

ネットワークの健全性を改善する方法

サイバーセキュリティ
健全なネットワークのための
10のベストプラクティス

AXIS[®]
COMMUNICATIONS

はじめに

サイバー攻撃が頻繁にニュースの見出しとなっている今、サイバーセキュリティが優先課題となっていることは不思議ではありません。企業に対するサイバーセキュリティの脅威はかつてなく高まっており、頻度と巧妙さが増大しています。

しかし、最近の統計によると、多くの組織は既存の脅威と進化する新しい脅威に対する備えができておらず、CIOおよびCISOの3人中2人が、自分の組織にとってサイバーセキュリティは優先事項ではないと述べています。* 幸いなことに、大多数の攻撃は、自社のサイバー対策の弱点を理解し、脆弱性を抑える計画を作成して実施することにより、くい止めることができます。

お客様の組織には情報セキュリティに関する効果的な計画がありますか?不正侵入が発生したときのサイバーセキュリティインシデント対応戦略をお持ちでしょうか?サイバーセキュリティポリシーについてスタッフを積極的に教育してきましたか?

脆弱性を特定して健全なネットワークを確かなものにする方法を理解しておくことは、サイバーレジリエンスの重要な側面です。しかし、ネットワークを脅威から確実に保護することで、それを必要とするユーザーがこれまでと同様にネットワークへアクセスすることが難しくなる場合があります。そのため、貧弱なネットワーク健全性の兆候を識別し、先手を打ってネットワークのセキュリティを改善できるようにすることが重要です。

* 2015 Global Megatrends in Cybersecurity” Ponemon Institute LLC – Raytheonに対して実施





この電子ブックでは、次の内容について説明します。

- 貧弱なネットワークの健全性の兆候を特定する方法
- データとネットワークを保護する戦術
- 映像監視システムがサイバー犯罪者にとって有益である理由
- サイバーセキュリティに関する社内文化の構築
- 現行システムの改善やメンテナンスに役立つリソース

物理的なセキュリティと同様、効果的なサイバーセキュリティは、脆弱性の識別、脅威の評価、適切な対策の実施からなる継続的なサイクルです。ネットワークを強力に保護する必要性は日々明白となっています。強固な防御を確実にするため、ネットワークだけでなく接続されているすべてのデバイスも強化していくことを検討してください。お客様のネットワークは最大限に保護されているでしょうか？



貧弱なネットワークの健全性の兆候を特定する方法

強化されたネットワークに加え、先手を打ってサイバー脅威を監視して対処するポリシー、プロセス、ユーザーが存在し、組織で定めたサイバーセキュリティ目標に足並みをそろえていれば、お客様のネットワークは健全といえます。普通の人々ために、サイバーセキュリティに注力することで増大するリスクに対し、苦境に立つことのないよう適切な手段を検討する必要があります。

セキュリティの実装が貧弱なネットワークはハッカーにとって非常に魅力的であり、多くの場合にウイルスやマルウェア、およびその他のサイバー脅威の急速な拡散につながります。しかし、ネットワーク上で活動するユーザーが非常に多くなっているため、生産性に影響を与えずに高いレベルのセキュリティを維持することが難しくなっています。

お客様と使用しているネットワークの、攻撃に対する備えはできていますか?お客様のネットワーク健全性に改善が必要かどうかを特定する方法をいくつか見てみましょう。いったん特定し調査すれば、包括的なサイバーセキュリティ計画を構築するためにポリシーや手順を修正していくことができます。

ITチームとセキュリティチームが足並みをそろえていない

ITチームはおそらく、インターネットが発明されたときからサイバーセキュリティについて考えています。ITポリシーは多くの場合、運用ネットワークでパスワード管理や標準のネットワークプロトコルなどの問題に対応するために存在します。しかし、おそらくIP監視ネットワークにはITポリシーが適用されていないでしょう。

ITチームとロス防止チームの間ではしばしば考え方が異なりますが、特にサイバーセキュリティについては、足並みをそろえることが大切です。足並みがそろっていない可能性を示す兆候には次のものが含まれます。

- > 異種のネットワークでポリシーやプロセスが異なるか、存在しない
- > パスワード管理が貧弱または不明瞭
- > すべてのシステムでセキュリティ手段を確認する権利または責任を持つ担当者が存在しない
- > ネットワークで送信されるビデオストリーム用に最新の高度な暗号化方式が使用されていない
- > ネットワークに接続されているハードウェアとソフトウェアがITポリシーに適合していない



