AXIS COMMUNICATIONS

Segurança cibernética

GARANTINDO JUNTOS UMA MELHOR PROTEÇÃO CIBERNÉTICA

AXIS COMMUNICATIONS

ÍNDICE

Atenuando o risco de incidentes cibernéticos

Proteger produtos e serviços de software em rede contra as ameaças cibernéticas é algo fundamental para proteger os dados e os sistemas em sua rede. Um sistema comprometido pode significar a perda da confidencialidade e da integridade dos seus dados ou a indisponibilidade dos dados ou do acesso quando você precisar.

Como parte da nossa responsabilidade enquanto parceiros de segurança cibernética, nós elaboramos algumas diretrizes e análises para ajudá-lo a adquirir — e proteger — produtos de segurança física baseados em IP. Queremos facilitar a implementação de proteções para que você possa usar as ofertas da Axis da maneira mais segura possível.

Para além destas páginas, você também pode aprender mais sobre segurança cibernética e sobre como podemos melhorar a proteção cibernética juntos em www.axis.com/cybersecurity.

Uma responsabilidade compartilhada

A segurança cibernética envolve pessoas, produtos, tecnologias e processos contínuos. E está claro que todos nós precisamos unir forças para garantir que cada elo da cadeia seja o mais forte possível. A segurança cibernética é uma responsabilidade compartilhada, que exige o trabalho conjunto de todas as partes interessadas, incluindo os clientes finais.

Fabricantes de dispositivos

É nesse ponto que a segurança cibernética começa. Os fabricantes devem aplicar as melhores práticas de segurança cibernética aos processos de desenho, desenvolvimento, produção e manutenção de software, para minimizar os riscos de falhas ao longo de todo o ciclo de vida do produto. É importante que eles controlem suas próprias cadeias de suprimentos com cuidado. Os produtos devem ter recursos integrados que permitam a implementação de vários controles de segurança. Devem haver ferramentas para configuração e gerenciamento eficientes dos dispositivos, que apoiem os processos ou políticas de segurança dos clientes. E devem existir canais para informar parceiros e clientes sobre as vulnerabilidades mais recentes detectadas.

Distribuidores

Para os distribuidores, que não entram em contato direto com os produtos que distribuem, a segurança cibernética é relativamente simples. Entretanto, os distribuidores de valor agregado devem considerar os mesmos aspectos que os integradores e instaladores, especialmente aqueles que adquirem equipamentos junto aos fabricantes e aplicam novas etiquetas com suas próprias marcas ou outras marcas. A transparência é muito importante, e a origem do equipamento deve ser clara.

Consultores, integradores e instaladores

Eles podem ajudar os clientes finais a identificar, desenhar e implementar controles de segurança e garantir que os dispositivos de segurança física não sejam um risco para a rede do cliente. Isso pode envolver o desenvolvimento de estratégias relacionadas a senhas, o gerenciamento do acesso remoto e também a manutenção do software e dos dispositivos conectados. Pode incluir a implementação das correções e atualizações mais recentes nos equipamentos instalados e verificações do sistema em busca de vírus. Os desafios do uso de equipamentos OEM/ODM — situação em que as responsabilidades sobre a segurança cibernética muitas vezes não estão claras — também devem fazer parte da discussão geral sobre segurança.

Clientes finais

Como cada organização tem necessidades específicas e únicas de segurança cibernética, não existe uma configuração de segurança universal. Em vez disso, é importante ter um conjunto de políticas de segurança da informação em vigor para definir a abrangência da segurança necessária. Remover contas padrão, definir senhas exclusivas e seguras, que sejam armazenadas com segurança e alteradas regularmente, atribuir permissões diferenciadas e sempre instalar correções e atualizações são apenas algumas das medidas que devem ser tomadas.

Pesquisadores

Geralmente descobrem as vulnerabilidades dos dispositivos. Se a vulnerabilidade não for intencional, o pesquisador normalmente informa o fabricante e dá à empresa a oportunidade de corrigi-la antes de divulgá-la. No entanto, se uma vulnerabilidade crítica tiver um caráter intencional, geralmente os pesquisadores informam o público, para conscientizar os usuários.

O que a segurança cibernética pode aprender com a segurança física

Para a maioria das pessoas, é fácil compreender os riscos à segurança física. Uma porta destrancada aumenta os riscos de que pessoas não autorizadas entrem. Bens valiosos que estejam visíveis podem ser mais facilmente subtraídos. Erros e acidentes podem causar danos a pessoas, propriedades e objetos. Geralmente, a segurança física e a segurança cibernética são abordadas da mesma maneira.

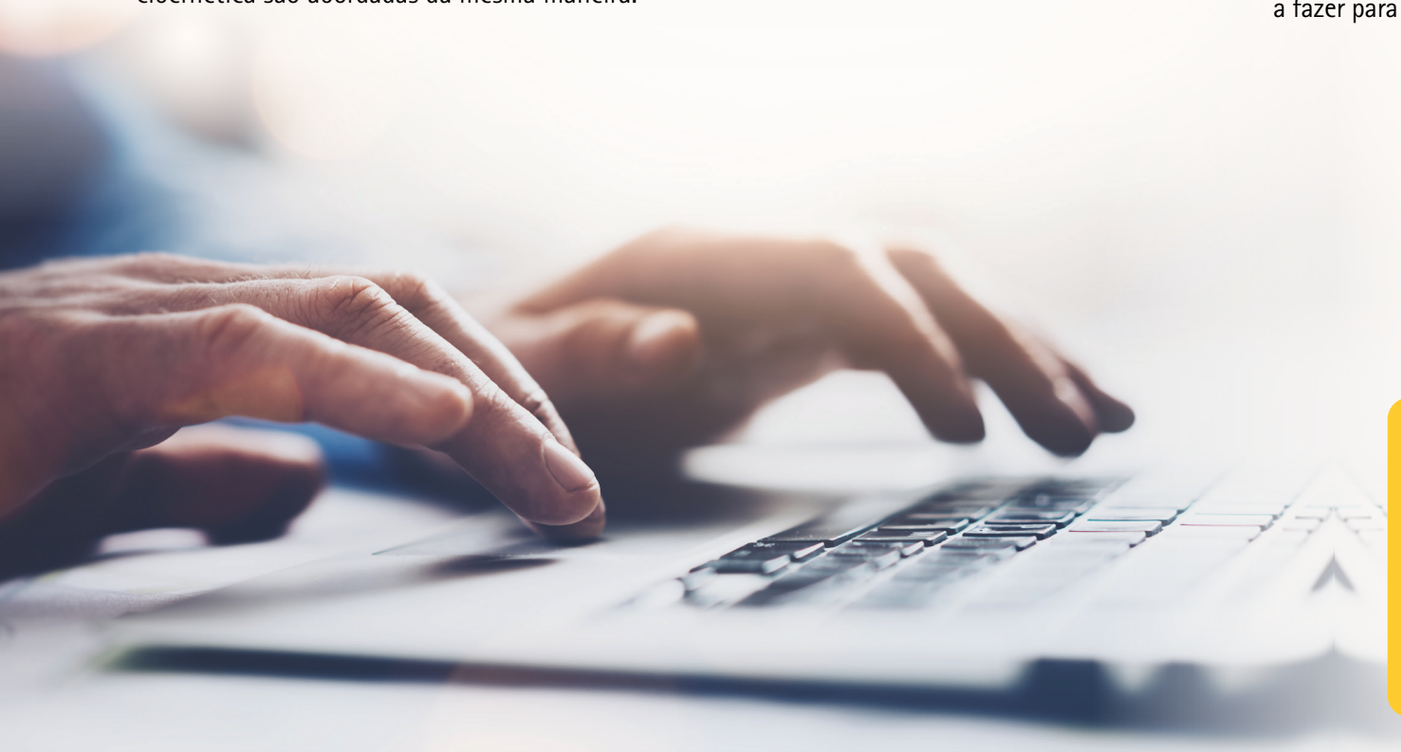
Como o responsável pela segurança física ou pela segurança cibernética da sua organização, você deverá aplicar os mesmos princípios:

> Identificar e classificar ativos e recursos (o que deve ser protegido).

> Identificar as ameaças prováveis (do que e de quem é preciso se proteger).

> Identificar possíveis vulnerabilidades que possam ser exploradas (a probabilidade).

> Identificar o custo esperado se algo ruim acontecer (as consequências). O risco geralmente é definido como a probabilidade de ocorrência de uma ameaça multiplicada pelo dano resultante. Após determinar isso, você deverá se perguntar o que está disposto a fazer para evitar esse impacto negativo.



O que é segurança cibernética?
Segurança cibernética é a proteção de sistemas de computadores e serviços contra ameaças cibernéticas. As práticas de segurança cibernética incluem processos para prevenir danos e restaurar computadores, sistemas e serviços de comunicações eletrônicas, comunicações por cabo e eletrônicas e informações armazenadas para garantir sua confidencialidade, integridade, disponibilidade, segurança, autenticidade e não repúdio.

