、セキュリティのベストプラクティスをすべての作業の最前線に保つことの重要性を理解し、特定のニーズを満たすように運用することを保証することが重要です。サードパーティとの関係は、健全なサプライチェーンを確立し、強力で信頼できる絆を築くための鍵です。

サードパーティとそのサプライチェーンへの影響を評価する際の重要な考慮事項:サイバーセキュリティに関連するリスクを理解し、認識している > 利用可能なプロセスとツールを使用して、成熟したサイバーセキュリティアプローチを実証できる > 自社の製品・サービスに対する規制や法律の影響を理解している > ユーザーのコンプライアンス要件をサポートする方法を提示できる > サイバーセキュリティは、テクノロジーだけでなくプロセスでもある - ユーザーの企業を保護するためのサイバーセキュリティライフサイクル管理を提示できる。

5.3 セキュリティ管理:ガバナンスとベンダープロセス

あらゆる効果的なセキュリティと同様に、サイバーセキュリティでも防御の深さが重要です。つまり、選択する製品、パートナー、要件など、すべてのレベルにおいてIPカメラネットワークを適切に保護する必要があります。

5.3.1 規格と指令

ISO 27001 - 情報セキュリティ管理、ISO/IEC 27001は、以下を必要とするセキュリティ管理システムです。

- 脅威、脆弱性、および影響を考慮した、組織の情報セキュリティリスクの体系的な調査
- 容認できないと見なされるリスクに対処するための、一貫性のある包括的な情報セキュリティ管理および/または他の形式のリスク管理 (リスク回避や移転など) の設計と実装
- 情報セキュリティ管理が組織の情報セキュリティニーズを継続的に満たすようにするための、全体的な管理プロセスの採用

5.3.2 Cyber Essentials Plus

Cyber Essentialsは、政府と業界が支援しているスキームで、組織が一般的なオンラインの脅威から自社を保護するのに役立ちます。Cyber Essentialsは、サイバーセキュリティがもたらす課題を理解している企業にとって効果的な指標で、企業のポリシーとプロセスの評価です。具体的には次のことを確認します。

- 安全な構成
- アクセスコントロールと管理
- マルウェア保護
- パッチ管理
- ファイアウォールとインターネットゲートウェイ

テクノロジーメーカーにとって、防御の最前線は、自社のシステムに関連するリスクの軽減である必要があります。2014年10月1日付けで、政府は、特定の機密情報および個人情報の取扱いを含む契約に入札するすべてのサプライヤーに、Cyber Essentialsスキームに従って認定を受けることを要求しました。

5.3.3 Secure by Design、Secure by Default

2019年に監視カメラコミッショナーによって立ち上げられた「**Secure by Design、Secure by Default (設計段階からの保護、デフォルトによる保護)**」は、監視カメラシステムとコンポーネントのメーカーに最低要件を定めています。このスキームは、メーカーに、症状を治すのではなく、根本原因であるセキュリティ問題の解決に対して包括的なアプローチを取り、確実に対応してシステムやコンポーネントの全体的な危害を減らすことを求めています。

「Secure by Design、Secure by Default」には、正しいセキュリティプリミティブがソフトウェアとハードウェアに組み込まれていることを保証するための、長期的な技術的取り組みが含まれています。また、市場が迅速に導入できるように、これらのプリミティブが入手・使用可能であることを保証するという、同じく要求の厳しいタスクについてもカバーされています。

当社のテクノロジーをサポートするため、Axisは「Secure by Design、Secure by Default」を国家サイバーセキュリティ戦略の行動規範に合わせました。

- パスワード入力要求
- パスワード強度インジケーター

- HTTPS暗号化
- 802.1x
- リモートアクセス 無効化済み (NAT traversal)

6 ガイドとツール (ベンダープロセス)

ネットワークのセキュリティ保護に関しては、多くの場合、組織は複数の技術的管理を展開し、単一障害点と露出の制限に役立つ「階層型防御」アプローチを構築します。ただし、見過ごされがちな重要なプロセスの1つは、「システムの強化」です。これには、情報セキュリティの脅威に対するシステムの安全性向上を目的とした、デフォルトのシステム設定への設定変更が含まれます。このプロセスは、すべてのシステムに存在する、固有の脆弱性の低減にも役立ちます。

6.1 製造強化ガイド

ネットワークに接続されているすべてのデバイスに対して、システム強化プロセスを実施する必要があります。これには、ワークステーション、サーバー、その他のネットワークデバイスが含まれます。各メーカーは、自社のシステムの設定と構成をどの会社よりもよく把握しているため、パートナーとユーザーに、デバイスの完全性とエンドユーザーのシステムの保護に必要な情報を提供するのはメーカーの責任です。強化ガイドは、映像監視ソリューションの導入に携わるすべての人を対象とした技術的アドバイスを提供する必要があります。ベースラインの設定を確立するとともに、進化する脅威に対処するための包括的な情報を提供する必要があります。