ネットワークユーザーがポリシーや手順に従っていない（または知らない）

ポリシーや手順はきちんと整っていますか？すべてのユーザーが容易に理解できるように文書化されていますか？

ITチーム向けのクイックヒント：
ITポリシーを実施し、それが会社のコンピューターとサーバーに適用されていることを確認してください。

答えがノーである場合、お客様は貧弱なネットワーク健全性の兆候の犠牲者になる可能性があります。下に挙げるのは、この兆候を診断できる追加の質問です。

- > 従業員はITポリシーに関する教育を定期的を受けていますか？
- > 新しい従業員は入社したときに適切な教育を受けていますか？
- > デバイスのパスワードについて、従業員向けの具体的なガイドラインが存在していますか？

セキュリティ侵害における人的エラーの例を尋ねられた際、42%の個人ユーザーは、エンドユーザー側でのポリシーの不履行や不注意に責任があると述べています。*

*CompTIA "2015 Trends in Information Security"

インストールとメンテナンスの計画 がはっきりと文書化されていない

物理的なインストール (IP監視カメラや他のネットワークデバイスの設置) とメンテナンスに関する問題も、サイバーセキュリティに関する問題の原因となることがあります。インストール担当者は、インストール時に要求される特定のニーズを理解していないことがあります。非常に多くのベンダーがいるため、インストール担当者がベンダーのセキュリティに関するベストプラクティスの一部または全体を実行していないことも考えられます。

さらに悪いことに、セキュリティ、IT、施設、およびメンテナンスの各部門がメンテナンス計画について足並みをそろえていないこともよくあります。そうした場合、システムの定期的なメンテナンスさえも一緒に実行されていません。

ネットワークに接続されたデバイスのインストールとメンテナンスに関する文書化された計画はありますか？

「正しいことを初めて行うときに大変なのは、それがどれほど難しいことであるかをだれも認識していないことです。」

- Walter J. Wright

4

使用するテクノロジーベンダーがサイバーセキュリティについて話をしない

ベンダーに対する質問:

- > 御社の製品に何らかのバックドアはありますか?
- > 御社は何らかのデータ収集を行っていますか?
- > 御社の最新の脆弱性レポートはどこから入手できますか?

選択した機器はお客様のITポリシーに適合していますか?またはベンダーに合わせてポリシーを調整していますか?賢く選択してください。

テクノロジーベンダーに関する警告となる兆候には次のものがあります。

- > サイバーセキュリティについての話をしない。
- > デバイスを強化する方法やベストプラクティスに関するガイドを持っていない。
- > 自社の製品に対する侵入テストを実行していない。
- > 第三者のサイバーセキュリティコンサルタントと協力して自社製品のリスクを評価していない。

それぞれのテクノロジーはより大きなシステムの一部であり、多くの場合、システムは完全には保護されていません。エコシステムの一部だけが保護され、他の部分は保護できない可能性もあります。最も弱い部分の強度がシステム全体の強度となります。パズルの各ピースは可能なかぎり保護されているでしょうか?



健全なネットワーク のための10のベ ストプラクティス

貧弱なネットワークの健全性を特定する方法がわかりましたら、次はネットワークのサイバーセキュリティを改善する方法について確認します。IT、セキュリティ、および施設管理の各チームと協力することで、一般的なリスクの多くを軽減することができます。

強力な一意のパスワードを使用する

ほとんどのIPベースのデバイスは、出荷時にデフォルトのパスワードと設定が付いています。これらのパスワードは推測が容易であったり、オンラインで公開されていたりすることもあります。これは、サイバー犯罪者がお客様のシステムに不正アクセスを試みる際の最も一般的な方法です。

パスワードを活用して攻撃を止める最も効果的な方法は次のとおりです。

- > 強力な一意のパスワードを設定する
- > パスワードを正しく確実に管理する
- > パスワードの代わりに証明書を使用する
- > パスワードを定期的に変更する

ご存じですか？

一般的な単語や名前をパスワードにした場合、どんなに長くても数秒のうちに破られてしまいます。パスワードクラッキング計算機は、暗号化されたパスワードのクラッキングにかかる時間を文字数に基づいて見積もります。熟練したハッカーがお客様のパスワードを破るのにかかる時間はどれほどでしょうか？