A quais ameaças você precisa ficar atento?

Os principais elementos que devem ser protegidos em um sistema de TI (tecnologia da informação) ou de TO (tecnologia operacional) são confidencialidade, integridade, disponibilidade e segurança. Qualquer coisa que afete negativamente algum desses elementos é considerado um incidente de segurança cibernética.

Vamos examinar as ameaças mais comuns à segurança cibernética e as vulnerabilidades que elas exploram. As quatro ameaças cibernéticas mais comuns aos sistemas de segurança física baseados em IP são:

1. **Ingenuidade e falha humana não intencional**
2. **Mau uso deliberado do sistema**
3. **Violação física e sabotagem**
4. **Exploração de vulnerabilidades de software**

1 Ingenuidade e falha humana não intencional

Independentemente do nível de excelência da tecnologia que você usa para proteger a sua rede, o elemento humano continuará sendo um fator importante para as violações de segurança.

Os tipos de falha humana que viabilizam os ataques cibernéticos incluem:

> **Engenharia social**
Quando o usuário é induzido por manipulação psicológica a cometer erros que coloquem em risco a segurança ou a fornecer informações confidenciais. Phishing e scareware são exemplos de engenharia social.

> **Uso indevido de senhas**
Incluindo deixar de usar senhas fortes ou deixar de proteger e/ou atualizar as senhas de maneira adequada.

> **Má gestão de componentes críticos**
Perder ou extraviar itens que permitam acessar o sistema. Cartões de acesso, telefones, notebooks e documentos são alguns exemplos.

> **Má gestão do sistema**
Deixar de instalar atualizações do sistema e correções de segurança.

> **Melhorias mal sucedidas**
Usuários que tentam corrigir um problema, mas que acabam reduzindo o desempenho do sistema.

Vulnerabilidades e falha humana
Algumas das vulnerabilidades mais comuns causadas por falha humana têm a ver com a falta de conscientização cibernética e a ausência de políticas e processos para um gerenciamento de riscos de longo prazo. Para minimizar os riscos de falha humana, todos na organização devem ser orientados sobre as melhores práticas de segurança cibernética. Além disso, você deve limitar o acesso aos dispositivos em rede apenas a algumas pessoas de confiança, por meio do sistema de gerenciamento de vídeo (VMS) ou gerenciador de dispositivos.

2 Mau uso deliberado do sistema

Outra ameaça cibernética muito comum é o mau uso deliberado de um sistema por pessoas que tenham acesso a ele de forma legítima.

Os tipos de usos indevidos intencionais incluem:

Manipulação de serviços e recursos do sistema

Roubo de dados

Dano intencional ao sistema

Vulnerabilidades e uso indevido intencional

É importante implementar políticas e processos de longo prazo para ajudar a gerenciar vulnerabilidades e atenuar as ameaças de uso indevido intencional do sistema. Ter um controle adequado sobre quem tem permissão para acessar dados confidenciais também é importante, assim como limitar o número de pessoas com tais permissões.

O software usado para gerenciar dispositivos de segurança física em rede, como câmeras, deve ter uma conta de administrador com credenciais próprias. Essa conta deve ser exclusiva e não deve ser compartilhada. Os operadores das unidades devem, então, ter contas individuais no software de gerenciamento, e ninguém deve ter acesso direto aos dispositivos de segurança física. Se houver alguma razão para permitir o acesso direto, esse acesso deverá ser temporário.

3 Violação física ou sabotagem

Do ponto de vista da segurança cibernética, a proteção física é muito importante:

> Equipamentos fisicamente expostos podem ser violados.

> Equipamentos fisicamente expostos podem ser roubados.

> Cabos fisicamente expostos podem ser desconectados, redirecionados ou cortados.

Vulnerabilidades e ameaças físicas

Algumas vulnerabilidades comuns envolvem os equipamentos em rede, como servidores e switches que não estejam em salas trancadas, câmeras facilmente acessíveis e que não estejam equipadas com caixas de proteção e cabos expostos ou instalados sem o uso de conduítes. Os dispositivos em rede também podem expor outros ativos na mesma rede.

Fique atento aos possíveis impactos negativos

Os sistemas de vídeo, áudio e controle de acesso não processam transações financeiras nem armazenam dados dos clientes. Isso significa que ataques a esses sistemas podem ser difíceis de monetizar e, portanto, seu valor para as organizações de criminosos cibernéticos será limitado. Mas um sistema comprometido pode se tornar uma ameaça para outros sistemas. Por isso pode ser tão complicado estimar os custos de um ataque. Infelizmente, é comum que as organizações aprendam isso da maneira mais difícil. Uma proteção de qualidade requer investimento, e se os fornecedores não levarem em consideração a segurança cibernética ao longo de todo o ciclo de vida do produto, equipamentos mais baratos podem acabar custando muito caro no longo prazo.

4 Exploração de vulnerabilidades de software

No desenvolvimento de software, existem riscos que podem levar a vulnerabilidades de segurança que, por sua vez, podem ser explorados em um ataque. Os riscos mais comuns envolvem bugs ou erros de codificação. Quanto maior o número de vulnerabilidades de software presentes em um produto, maior será o risco de exposição a ataques. Antes de lançar um produto, o ideal é que o fabricante tenha um modelo de desenvolvimento de software que inclua processos e ferramentas que minimizem o risco de vulnerabilidades em todas as etapas de desenvolvimento do software.

Embora lançamentos de software totalmente livres de erros sejam algo raro no setor, bugs e outras implementações incorretas, que representam riscos à segurança, devem ser identificados, corrigidos e comunicados aos clientes pelo fabricante do produto. Portanto, o fabricante precisa ser transparente na comunicação sobre novas vulnerabilidades de software descobertas e oferecer soluções para os clientes de maneira oportuna. Além disso, é importante que o cliente implemente continuamente atualizações de software contendo correções de segurança e correções de bugs à medida que forem disponibilizadas pelo fabricante do produto.

O que os clientes finais devem considerar para atenuar os riscos?

Para começar, do ponto de vista da segurança cibernética, há vários aspectos a serem considerados ao adquirir produtos de segurança física.

Primeiro, examine a abordagem de segurança cibernética de seus fornecedores de segurança física: a empresa tem uma política de governança para a segurança cibernética, que identifique e avalie continuamente os ativos? A empresa conduz avaliações dos riscos relacionados a esses ativos? Também é importante que você entenda como seus fornecedores trabalham com suas respectivas cadeias de suprimentos. Os produtos deles são projetados e fabricados com recursos integrados e suporte à segurança cibernética?

Quais medidas eles tomam para apoiar a segurança cibernética ao longo de todo o ciclo de vida de um produto em rede? E o que acontece se o seu sistema for atacado? Seus fornecedores têm orientações para ajudar você a responder a um incidente de segurança cibernética envolvendo os produtos deles?

Essas são apenas algumas questões que devem ser consideradas. Entraremos em maiores detalhes nas próximas páginas.

O que você deve saber sobre o seu fornecedor de monitoramento? E sobre os fornecedores do seu fornecedor?

As ameaças à segurança estão sempre presentes. Novas ameaças continuarão a surgir e suas características podem mudar a qualquer momento. Muitas vezes, as organizações se concentram apenas na forma como os fornecedores avaliam e combatem esses riscos. Mas e quanto aos fornecedores do fornecedor? Como ele controla e mantém toda sua cadeia de suprimentos e garante que todos os produtos tenham uma jornada segura, do nível do componente até o produto final?

O seu fornecedor prioriza a redução dos riscos à segurança?

- Ele controla toda a cadeia de suprimentos, dos componentes ao produto final?
- Ele tem um modelo de desenvolvimento de software que tenha as considerações de segurança como um componente essencial?
- Ele projeta e fabrica produtos com proteção integrada?
- Ele compartilha conhecimentos e ferramentas para implementar proteções?
- Ele fornece respostas rápidas e atualizações gratuitas caso novas vulnerabilidades de software sejam descobertas?

Parceiros de cadeia de suprimentos

A segurança da cadeia de suprimentos começa com a escolha dos parceiros certos, por meio de avaliações rigorosas, que devem incluir análises de cada processo de gestão de qualidade e sustentabilidade da empresa. Como requisito mínimo, a empresa deve ser certificada por um terceiro, de acordo com a norma ISO 9001 ou IATF 16949.

Avaliando os subfornecedores

O seu fornecedor deve avaliar os processos de seus respectivos subfornecedores com relação ao gerenciamento de riscos e também com relação as instalações e processos de fabricação. Visitas e auditorias de acompanhamento no local devem ser conduzidas, a fim de avaliar se as instalações atendem aos padrões e requisitos estabelecidos para a qualificação dos fornecedores aprovados. Como parte da avaliação de um possível novo parceiro da cadeia de suprimentos, é preciso conduzir uma análise aprofundada da posição financeira e da estrutura de propriedade dos subfornecedores.