すべてのベンダーは、デバイスの設計、開発そして試験に対して最善のサイバーセキュリティ対策を講じ、不正行為によって悪用される可能性のある欠陥のリスクを最小限に抑えるよう努めなくてはなりません。しかし、ネットワークやそのデバイス、そしてネットワークによりサポートされるサービスを保護するには、ベンダーのサプライチェーン全体とエンドユーザー組織が積極的に連携する必要があります。環境が安全かどうかは、ユーザー、プロセス、テクノロジーによって決まります。優れた強化ガイドは、CISコントロール - バージョン6.1などのベースラインの使用法に沿って作成します。これらのコントロールは、以前はSANS Top 20 Critical Security Controlsとして知られていました。

6.2 デバイスの管理

デバイスマネージャーは、接続されたデバイスを管理するための、シンプルで費用対効果に優れた安全な方法を提供するオンプレミスツールです。設置担当者とシステム管理者に、設置、セキュリティ、メンテナンスに関する、あらゆる主要タスクを管理するための非常に効果的なツールを提供します。

デバイスインベントリ/アセット管理システム：

- アカウントとパスワードに関するポリシー
- ファームウェアのアップグレードやアプリケーションの効率的なインストール
- サイバーセキュリティコントロールの適用 - HTTPSの管理、IEEE 802.1x 証明書のアップロード、アカウントとパスワードの管理

- 証明書のライフサイクル管理 - 設置、セキュリティ、運用に関するすべての主要タスクを管理
- 新しいデバイスを素早く簡単に設定 - 設定のバックアップと復元
- あらゆる規模の現場に最適 — 1つまたは複数の設置場所

6.3 OEM / ODMに関連する課題

相手先ブランド供給 (OEM) とは、他社の製品を自社の名前やブランドで再販するメーカーです。相手先ブランドによる設計・製造 (ODM) は、他社が指定し、最終的にブランド化して販売する製品を設計・製造する会社です。このような企業は、ブランド会社が工場の立ち上げや運営を行わずに、生産に従事することを可能にします。

別のサプライヤーによる製品のOEMまたはODMに頼る製造業者には、多くのメリットがあります。まず、製造のリスクとコストを排除し、企業が販売およびマーケティングプロセスに集中できるようになります。これは、セキュリティ業界全体で、多くのカメラメーカーが自社ブランド製品をOEMまたはODMする主な理由の1つです。96社ものベンダーが、別のサプライヤー製のOEMまたはODMカメラを販売していると報告されています。

これにはいくつかの課題がありますが、最も明白なものの1つがサイバーセキュリティです。あるメーカーの製品に脆弱性がある場合、これは、サプライチェーン全体の他のすべての再販業者とパートナーに影響を与える可能性があります。また、サプライチェーンの完全な可視性を困難にすることがあります。膨大な数のOEMとODMが稼働しているため、デューデリジェンスを実施し、特定のメーカーのテクノロジーを拒否したエンドユーザーが、無意識のうちにそれらのテクノロジーをリブランドされた形式で使用し、その事実にまったく気づかない可能性があります。

6.4 CPUマイクロプロセッサチップ

デバイスにインストールされている一般的なCPU処理チップがハッカーの標的にされており、多くの脆弱性が特定されていることが明らかになっています。これの主な理由の1つは、特定された単一の脆弱性からハッカーが生成する拡張性です。最近の例には、関連する2つの脆弱性、「Meltdown」と「Spectre」が含まれます。これは、特権のないコードを使用してデータに不正アクセスする機能を持つ、最新のCPUマイクロプロセッサに対するサイドチャネル攻撃です。

スマートフォンからデータセンターのハードウェアまで、ほとんどのデバイスはある程度脆弱であると言えます。大手のオペレーティングシステムベンダーは、問題を軽減するパッチを作成しましたが、パッチの一部はプラットフォーム固有の要素を含むため、設備メーカー (OEM) を介してインストールする必要があります。ナショナルサイバーセキュリティセンター (NCSC) は、速やかにデバイスにパッチを適用するようアドバイスしています。

6.5 ファームウェア戦略

署名付きファームウェアはエンドユーザーにとって重要であり、ロジスティクスや配布の工程でデバイスが改ざんされるリスクを軽減します。署名 (ハッシュとも呼ばれる) は、配布時にファームウェアに追加されます。プロセッサは独自のハッシュを計算し、信頼する証明書によって署名されたハッシュと一致するハッシュを持つファームウェアイメージのみをロードします。