当社では、8文字以上の推測しにくいパスワードの使用をお勧めしています。

2

推奨された方法でデバイスを展開してインストールする

デバイスを展開する際に使用しないサービスを有効にしておくと、攻撃を受けやすくなる可能性があります。たとえば、サイバー犯罪者は、ファイル転送プロトコル (FTP) や信頼されていない開発者によるアプリケーションプラットフォームを使用して、悪意のあるアプリケーションやスクリプトをインストールしてしまいます。使用しないサービスを無効にし、信頼されているアプリケーションのみインストールすることにより、加害者がシステムの脆弱性を突く可能性を下げることができます。

デバイスを正しくインストールすることもセキュリティ問題を回避するのに役立ちます。たとえば、人の手が届く位置にカメラを設置すると、いたずらされたり破壊されたりする危険があります。カメラは、シーンをはっきり観察できる画角を持つとともに攻撃者の手が届かない位置に設置する必要があります。



明確な役割と所有権を定義する

多くの組織では、特定のアクセス権限を持つ従業員を定める明確な規則や手順がなかったというだけの理由でネットワークセキュリティ障害が発生しています。

たとえば、監視システムのセキュリティ手段を確認してベストプラクティスを実施されていることを確かめる責任者がはっきりしていない場合があります。当社はお客様に、“アカウントに与える権限は最小に”の原則に従うことをお勧めしています。つまり、仕事を行うのに必要なリソースに関する権限だけをユーザーに与えるという意味です。

露出を減らすため、ソリューションで要求されていないかぎり、映像にアクセスするデバイスがカメラに直接アクセスできるようにすることは避けてください。クライアントはVMS (ビデオ管理システム) かメディアプロキシ経由でのみ映像にアクセスできるようにします。



4

適用可能な最新のファームウェアを使用する

ワークステーション、サーバー、カメラ、プリンター、およびその他のネットワークデバイスのオペレーティングシステムにバグや欠陥が存在すると、組織がリスクにさらされる可能性があります。

よく知られている2014年のHeartbleedバグはその良い例です。これは、ハッカーがサーバーの秘密鍵とユーザーパスワードを盗めるようになったOpenSSLのセキュリティ脆弱性でした。

この脆弱性が公表されるのとほぼ同時にパッチがリリースされましたが、ユーザーがそのパッチをインストールしなければ脆弱性は残ったままでした。そのため、適切に文書化されたメンテナンス計画を持ち、ネットワークデバイスに現行のファームウェアとセキュリティ更新を適用しておくことが非常に重要です。

多くのベンダーは一般的な脆弱性を明らかにし、特定の脆弱性に対する解決策や回避策を文書化したレポートを公開しています。ご使用のデバイスは使用可能な最新のファームウェアによって更新されていますか？




リスク分析を実行する

サイバー脅威の分析では、損失する可能性のある金額と保護にかかる必要のある費用額を定義します。潜在的な脅威に加え、システムが攻撃または侵入された場合に発生する可能性のある損害とコストを分析します。鍵となる資産を識別し、特に価値のあるものを保護するための取り組みに優先順位を付けます。

考えてみましょう:

- > 何を保護する必要があるか?
- > 脅威や脆弱性となるのは誰/何か?
- > 資産が破損または消失するとどうなるか?
- > 組織にとって価値のあるものは何か?

危険をもたらす可能性のある資産の脆弱性について必ず検討してください。分析と優先順位付けを行う際は、内部と外部の両方の脅威について考えてください。



2015年に行われたサイバー攻撃の60%は内部関係者によるものであり、そのうち44.5%は“悪意のある”攻撃とみなされました。*

* IBM “2016 Cyber Security Intelligence Index”

6

システムの保護と発生する可能性のある脅威についての知識を習得する

リスク分析に続いて、ネットワーク上で稼働しているシステムそのものを細かく確認してください。ベンダーのサプライチェーン全体と緊密に協力して、選択したデバイスをネットワークで使用する際に発生する可能性のある脅威について理解します。

現在、多くのITベンダーはネットワークで自社のデバイスを保護するためのベストプラクティスやガイドを文書の形式で提供しています。選択したベンダーがこの種の情報を提供していない場合は、この件についての話し合いを始めるか、別のユーザーが作成した資料を入手することが大切です。

真の意味で統合されたシステムではデバイス同士が相互にやり取りする必要があるため、システムを個々のデバイスではなく全体として理解してください。すべてのデバイスは、単体で使用した場合だけでなく、協働するように構成した場合でもITポリシーに適合する必要があります。



デバイスの工場出荷時設定を変更する

いかなるデバイスも工場出荷時の設定のまま使用しないでください。パスワードは特に重要です。パスワードの変更は最初に行う必要があります、システムを保護するために実行できる最も重要なステップの1つです。* 何と云っても、パスワードはネットワーク全体への入口となるからです。

一般的なデバイスのデフォルトの管理アカウントIDとパスワードは、単純なGoogle検索で容易に発見できてしまいます。工場出荷時設定のままにしておけば、ハッカーがさらに侵入しやすくなります。デバイスの保護サービスを有効にして構成し、使用しないサービスは常に無効にします。

デフォルト設定はデモ目的でのみ使用します。最小規模のシステムであっても、デフォルト設定を使用すると脆弱になってしまいます。

*これはベストプラクティス1ですすでに述べたことであり、非常に重要です!