Subfornecedores estratégicos

Quando se trata de fornecedores de componentes críticos e parceiros de fabricação, os relacionamentos com essas partes tendem a ser particularmente próximos e de longo prazo. Esses são os subfornecedores estratégicos, com os quais o seu fornecedor desenvolve projetos e produtos, define metas, faz planos e assume compromissos mútuos de longo prazo. Todos os componentes críticos dos produtos do seu fornecedor devem ser adquiridos diretamente junto a subfornecedores estratégicos, e armazenados internamente. Componentes não críticos podem ser adquiridos junto a parceiros de fabricação, mas somente de fornecedores de uma lista de empresas aprovadas.

Qual é o nível de segurança dos processos de fabricação do seu fornecedor?

- Ele define e monitora os processos de fabricação?
- Ele desenvolve e produz equipamentos críticos de fabricação?
- Ele tem implantado um sistema para testar componentes, módulos e produtos durante a fabricação, juntamente com software, computadores para testes e outras infraestruturas de hardware de TI?
- Ele coleta dados de produção 24 horas por dia, 7 dias por semana, para permitir análises em tempo real, avaliações dos riscos potenciais à segurança e implementação de planos de redução de danos?

A melhor maneira para que o seu fornecedor garanta a conformidade dos subfornecedores de acordo com os requisitos especificados é conduzir auditorias regulares no local, anuais ou semestrais. Essas auditorias devem abranger uma série de aspectos importantes, como conformidade de processos, controle de qualidade e registros de rastreabilidade. Também devem incluir revisões do manuseio físico na fábrica, do manuseio do estoque e dos equipamentos de produção.

As análises trimestrais dos negócios são uma boa maneira de acompanhar o desempenho em comparação com as expectativas. Para subfornecedores estratégicos, é recomendável que essas análises sejam conduzidas no nível da alta administração.

Segurança física

Cada unidade na cadeia de suprimentos, do fornecedor dos componentes ao centro de distribuição, deve atender a níveis elevados de exigências de segurança das instalações. Por exemplo, é preciso garantir que as entradas e saídas sejam monitoradas continuamente e que os controles de acesso e registros de visitantes sejam devidamente documentados e armazenados. Além disso, as unidades devem utilizar equipamentos de verificação para detectar a presença de objetos ou materiais indesejados. E o transporte deve ser organizado usando apenas transportadoras reconhecidas e estabelecidas, que sigam os devidos regulamentos e mantenham controles de segurança rigorosos. Também é recomendável que as mercadorias que entram e saem sejam inspecionadas com frequência e registradas por câmeras.

Redes de confiança zero

As redes estão cada vez mais vulneráveis. O crescimento exponencial de dispositivos conectados cria na rede pontos de extremidade que estão sujeitos a ataques. E os ataques cibernéticos estão cada vez mais numerosos e sofisticados. Como resultado, surgiu o conceito de "confiança zero".

Não confie em nada e em ninguém na rede

Como o nome sugere, o posicionamento padrão adotado pela confiança zero é que nenhuma entidade conectada à rede e dentro dela — seja humana ou computadorizada — é confiável. Isso não depende de onde as entidades estão nem da forma como se conectam. A principal filosofia das redes de confiança zero é "nunca confiar, sempre verificar".

Atenha-se ao acesso mínimo necessário

Isso exige que a identidade de qualquer entidade acessando a rede ou dentro dela seja verificada várias vezes e de diferentes maneiras, dependendo do comportamento e da confidencialidade dos dados específicos que estão sendo acessados. Essencialmente, as entidades recebem o nível de acesso mínimo necessário para concluírem suas tarefas.

Redes e arquiteturas de confiança zero

À medida que os clientes compreendem a necessidade de reforçar a segurança cibernética, eles passam a implementar redes e arquiteturas de confiança zero, incluindo HTTPS e o padrão mais sofisticado IEEE 802.1X, que podem permitir automaticamente a entrada de dispositivos autenticados na rede ou bloquear dispositivos não autenticados. É essencial que os fabricantes de dispositivos em rede atendam a tais requisitos, incluindo tecnologias ou interfaces compatíveis com as redes.

O posicionamento padrão adotado pela confiança zero é que nenhuma entidade conectada à rede e dentro dela pode ser confiável.

É aí que entra o mecanismo de política...

No centro de todas as redes de confiança zero, existe um mecanismo de política: um software que permite que uma organização crie, monitore e aplique regras sobre como os dados e os recursos da rede poderão ser acessados. Os mecanismos de política usam uma combinação de analíticos de rede e regras programadas para conceder permissões de acordo com a função e com base em vários fatores.

Aprove ou rejeite todas as solicitações

Em termos simples, o mecanismo de política compara cada solicitação de acesso à rede com a política e informa à pessoa responsável pela aplicação se a solicitação será aprovada ou não. Em uma rede de confiança zero, o mecanismo de política define e aplica a segurança de dados e as políticas de acesso em todos os modelos de hospedagem, locais, usuários e dispositivos.

Definindo e aplicando as regras

Para que um mecanismo de política funcione, as organizações devem definir cuidadosamente as regras e políticas dos principais controles de segurança, como NGFWs (firewalls de próxima geração), gateways de segurança de e-mail e de nuvem e componentes de software de DLP (prevenção contra perda de dados). Juntos, esses controles são combinados para aplicar microssegmentações de rede além dos modelos e locais de hospedagem.

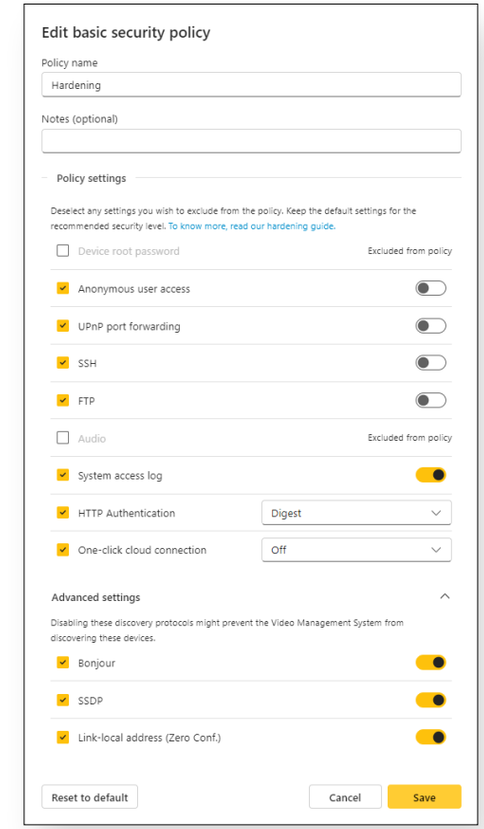
Como os dados e os recursos em rede podem ser acessados?

Os mecanismos de política permitem:

> Criar regras
> Monitorar regras
> Aplicar regras

Mecanismos de política hoje e no futuro

Atualmente, as políticas ainda precisam ser definidas no console de gerenciamento de cada solução individualmente. Mas, cada vez mais, os consoles integrados são capazes de definir e atualizar as políticas em todos os produtos automaticamente. Soluções como o IAM (gerenciamento de identidade e acesso), autenticação multifator, notificações por push, permissões de arquivos, criptografia e coordenação de segurança desempenham um papel importante no desenho de arquiteturas de rede de confiança zero.



Configuração de um mecanismo de política.

Por que é tão importante implementar uma gestão eficaz do ciclo de vida

Acompanhando as ameaças

Um gerenciamento eficaz do ciclo de vida pode ajudar as organizações a manter seus negócios seguros e a se preparar melhor para o futuro. Assim, é preciso saber quais são os riscos e estar sempre atualizado sobre as áreas que podem ser exploradas. Isso é especialmente importante para sistemas de segurança, pois se uma câmera de monitoramento em rede deixa de funcionar, as consequências podem ser graves.

Dispositivos em rede precisam ser atualizados

Todos os dispositivos tecnológicos — de câmeras em rede a VMSs — precisam receber atualizações e correções, para impedir que os invasores explorem vulnerabilidades conhecidas e comprometam as proteções existentes.

Os fabricantes lançam regularmente atualizações e correções de segurança para os componentes de software dos dispositivos, que abordam vulnerabilidades, corrigem bugs e resolvem outros problemas de desempenho, o que ajuda a garantir um sistema mais estável e protegido. No entanto, muitas vezes as organizações deixam de atualizar o firmware ou o sistema operacional executado no hardware.

Isso geralmente ocorre porque elas não têm uma visão geral completa de todos os dispositivos em suas redes. E, mesmo com a visão geral, o processo de atualização de todos os dispositivos pode ser complicado e demorado.