6.6 脆弱性の管理

サイバー犯罪とそれに関連するリスクの継続的な増加により、多くの組織は情報セキュリティにさらに注力することを余儀なくされています。組織は、情報セキュリティリスク管理の取り組みに、脆弱性管理プロセスを含める必要があります。このプロセスにより、IT環境の脆弱性とそれに関連するリスクの概要を継続的に把握することができます。IT環境の脆弱性を特定して低減することによってのみ、攻撃者によるネットワークへの侵入と情報窃取を防ぐことができます。

サプライヤーは、すべてのシステムの脆弱性を検出して修正するプロセスや、プロセス変更時や新しいシステムの展開時に新たな脆弱性が発生するのを防ぐプロセスなど、運用に脆弱性の管理を含めることが重要です。サプライヤーが受諾するリスクに関連するすべての問題についてエンドユーザーに伝達し、同意を求める必要があります。この原則が実行されない場合、攻撃者がシステム内の脆弱性を悪用し、企業とそのサプライヤーに対してサイバー攻撃を仕掛けてくるおそれがあります。

セキュリティ侵害を防止するため、ITセキュリティパッチとセキュリティ脆弱性の更新は、承認されたプロセスを通じてタイムリーにインストールする必要があります。何らかの理由で更新できないサプライヤーシステムには、脆弱なシステムを保護するための対策を講じる必要があります。すべての変更は、サプライヤーの変更管理プロセスに従って行う必要があります。

6.7 セキュリティアドバイザリ通知

セキュリティアドバイザリは、既知の脆弱性によるリスクを軽減するのに役立ちます。セキュリティアドバイザリは、公式のCVE (Common Vulnerability and Exposure (共通脆弱性識別子)) またはその他の脆弱性レポートを参照する場合があり、脆弱性の説明、リスク評価、推奨事項、およびサービスリリースが利用可能になる時期に関する情報が含まれます。ほとんどのベンダーは、間接販売モデルを展開し、パートナープログラムを設けています。

セキュリティアドバイザリ通知を使用することで、製造元が実施しているパートナープログラムに登録されていない顧客は、チャネルに通知されたときに、早期に関連するサイバーセキュリティ通知を取得することができます。これは、設備を設置しているものの、最初に設置を行った会社と契約を結んでいないエンドユーザーにとって重要なツールです。

6.8 セキュア開発成熟度モデル (Building Security in Maturity Model (BSIMM))

BSIMMは、組織が自社のソフトウェアセキュリティを他のイニシアチブと比較して、評価できるよう確立された、ソフトウェアセキュリティ測定フレームワークです。BSIMMは、以下のプロセス、アクティビティ、役割、および責任を評価するのに役立ちます。

- 設計および構造の見直し
- コードの見直し
- 既知の脆弱性のテスト
- オープンソースパッケージのCVE脆弱性を発見できる、標準の脆弱性スキャンツールの実行

6.9 長期サポート (LTS)

長期サポート (LTS) は、安定したソフトウェアリリースが標準版よりも長期間維持される、製品ライフサイクル管理ポリシーです。長期サポートファームウェアには、安定性、パフォーマンス、セキュリティのためのパッチのみが含まれます。ベンダーは、デバイスが市場に投入されてから最大10年間、LTSファームウェアを提供します。

LTSは、既存の有効なソフトウェアサポートと並行して、ただし独立して存在することが期待されます。LTSサポートの主な利点の1つは、元のファームウェアバージョンに関連するサードパーティとの統合を維持できることです。

6.10学習と連携

テクノロジーベンダーを選択する際に考慮すべき重要な領域の1つは、提供されるトレーニングとサポートです。チャネルと業界が直面する課題、特にサイバーセキュリティの課題が進化するにつれて、メーカーはこの問題に積極的に取り組み、市場に販促用品やコンテンツを提供するよう努める必要があります。以下のような例が挙げられます。

- サイバーセキュリティに関する無料の集合形式のコース
- オンラインによるサイバーセキュリティトレーニング
- オンラインによるサイバーセキュリティに関するクイックテスト
- 強化ガイド
- 脆弱性ポリシー
- サイバーセキュリティのベストプラクティス
- サイバーセキュリティに関するコンセプトや用語集