暗号化された接続を使用する

ローカルや“内部”のネットワークを含むすべてのネットワークで、暗号化された接続を使用する必要があります。

システムで、一般的な認証プロトコルであるHTTPダイジェスト認証とHTTPSの少なくとも1つが使用されていることを確認してください。これにより、すべての情報がネットワークで送信される前に確実に暗号化されます。これらのプロトコルにより、悪意のあるコードによって暗号化されていない通信を待ち伏せて盗聴するタイプの攻撃の可能性を効果的に減らすことができます。たとえ保護しているのが財務データでなくとも、お客様のデータには暗号化によって保護するのに十分な重要性があります。

ITチームに感銘を与える話題

HTTPダイジェスト (アクセス) 認証は、Webサーバーが認証情報とユーザーの身元 (ユーザー名やパスワードなど) を確認するために使用できる、合意に基づく方式の1つです。

HTTPS (HyperText Transfer Protocol Secure) は、現在最も一般的なデータ暗号化プロトコルです。HTTPSはHTTPとほとんど同じですが、ひとつの重要な違いとして、転送されるデータがSecure Sockets Layer (SSL) や Transport Layer Security (TLS) を使用してさらに暗号化される点があります。

ネットワークを保護する

ネットワーク保護に欠陥があると、機密情報が探られて個々のサーバーやネットワークデバイスが攻撃されるリスクが増します

ご使用のファイアウォールとフィルターについて理解してください。時間をかけてネットワークをバックボーンから保護すれば、サイバーセキュリティのベストプラクティスを実施するその他のすべての取り組みを補強することができます。

システムの選択から実装とメンテナンスまでのプロセス全体にわたって、ITチームと協力してください。



10

システムとプロセスをメンテナンスする

システムの適切なメンテナンスは、達成が特に困難なプラクティスの1つですが、全体的なシステム健全性にとって非常に重要です。

すべてのデバイスを定期的に監視し、適用可能で、機能としてサポートされている場合はシステム通知を有効にしてください。また、アクセスログを定期的にチェックして不正アクセスが試行されたかどうかを検出する必要があります。

計画が実行された後は、検証と評価を定期的に行う必要があります。ペースの速いテクノロジーの世界では、新しいアップデート、機能、およびベストプラクティスが絶えず作り出されています。メンテナンス手順を必ず文書化し、現在と将来の同僚がプロセスを理解できるようにしてください。



映像監視とサイバーセキュリティに関する現実

「なぜAxis Communicationsは私のサイバーセキュリティに関心があるのだろうか?」とお考えかもしれません。そこには、監視映像が貴重なデータ資産であり、他のすべての機密データと同様に多くの不正な目的で使用される可能性があるという現実があります。犯罪者は盗んだ映像を見て、高リスクの資産領域を特定したりVIPの行動パターンを追跡したりできるほか、カメラを妨害して業務を混乱させることもできます。いたずら、破壊行為、映像サービス拒否などの潜在的な脅威もあります。

IP監視システムはローカルエリアネットワーク上に存在するため、ITポリシーで考慮に入れる必要があります。また、IPカメラは他のネットワークデバイス、クライアント、サーバーなどと同様に保護する必要があります。

脅威はシステムレベルで管理する必要があります。お客様の組織のサイバーセキュリティはお客様だけの問題ではありません。ネットワークとそのデバイスやサービスを保護する責任はベンダーのサプライチェーン全体に及びます。同時に、ユーザー、プロセス、およびテクノロジーも考慮する必要があります。

ネットワークセキュリティ侵害の大多数は、人的エラー、怠慢、誤った構成、および貧弱なメンテナンスが原因です。ITネットワークセキュリティポリシーが監視ネットワークに適用されていない場合もありますが、これらのポリシーを考慮に入れることは不可欠です。