Negligenciar as atualizações de software pode deixar os dispositivos vulneráveis a ataques cibernéticos e pode resultar na perda da operação ou mesmo em multas aplicadas pelos órgãos reguladores, devido à não conformidade.

Como costumamos dizer, a segurança de toda a rede depende da segurança dos dispositivos individuais conectados a ela, por isso, é importante gerenciar com eficácia o ciclo de vida dos ativos físicos na rede.

Um dispositivo, dois ciclos de vida

Existem dois tipos de ciclos de vida associados a dispositivos baseados em software:

1) A vida útil funcional — ou uma estimativa realista quanto ao tempo de operação e funcionamento de um dispositivo. Por exemplo, uma câmera em rede normalmente tem uma vida útil funcional de 10 a 15 anos.

2) O ciclo de vida econômico — ou o tempo até que a manutenção do dispositivo comece a custar mais do que a adoção de uma nova tecnologia. Embora uma câmera IP possa funcionar por até 15 anos, sua vida útil real será mais curta, devido às rápidas mudanças que ocorrem no cenário da segurança cibernética.

Gerencie seus ativos de forma proativa

O gerenciamento do ciclo de vida é a gestão eficaz dos ciclos de vida funcional e econômico dos ativos físicos. As organizações precisam de uma visão geral clara de todos os dispositivos implantados na rede, para garantir que eles estejam protegidos contra ameaças.

A abordagem de segurança cibernética da Axis

A Axis está comprometida em apoiar uma segurança cibernética de alto nível. Nós trabalhamos continuamente para melhorar nossas ofertas e processos de segurança cibernética. Acreditamos na importância de sermos transparentes quanto aos métodos que usamos para proteger nossas operações e nossa cadeia de suprimentos; para tratar o desenvolvimento dos componentes de software, a fim de reduzir os riscos de vulnerabilidades; para gerenciar vulnerabilidades recém-descobertas; e para integrar a segurança aos nossos produtos, apoiando a segurança cibernética ao longo de todo seu ciclo de vida.

As páginas a seguir detalham as medidas que adotamos como nossos pilares de segurança, bem como nossas ações e providências ao longo das diversas fases do ciclo de vida de um produto — da fabricação à implementação, em serviço e na desativação — para atenuar riscos e ajudar você a proteger seus produtos Axis.

Pilares da segurança

Uma abordagem estruturada e sistemática da segurança interna

Na Axis, nós estimulamos uma abordagem colaborativa da segurança, em que todos os funcionários ajudam a promover melhorias contínuas para a segurança interna. Nosso Sistema de gerenciamento de segurança da informação (SGSI) com certificação ISO 27001 é a base da nossa estrutura de segurança cibernética. Como parte do SGSI, nós implementamos controles de segurança cibernética para garantir que apliquemos as melhores práticas ao gerenciar nossa infraestrutura de TI e nossa plataforma de desenvolvimento de software e serviços conectados.

Seguindo uma abordagem estruturada e sistemática, nós protegemos a confidencialidade, a integridade e a disponibilidade de nossos ativos. Além disso, a Axis está em conformidade com diversos requisitos regulatórios, estruturas e padrões estrategicamente selecionados, incluindo o padrão de segurança cibernética ETSI EN 303 645 para o portfólio de dispositivos AXIS OS. Mas nós não nos baseamos apenas em regulamentações e certificações, pois ter várias certificações não significa necessariamente ter uma segurança cibernética melhor.

Saiba mais sobre a conformidade da Axis


RI. SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

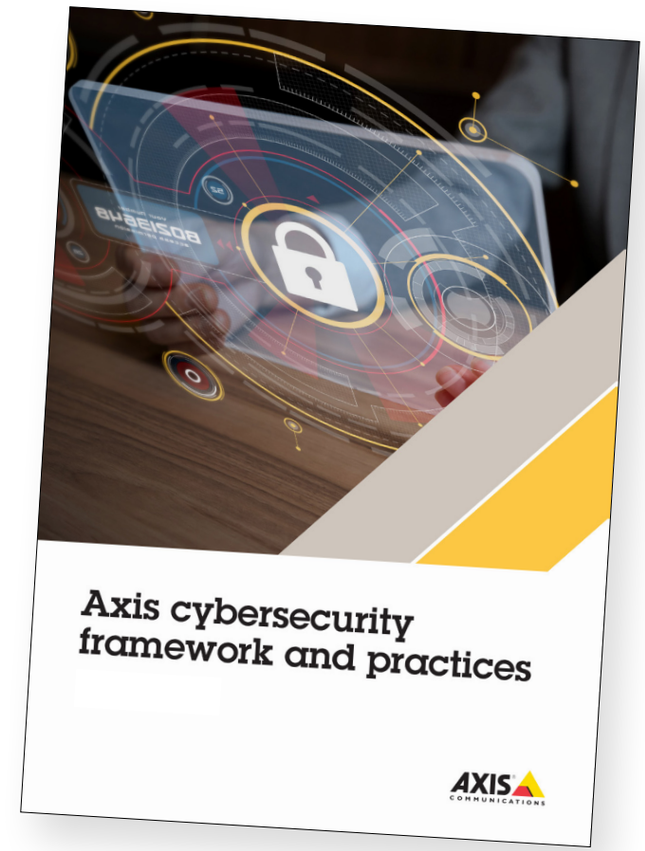
RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
+46 10-516 50 00
certifiering@ri.se | www.ri.se

SP

Certifikat/Certificate 6134 | | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page 1(1)



Protegendo a integridade do produto e reduzindo o risco de vulnerabilidades no software

Passando da segurança interna para a segurança do produto, as medidas a seguir formam as bases da segurança dos componentes de hardware e software da Axis e refletem os princípios que orientam a nossa transparência.

Plataforma de segurança cibernética Axis Edge Vault

Integrada aos dispositivos, essa plataforma baseada em hardware inclui recursos que protegem a integridade dos dispositivos Axis, para que eles possam ser inicializados e integrados com segurança, o que garante que dados confidenciais, como chaves criptográficas, fiquem protegidos contra acesso não autorizado.

Leia mais sobre Axis Edge Vault

Modelo de desenvolvimento de segurança Axis (ASDM)

ASDM é uma metodologia de desenvolvimento aplicada pela Axis para reduzir os riscos de que produtos com vulnerabilidades de software sejam lançados. O modelo garante que a preocupação com a segurança seja parte integrante do desenvolvimento dos componentes de software, abrangendo áreas como avaliações de risco, elaboração de modelos de ameaças, análises de códigos, testes de penetração, programas de recompensas para a identificação de bugs e também verificações e gerenciamento de vulnerabilidades. Detectando e resolvendo problemas rapidamente em todas as fases do desenvolvimento, o ASDM ajuda a reduzir os riscos relacionados à segurança para nossos clientes.

Leia mais sobre ASDM

AXIS OS

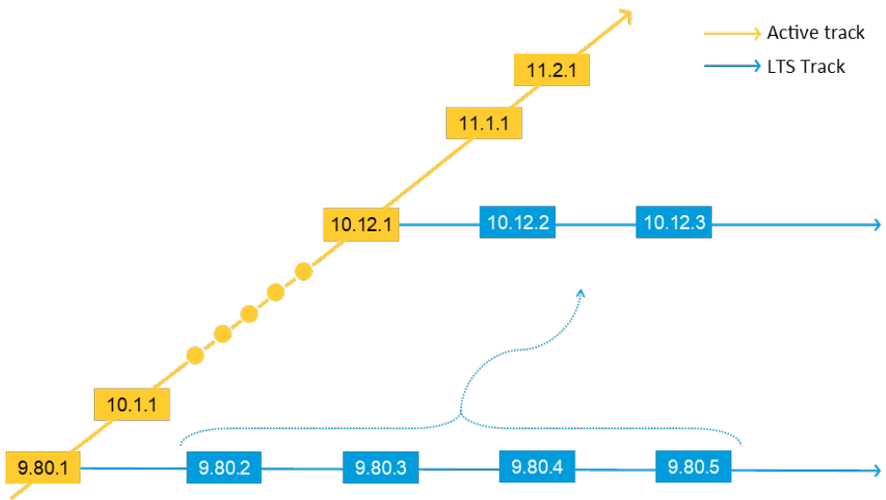
O AXIS OS é o nosso sistema operacional baseado em Linux para dispositivos na borda. Concebido em torno dos conceitos de abertura, transparência e segurança cibernética, esse poderoso sistema operacional apresenta diferentes faixas de sistema operacional para dispositivos Axis, permitindo que a Axis lance rapidamente recursos e correções de segurança de software para um grande número de produtos. Ele foi projetado para ajudar a atenuar riscos e manter seus produtos e serviços Axis atualizados e protegidos. As datas de término do suporte de diversos produtos são apresentadas no site da Axis, o que possibilita o planejamento da desativação e substituição de maneira oportuna.