7 サイバー衛生プロファイルの作成: 次のステップと考慮事項

優れたサイバー衛生には、組織の主要なサービスと製品に対するリスクの特定、優先順位付け、および対応が含まれます。サイバー衛生セキュリティのベストプラクティスを展開することで、データ侵害や不適切なシステム設定を防止するとともに、ビジネスに関連するリスクを最小限に抑えることができます。リスク管理の主な目的に焦点を合わせるため、主要な脅威の領域について利害関係者の合意を得ることが重要です。

完全なリストではありませんが、次の考慮事項は、サイバー脅威に対する対処の効率性向上に役立ちます。

7.1 サプライヤー

登録や認証を確認する

適切な登録や認証を確認します (ISO 9000登録やその他の品質認証の証拠の要求など)。サプライヤーの製品が、企業ネットワークでの使用向けに設計されているかどうかを確認します。

ベストプラクティスの証拠を取得する

選択したプロバイダーが、サイバーセキュリティのベストプラクティスを実施できることを確認します。プロバイダーは、ネットワークの保護に役立つサイバーセキュリティ対策、物理セキュリティ対策、ベストプラクティスに関する説明が記載された、サイバー強化ガイドを提供できる必要があります。

プロバイダーを監査する

購入を確約する前に、徹底的な監査を実施します。取引条件を確認し、明確で透明性があることを確認します。財務上の観点から、ビジネスに問題が発生した場合の製品とサポートへの影響を尋ねることが重要です。

継続的なサポートのためのリソースを確認する

プロバイダーが、将来必要になると予想されるソリューションを構築し続けるためのリソースを備えているかどうかを見極めます。プロバイダーが、今後のビジネス要件をサポートできる規模、範囲、能力を備えていることを確認します。

今後のビジネスニーズを明確にする

自社の今後のニーズに焦点を合わせます。インテリジェントなデバイスとソリューションには、ビジネスを強化し、将来を見据える能力があるため、メンテナンス契約と継続的なサポートによって、サプライヤーが期待以上のものを提供すると確信できる必要があります。

倫理的なビジネスの運用を検証する

倫理的かつ持続可能なビジネスの証拠を確認します。信頼と共通の目標に基づいて構築されたパートナーシップは、長期的な存続に対する強力な基盤です。プロバイダーは、環境管理システム、企業の社会的責任 (CSR) プログラム、倫理的な調達方針などを実施していますか？

7.2 製品とシステム

デューデリジェンスを実施する

システムとそのコア要素に対して技術的なデューデリジェンスを実施し、システムが価値を提供すること、そして現在の運用に影響を与える可能性のある根本的な要因がないことを確認します。リスク評価とリスク軽減に関する情報が、明確かつ利用可能であることを確認します。

メンテナンス契約を確認する

メーカーのソフトウェアアップデートやファームウェアアップグレードなど、サービス・メンテナンス契約に含まれているものを確認します。

接続されたデバイスを保護する

ネットワークに接続された物理セキュリティシステムが、安全であることを確認します。セキュリティシステムは、デフォルトのユーザー名とパスワードの変更、最新のファームウェアのインストール、暗号化 (理想的にはHTTPS) の利用、リモートアクセスの無効化など、サイバーセキュリティを念頭に置いて展開する必要があります。

デザインセキュリティの明細書を要求する

サプライヤーは、ネットワークに接続されたデバイスのサイバーセキュリティの状態の証明として、デザインセキュリティの明細書を提供できる必要があります。

システムのインテリジェンスを評価する

総合的にインテリジェントな接続デバイスとは、MACアドレスでネットワーク化され、システムアーキテクチャの本質的な部分を形成するデバイスです。MACアドレスのないデバイスはインテリジェントではなく、個別に識別、管理、保護することはできません。

GDPR/ データ保護法へのコンプライアンスを評価する

EU一般データ保護規則 (GDPR) は、「1998年データ保護法」の改正とともに、2018年に発効しました。製品とシステムが「2018年データ保護法」とGDPRに準拠する機能に対応していることを確認してください。

T10168631/ja/M1.7/2107

Axis Communicationsについて

Axisは、セキュリティの向上とビジネスの新しい推進方法に関する洞察を提供するネットワークソリューションを生み出すことで、よりスマートでより安全な世界の実現を目指しています。 ネットワークビデオ業界をけん引するリーダーとして、Axisはビデオ監視および分析機能、アクセスコントロール、インターコムおよび音声システムなどに関連する製品とサービスを提供しています。 Axisは50ヶ国以上に3,800人を超える熱意にあふれた従業員を擁し、世界中のパートナーと連携することで、カスタマーソリューションをお届けしています。 Axisは1984年に創業し、スウェーデン・ルンドに本社を構えています。

Axisの詳細については、弊社Webサイト *axis.comをご覧ください.*