お客様には選択する力があります。既存のネットワーク保護を低下させることなく保護された映像システムをインストールする方法を推奨している映像監視メーカーを選択してください。ITチームおよびソリューションプロバイダーと協力し、リスク分析、システム展開、メンテナンスを実施してください。





サイバーセキュリティに関する社内文化を構築する

貧弱なネットワークの健全性が頻繁に組織を苦しめています。お客様の組織ではそのようなことがないようにしてください!サイバーセキュリティのプラクティスに関する従業員の知識を増やすことで、セキュリティリスクを30%下げることができるという報告があります。*

サイバーセキュリティに関する仲間を増やしてください。組織内でITポリシーについて知っているユーザーが多いほど、組織の状況は良くなります。サイバーセキュリティチームに属さないユーザーも、ポリシーに同意して従うだけでなく、完全に理解している必要があります。

おまけのベストプラクティス

安全なネットワークの作成と維持はチームによる取り組みであり、多くの異なる部門からの支持が必要です。1人では行うことができません。

計画を整えた後は、組織全体にそれを伝え、ネットワーク内で新しくデバイスを選択したりインストールしたりする際の最重要事項としてください。

では、どうすればサイバーセキュリティに関する社内文化を構築して維持できるでしょうか?計画を作成する際は次の点を考慮してください。

- > 従業員の健全性に関する教育に投資する
- > 新しい従業員の入社時にプロセスについて教育する
- > サイバーセキュリティの重要性を強調することを上級幹部に依頼する
- > 進化を続けるサイバー脅威について、その発生とともに継続的に学習し、既知の脅威を組織の適切なメンバーに伝える
- > サイバーセキュリティを新しいネットワーク機器を選択する際の要件として確認する
- > BYOD (自分のデバイスを持ち込む) ポリシーを実施する
- > 侵害が発生したときのサイバーセキュリティインシデント対応戦略を作成して適用する

組織全体がお客様のサイバーセキュリティ計画と足並みをそろえることにより、ネットワークおよびデバイスのセキュリティを保証するうえでより良い立場につくことができます。

* 2015 Global Megatrends in Cybersecurity (Rep.). (2015).Ponemon Institute LLC. 実施者: Ponemon Institute©

結論と追加のリソース

サイバーセキュリティ脅威が増大し、進化を続けていることにより、ネットワークの健全性について先手を打つことがこれまでになく重要になっています。リスクを軽減して侵害に対処する計画を持つことは、組織が現在の脆弱性を軽減して将来の潜在的なハッキングを回避することにつながります。

データとネットワークを保護する戦術に従うことにより、侵害を難しくし、時間とリソースの両面で代償の大きいものとすることができます。

成功の鍵となる次の主要な要因は、以下のとおりです。

- > ITポリシーを、監視ネットワークを含むすべてのネットワークで実装する
- > サプライチェーン全体を関与させる
- > ユーザー教育を優先度を上げて取り組む
- > サイバーセキュリティを社内文化に取り込む
- > ユーザーフレンドリーなプロセスを定義する
- > 適切なシステム構成、更新、および監視を保証する
- > 使用可能なリソースを活用して行動を起こす

サイバーセキュリティを恐れてはいけません。攻撃の失敗例が耳に入らないだけで、ほとんどの攻撃は成功しないことに留意してください。データとネットワークを保護する手段を整えていれば、それはネットワークの健全性を改善して侵害のリスクを軽減していることになります。



お客様のネットワークとそこで稼働するデバイス の健全性は十分ですか？

詳細については、www.axis.com/jp/ja/about-axis/cybersecurityをご覧ください

Axis Communicationsについて

アクシスは、インテリジェントなセキュリティソリューションを通じて、よりスマートで安全な環境の実現を目指しています。ネットワークビデオ市場をけん引するリーダーとして、アクシスはオープンプラットフォームを基盤とした革新的なネットワーク機器を次々と開発し、製品化しています。また、パートナーとのグローバルな連携体制を通じて、お客様に付加価値の高い製品をお届けします。アクシスでは、長年にわたってパートナーと協力関係を築いてきました。アクシスはこうしたパートナーに向け、蓄積された知見と、既存および新規市場における画期的なネットワーク製品を提供しています。

アクシスは全世界50ヶ国以上に2,700人を超える熱意にあふれた従業員を擁し、90,000以上のグローバルパートナーから成る連携体制に支えられています。スウェーデンに本社を置くアクシスは1984年に設立され、NASDAQ Stockholm (ティッカーシンボルAXIS)に株式上場しています。

より詳しい情報はwww.axis.comをご覧ください。