Leia mais sobre AXIS OS

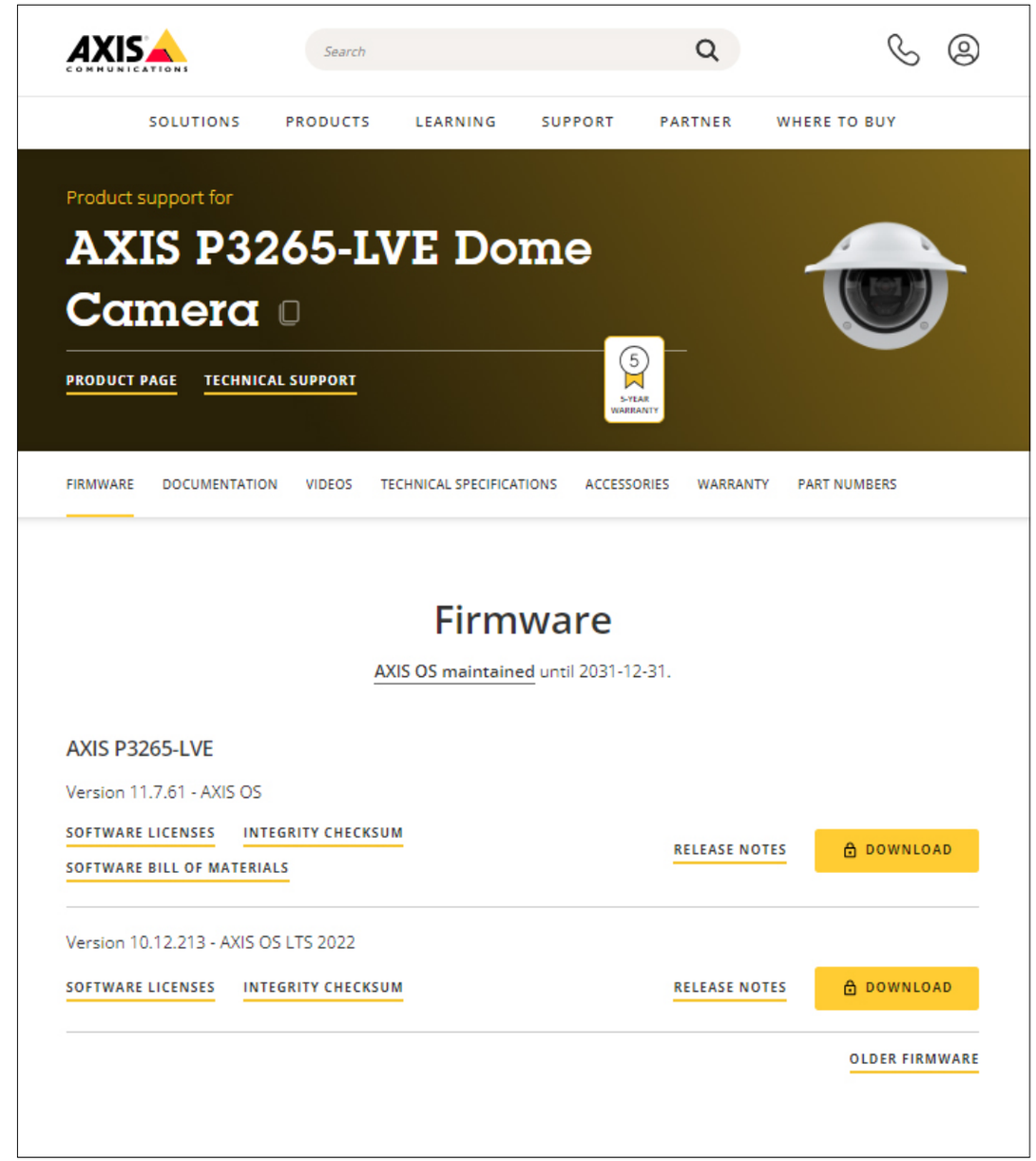
Lista de materiais de software (SBOM)

Além disso, nós publicamos uma lista de materiais de software (SBOM) do AXIS OS, com foco adicional na segurança cibernética e maior transparência para clientes, pesquisadores de segurança e autoridades. A lista SBOM apresenta uma listagem abrangente e detalhada dos componentes usados para desenvolver o sistema operacional dos dispositivos Axis. Ela oferece informações sobre as melhores práticas de segurança cibernética implementadas pelos fornecedores e inclui dados valiosos para outras empresas especializadas em avaliações de vulnerabilidades, análises de ameaças e planos de reparação.

Leia mais sobre a lista de materiais de software



Faixas do AXIS OS.



Gerenciando vulnerabilidades recém-descobertas

Como membro do programa de Autoridade de Numeração de Vulnerabilidades e Exposições Comuns (CVE) (CNA), a Axis publica e notifica as partes interessadas sobre vulnerabilidades, para que nossos clientes possam tomar medidas adequadas e oportunas. Trabalhando com pesquisadores externos, a Axis divulga vulnerabilidades e exposições de uma maneira transparente, responsável e coordenada. A Axis fornece correções para os dispositivos, componentes de software ou serviços afetados e publica todas as informações pertinentes **no site da Axis** e por meio do banco de dados de vulnerabilidades do Programa CVE, que é de acesso público. Além disso, nós fornecemos um serviço de notificação de segurança, no qual você pode se inscrever para receber informações sobre vulnerabilidades e outros assuntos relacionados à segurança. A Axis ressalta a importância de manter o sistema operacional dos produtos instalados atualizado, para garantir que as correções de segurança mais recentes sejam incorporadas.

Leia mais sobre a Política de gerenciamento de vulnerabilidades da Axis

Programa de recompensas para a identificação de bugs

Como parte da nossa estratégia transparente de gerenciamento de vulnerabilidades, nós desenvolvemos um programa de recompensas para a identificação de bugs, conduzido em colaboração com a Bugcrowd, que é líder em segurança cibernética colaborativa. Estamos comprometidos em construir relacionamentos profissionais com pesquisadores de segurança externos e hackers éticos. Como parte do programa, pesquisadores que descobrirem vulnerabilidades em produtos baseados no AXIS OS serão elegíveis para receber uma recompensa em dinheiro. Então, a Axis divulgará de forma transparente as vulnerabilidades encontradas e fornecerá correções para os produtos afetados.

FABRICAÇÃO

DISTRIBUIÇÃO

Reduzindo os riscos de comprometimento de componentes de hardware e software

Segurança da cadeia de suprimentos

Assim como ocorre com qualquer produto, os produtos de segurança física devem funcionar conforme projetados e planejados, mantendo sua integridade. Para isso, o hardware e o sistema operacional do produto devem ser efetivamente protegidos contra alterações ou manipulação não autorizada ao longo de toda a jornada do produto pela cadeia de suprimentos.

Controles de qualidade

Juntamente com nossos fornecedores e parceiros de fabricação, a Axis aplica diversos controles de qualidade, para manter e proteger a integridade dos produtos. Os componentes são sempre obtidos junto a fornecedores que constem da Lista de fornecedores aprovados e de acordo com os materiais especificados pela Axis. O fornecedor não pode alterar as especificações, instruções de trabalho ou documentos de inspeção de qualidade sem a permissão da Axis. Todas as alterações aprovadas devem ser documentadas e registradas.

Rastreabilidade

O processo de movimentação sempre garante o estado dos materiais, revelando eventuais desvios que possam comprometer a qualidade. Os fornecedores e parceiros de fabricação devem manter um sistema que garanta a rastreabilidade dos lotes produzidos, desde o material recebido até o componente finalizado. Durante a fabricação, o componente físico passa por vários testes, que verificam a conformidade e apontam eventuais desvios.

Detecção de componentes falsificados

A AOI (Inspeção óptica automática) contribui para garantir que componentes falsificados não sejam usados. Na Axis, nós desenvolvemos e produzimos nossos equipamentos críticos de fabricação, bem como o sistema para testar os componentes, módulos e produtos nas diversas etapas do processo de fabricação. Esse processo limita os riscos de violações. Como um controle de segurança adicional, todos os dados dos testes são compartilhados com o Axis 24 horas por dia, 7 dias por semana, para que alterações não autorizadas sejam imediatamente identificadas.

Leia mais sobre a segurança da cadeia de suprimentos da Axis

Combatendo ameaças durante a distribuição

Os recursos de segurança cibernética integrados aos dispositivos Axis, juntamente com a opção de redefinição para as configurações padrão de fábrica, protegem contra alterações não autorizadas no software durante o envio. Os recursos suportados pelo Axis Edge Vault (detalhados na próxima página) protegem informações confidenciais e garantem que os dispositivos só executem um sistema operacional Axis original.

É necessário compreender a segurança da cadeia de suprimentos ao fazer a avaliação de riscos dos fornecedores, a fim de determinar se eles implementam medidas que atenuem os riscos à sua organização.

Recursos de segurança cibernética integrados

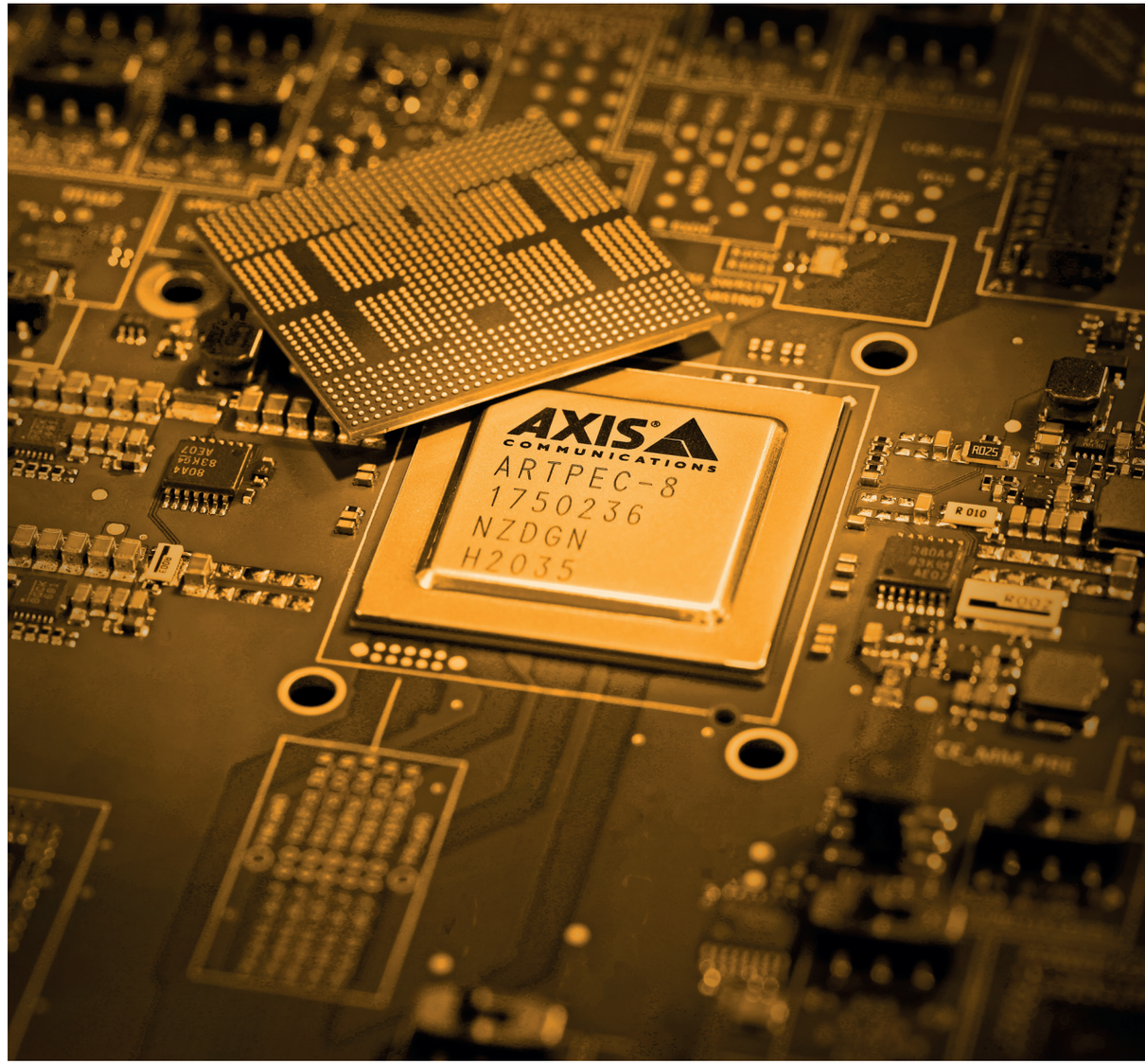
Os dispositivos Axis contam com recursos de segurança que permitem a inicialização e integração seguras, garantindo a proteção de informações confidenciais.

Plataforma de segurança cibernética Axis Edge Vault
Nossa plataforma de segurança cibernética baseada em hardware fornece uma base sólida, que garante a confiabilidade do seu dispositivo Axis enquanto parte integrante da sua rede. O Axis Edge Vault inclui recursos* como:

- **Armazenamento seguro de chaves**, que envolve módulos de computação criptográfica para o armazenamento seguro de chaves criptográficas, protegendo a identidade do dispositivo e outras informações confidenciais contra acesso não autorizado, mesmo se o dispositivo for comprometido. Os módulos de computação criptográfica podem ser um Ambiente de execução confiável integrado ao sistema em um chip (SoC) da Axis. Também podem ser um elemento seguro ou um Módulo de plataforma confiável, que são chips individuais na placa-mãe. Os dispositivos Axis são projetados usando um ou qualquer combinação desses três módulos.
- **Firmware assinado** e **inicialização segura**, que garantem que o dispositivo baixe e execute somente sistemas operacionais Axis originais (AXIS OS).
- **ID do dispositivo Axis**, que é compatível com o padrão IEEE 802.1AR e garante a identificação e a integração seguras dos dispositivos em uma rede.
- **Sistema de arquivos criptografados**, que protege os dados no sistema de arquivos contra extração ou adulteração enquanto o dispositivo não estiver em uso, como durante o transporte entre o local de um integrador de sistemas e o local do cliente final.
- **Vídeo assinado**, que permite que o usuário verifique a autenticidade do vídeo capturado e garante que não houve adulteração.

**Observação: nem todos os modelos de dispositivos são compatíveis com todos os recursos do Axis Edge Vault. Verifique a folha de dados ou o seletor de produtos Axis para confirmar quais recursos são compatíveis com o produto.*

Saiba mais sobre o Axis Edge Vault



Configurações padrão

Além dos recursos de segurança do produto, os dispositivos Axis são fornecidos com configurações de proteção padrão predefinidas.

Credenciais e protocolos de rede

O dispositivo Axis não funcionará até que contas com nome de usuário e senha sejam devidamente configuradas. Após a configuração, o acesso às funções de administrador e/ou às transmissões de vídeo só será concedido mediante o uso dessas credenciais.

Além disso, apenas um número mínimo de protocolos e serviços de rede estão habilitados nos dispositivos Axis por padrão, como HTTP e HTTPS para acessar as interfaces dos dispositivos, RTSP e RTP para transmissões de vídeo e áudio e alguns protocolos, como UPnP e Bonjour, que possibilitam que aplicativos de outros fornecedores detectem os dispositivos Axis.

Atendendo aos requisitos das redes de confiança zero dos clientes

A Axis atendeu aos requisitos de confiança zero produzindo produtos com IDs de dispositivos Axis exclusivos e compatíveis com o protocolo HTTPS e com o padrão IEEE 802.1X, bem como com os padrões IEEE 802.1AR para autenticação de dispositivos e IEEE 802.1AE MACsec para criptografia automática de dados.

O padrão HTTPS está habilitado por padrão, permitindo que as senhas dos dispositivos sejam definidas de maneira segura. Isso também possibilita que um software de gerenciamento de vídeo usando o padrão HTTPS verifique o certificado SSL assinado por uma autoridade de certificação confiável, compatível com o ID do dispositivo Axis dos produtos mais novos.

A compatibilidade com os padrões IEEE 802.1X, IEEE 802.1AR e IEEE 802.1AE, habilitada por padrão nos produtos Axis, viabiliza a integração, autenticação e criptografia de ponta a ponta dos dispositivos de forma automatizada. Isso oferece aos profissionais de TI mecanismos padrão para integrar os dispositivos Axis a uma rede corporativa compatível com IEEE 802.1X, de maneira eficiente e segura. Os clientes que usam dispositivos Axis em uma rede da Aruba podem baixar o guia de integração, que descreve as configurações recomendadas para a integração e gerenciamento seguros dos dispositivos Axis.

Saiba mais sobre as soluções Axis para TI empresarial

IMPLEMENTAÇÃO

Segurança cibernética durante a implementação

Um dispositivo Axis é um endpoint como qualquer outro dispositivo na rede, como notebooks, computadores de mesa ou dispositivos móveis. No entanto, diferentemente de um notebook, os dispositivos Axis não permitem que os usuários visitem sites potencialmente prejudiciais, abram anexos de e-mail maliciosos ou instalem aplicativos não confiáveis. Ainda assim, um produto de vídeo, áudio ou controle de acesso em rede é um dispositivo que tem uma interface que pode expor a riscos o sistema ao qual está conectado.

Os guias para aumento do nível de proteção, disponíveis para os produtos Axis, fornecem recomendações sobre como reduzir a exposição aos riscos cibernéticos. Vamos apresentar algumas recomendações básicas a seguir. Por exemplo, recomendamos redefinir o dispositivo para as configurações padrão de fábrica antes de configurá-lo, para garantir que não haja nenhum software ou configuração indesejada.

Além disso, verifique se o dispositivo está executando o AXIS OS mais recente, que contém as correções de segurança e as correções de bugs mais recentes para o dispositivo específico.

Você deve definir senhas fortes, limitar o acesso direto à interface Web do dispositivo, configurar o dispositivo para usar apenas HTTPS (que criptografa o tráfego de dados entre o cliente e o dispositivo) e desativar serviços e funções não utilizados, para evitar riscos desnecessários. Também é importante definir a data e a hora no dispositivo corretamente, para permitir registros precisos do sistema e garantir que os certificados digitais (dos quais serviços como HTTPS e IEEE 802.1X dependem) possam ser validados e usados.

Uma ferramenta da Axis que permite configurar e gerenciar com eficiência os dispositivos Axis localmente é o AXIS Device Manager. A ferramenta possibilita o processamento em massa de tarefas de instalação e segurança, como gerenciamento de credenciais de dispositivos, implantação de certificados digitais, desativação de serviços não utilizados e atualizações do AXIS OS. Continue lendo na próxima página para obter mais informações sobre software de gerenciamento de dispositivos.

Para obter recomendações completas e abrangentes para aumentar a proteção dos dispositivos baseados no AXIS OS, acesse **o** Guia para aumento do nível de proteção do AXIS OS. Para acessar os guias para aumento do nível de proteção para software de gerenciamento de vídeo e switches de rede da Axis, acesse a Página de recursos de segurança cibernética. E para obter informações sobre como os dispositivos Axis podem ser perfeitamente integrados à infraestrutura e às redes de TI empresariais, consulte as soluções Axis para TI empresarial.

A Axis fornece ferramentas, documentação e treinamento para ajudar a você a reduzir os riscos e manter seus produtos e serviços Axis atualizados e protegidos. **Acesse nossos recursos de segurança cibernética**.

EM SERVIÇO

Segurança cibernética dos dispositivos em serviço

Enquanto um dispositivo está em operação, uma das principais maneiras de manter sua segurança cibernética é garantir que seu firmware ou sistema operacional, o AXIS OS, seja mantido atualizado. Isso garantirá que o dispositivo incorpore as correções de segurança e correções de bugs mais recentes. Os recursos, firmware assinado e inicialização segura dos dispositivos Axis garantem que apenas o AXIS OS original possa ser instalado e operado. As versões do AXIS OS, fornecidas gratuitamente, estão na faixa ativa ou nas faixas de suporte de longo prazo (LTS). As versões do AXIS OS na faixa ativa oferecem suporte a novos recursos, enquanto aquelas nas faixas LTS não oferecem, para minimizar o risco de problemas de compatibilidade. No entanto, ambas as faixas incluem correções de segurança e correções de bugs. Uma maneira de ficar de olho nas vulnerabilidades recém-descobertas é inscrever-se no Axis Security Notification Service. As vulnerabilidades publicadas terão instruções sobre como os produtos afetados deverão ser corrigidos com o novo software do dispositivo.

Para tornar a atualização do sistema operacional de um grande número de dispositivos mais fácil e eficiente, a Axis oferece opções de software de gerenciamento de dispositivos, como o AXIS Device Manager e o AXIS Device Manager Extend.

Como o software de gerenciamento de dispositivos funciona?

Um software de gerenciamento de dispositivos pode criar rapidamente um inventário completo e em tempo real de todas as câmeras, codificadores, dispositivos de controle de acesso e de áudio, entre outros dispositivos conectados. Ele examina toda a rede e, ao encontrar um dispositivo novo ou atualizado, ele reúne todas as informações importantes, incluindo números de modelos, endereços IP e MAC, versões do software dos dispositivos e estado dos certificados.

Uma visão geral completa

Com uma visão geral altamente detalhada de todo o ecossistema da rede, fica mais fácil implementar políticas e práticas de gerenciamento do ciclo de vida consistentes em todos os dispositivos e gerenciar com segurança todas as principais tarefas de instalação, implantação, configuração, segurança e manutenção.

As políticas e práticas recomendadas de segurança cibernética para o gerenciamento de dispositivos precisam abordar aspectos como a força das senhas e a frequência com que os usuários precisam alterar suas senhas; quais serviços não utilizados devem ser desativados para reduzir a área da superfície de possíveis ataques; com que frequência os dispositivos devem ser verificados em busca de vulnerabilidades; e quais procedimentos estão em vigor para avaliar os níveis de risco quando um fabricante publica explorações conhecidas.

Poupe tempo e esforços

O software de gerenciamento de dispositivos ajuda as organizações a poupar tempo e esforços ao gerenciar riscos de segurança cibernética. Ele pode ser usado para:

> Enviar alterações para o sistema, atualizações de software para os dispositivos e novos certificados digitais para todos os dispositivos pertinentes simultaneamente.

> Criar ou reconfigurar facilmente as configurações de segurança e aplicá-las a toda a rede, garantindo que todos os dispositivos estejam em conformidade com as políticas e práticas de segurança mais atuais.

> Verificar se todos os dispositivos estão executando a versão mais recente e segura do software.

> Gerenciar os níveis de privilégios dos usuários na rede e configurar alterações.

Obtenha informações em tempo real

As ferramentas de gerenciamento de dispositivos oferecem às organizações informações em tempo real sobre o estado de seus ecossistemas. Por exemplo, você pode ver quais dispositivos precisam das atualizações de software e certificados mais recentes, bem como obter informações sobre a descontinuação do produto e a data de término do suporte, para poder planejar a substituição dos dispositivos.

Ferramentas de gerenciamento de dispositivos Axis

Nossas opções de software de gerenciamento de dispositivos, o AXIS Device Manager e o AXIS Device Manager Extend, ajudam você a gerenciar com eficiência seus dispositivos Axis. O AXIS Device Manager e o AXIS Device Manager Extend se complementam.

AXIS Device Manager

O AXIS Device Manager ajuda a garantir que a instalação e a configuração dos novos dispositivos sejam conduzidas de forma rápida e fácil. Essa ferramenta local é compatível com todas as principais tarefas de instalação, segurança e operação, incluindo a instalação de atualizações de software e aplicativos. Ela permite configurar os dispositivos Axis com definições de backup e restauração, e você pode visualizar o estado da garantia. Também é possível aplicar controles de segurança cibernética, como certificados HTTPS e IEEE 802.1X.

Leia mais sobre o AXIS Device Manager

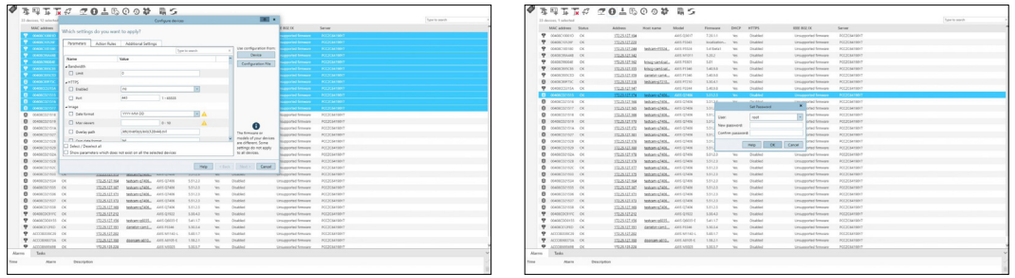
AXIS Device Manager Extend

Ideal para operações com várias unidades, o AXIS Device Manager Extend ajuda a gerenciar seus ativos remotamente, em todas as unidades. Esse aplicativo fácil de usar simplifica o dimensionamento de tarefas cruciais de manutenção, como a atualização do AXIS OS, definição e aplicação de políticas de segurança e gerenciamento de aplicativos. Com um painel ao vivo, ele acelera a solução de problemas, proporcionando o reconhecimento de possíveis problemas no sistema, como dispositivos off-line ou fora da garantia. Além disso, ele oferece recomendações de configuração dos dispositivos, para ajudar a minimizar ameaças de segurança e mitigar vulnerabilidades. As políticas de segurança podem ser definidas e aplicadas a todos os dispositivos Axis simultaneamente.

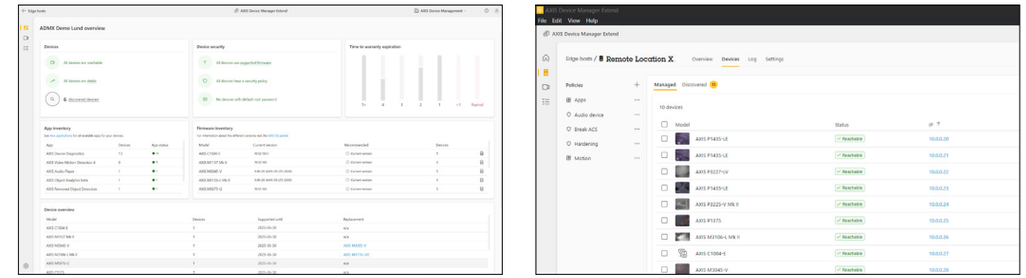
Leia mais sobre o AXIS Device Manager Extend

Em caso de violação da segurança

Se houver uma violação de segurança na sua rede, a Axis fornece o Guia forense do AXIS OS, para ajudar você a conduzir uma análise forense dos seus dispositivos em rede Axis.



Instantâneos da interface do AXIS Device Manager.



Instantâneos da interface do AXIS Device Manager Extend.

DESATIVAÇÃO

Planejando a desativação

Atualizações e correções são a melhor maneira de manter a segurança cibernética de um produto, mas nem sempre elas estão disponíveis quando um produto é mais antigo e já não tem suporte. Do ponto de vista da segurança cibernética, produtos mais antigos e sem correções representam um grande risco. Qualquer dispositivo negligenciado pode facilmente se tornar uma porta de entrada para os invasores.

É importante planejar a desativação dos produtos, para evitar o risco de operar dispositivos que não tenham mais suporte e que apresentem vulnerabilidades potencialmente não corrigidas. A Axis mostra a data de término do suporte do sistema operacional do produto, para que você possa se preparar para desativar e substituir o dispositivo em tempo hábil. Além disso, o AXIS Device Manager Extend permite obter informações sobre garantia, descontinuação e fim de suporte de todos os dispositivos no sistema.

A remoção dos dados em um dispositivo desativado também é importante. Realizando uma redefinição para as configurações padrão de fábrica, é possível apagar rapidamente todas as configurações e dados do dispositivo. Visite o portal do AXIS OS para obter detalhes sobre a desativação de produtos.

Conformidade

As autoridades governamentais estão aprovando cada vez mais leis e regulamentações relacionadas à segurança cibernética, que todas as empresas que operam dentro de suas fronteiras são obrigadas a cumprir. Da mesma forma, setores e organizações exigem cada vez mais conformidade com determinados padrões, incluindo a certificação de produtos e serviços. É responsabilidade de todas as partes interessadas garantir o cumprimento das leis e regulamentos e implementar diretrizes e especificações relevantes a seus respectivos processos empresariais.

Conformidade com a segurança cibernética por padrão

Conformidade com a segurança cibernética significa seguir as normas e requisitos regulatórios definidos pelas autoridades. E, embora não haja dúvidas sobre a importância das normas e certificações, elas são apenas o começo.

Há sempre o risco de que a adesão a normas e certificações se torne uma mera formalidade.

A conformidade com a segurança cibernética está evoluindo continuamente, e o que antes era "desejável", agora está rapidamente se tornando obrigatório.

Por isso, as organizações devem encará-las como um padrão a ser seguido — um requisito mínimo, não uma meta. A verdadeira meta é que os fornecedores ofereçam produtos e serviços que possam ser operados da forma mais segura possível, fornecendo aos clientes orientações e transparência para apoiar a necessidade de manutenção contínua da segurança cibernética.

Regulamentações

As regulamentações de segurança cibernética visam forçar as organizações a proteger seus sistemas e informações e garantir que os produtos e os serviços que oferecem tenham um nível de segurança mínimo. Vamos ver alguns regulamentos importantes e como eles são aplicados.

Em 2023, a Diretiva NIS2 entrou em vigor, e os estados membros da União Europeia têm até outubro de 2024 para transpor as medidas para a legislação nacional. Essa diretiva exigirá que todas as empresas da UE que operam em setores essenciais tenham um alto nível de segurança cibernética comum. As empresas podem ser penalizadas por negligenciar a segurança cibernética, mesmo que isso se deva a uma falha por parte de um de seus fornecedores.

Portanto, de agora em diante, as avaliações dos fornecedores e a segurança da cadeia de suprimentos serão ainda mais importantes. A diretiva vai impor indiretamente obrigações aos fabricantes, importadores e distribuidores, que terão o dever de cuidar de todo o ciclo de vida de seus produtos.

Em dezembro de 2023, a UE chegou a um acordo provisório sobre uma nova regulamentação denominada Lei de Resiliência Cibernética, que define padrões comuns de segurança cibernética para produtos de hardware e software com elementos digitais. Isso inclui produtos conectados direta ou indiretamente a outro dispositivo ou rede, como os dispositivos de IoT. A lei proposta visa reduzir o número de incidentes de segurança cibernética, ao mesmo tempo aumentando a transparência e assegurando uma maior proteção dos dados. O Reino Unido aprovou uma legislação semelhante, denominada Infraestrutura de Segurança de Produtos e Telecomunicações do Reino Unido, que entrará em vigor em abril de 2024.

Organizações que fazem negócios com o governo dos EUA também precisam cumprir normas, como a da Certificação de Modelo de Maturidade em Segurança Cibernética, que exige certificação de auditoria com base no gerenciamento interno dos procedimentos de segurança cibernética.

Garantir a segurança cibernética requer monitoramento e manutenção contínuos.

Normas e certificações

A maioria das normas e certificações concentra-se em recursos, contramedidas e processos para garantir que a segurança seja um elemento integrante. A conformidade pode ser alcançada por meio de testes terceirizados, como testes de penetração e programas de recompensas para a identificação de bugs, a fim de encontrar vulnerabilidades de software.

Embora recorrer à certificação de produtos possa trazer certa tranquilidade para clientes e autoridades governamentais, é preciso observar que as certificações geralmente têm um período de validade de um ano, após o qual o produto requer recertificação. Com novas tecnologias e recursos sendo constantemente desenvolvidos e lançados no mercado, as certificações podem ficar defasadas.

É importante observar também que, mesmo que as normas possam ajudar a melhorar a postura de segurança cibernética, elas não servem como garantia contra incidentes. As organizações precisam analisar continuamente as ameaças e as políticas de segurança.

Por que Axis?

Estímulo da cibersegurança

A segurança cibernética é parte integrante da Axis. Ela orienta nosso sistema interno de segurança da informação, nossa gestão da cadeia de suprimentos, o desenvolvimento de nossos produtos e serviços e nosso tratamento das vulnerabilidades de software. Nós vemos a segurança cibernética como uma responsabilidade compartilhada e permanente, que fundamentalmente envolve transparência. Nosso objetivo é permitir que você use nossas ofertas da maneira mais segura possível. É por isso que nossos produtos são projetados e fabricados com recursos integrados de segurança cibernética e configurações de proteção padrão. Também é por esse motivo que nós fornecemos guias para aumentar o nível de proteção. Monitoramos continuamente as ameaças e buscamos maneiras de melhorar a segurança. Como Autoridade de Numeração CVE, nós respondemos às vulnerabilidades recém-descobertas divulgando as informações e aplicando as correções pertinentes, para que você possa tomar as medidas adequadas e de maneira oportuna. Oferecemos atualizações de software para que você continue a reforçar a segurança dos dispositivos Axis após a instalação. E, com ferramentas como o AXIS Device Manager e o AXIS Device Manager Extend, nós facilitamos o gerenciamento dos seus dispositivos Axis, para reduzir os riscos de segurança cibernética ao longo de todo seu ciclo de vida.

Outras razões para escolher a Axis

> **Qualidade em tudo o que fazemos:** Todos os nossos produtos passam por testes abrangentes para proporcionar tranquilidade aos nossos clientes.

> **Tecnologia inovadora:** Combinamos a tecnologia e a imaginação humana para aprimorar o desempenho e a funcionalidade. Baseada em padrões abertos do setor, nossa tecnologia é flexível, dimensionável e fácil de integrar.

> **Sustentabilidade em todos os níveis:** A Axis tem um compromisso contínuo com o desenvolvimento, associado à responsabilidade ambiental, e usa materiais sustentáveis. Cerca de 90% das câmeras e codificadores Axis lançados em 2022 não contêm PVC.

> **Presença internacional com expertise local:** A Axis tem a maior base instalada de produtos de vídeo em rede do mundo e funcionários em mais de 50 países. Compartilhamos informações e experiências e nos mantemos atualizados sobre os avanços mais recentes.

> **O poder das parcerias:** O compromisso com nossos parceiros fez da Axis a marca de câmeras mais integrada do mercado.

Sobre a Axis Communications

A Axis viabiliza um mundo mais inteligente e seguro, criando soluções que melhoram a segurança e o desempenho empresarial. Como uma empresa de tecnologia em rede e líder do setor, a Axis oferece soluções para sistemas de videomonitoramento, controle de acesso, interfone e áudio. Esses sistemas são aprimorados por meio de aplicativos de análise inteligentes e apoiados por treinamentos de alta qualidade.

A Axis conta com cerca de 4.000 funcionários dedicados, em mais de 50 países, e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para oferecer soluções aos clientes. A Axis foi fundada em 1984 e está sediada em Lund, na Suécia.