SEGURANÇA CIBERNÉTICA

Gerenciamento do ciclo de vida do dispositivo

Os riscos de segurança cibernética estão presentes em todas as etapas do ciclo de vida de um dispositivo em rede, desde a fabricação até a desativação. Se esses riscos forem negligenciados, eles podem levar a falhas operacionais e a perdas em termos de confidencialidade, integridade e disponibilidade dos dados. Portanto, é essencial que todas as partes interessadas, do fornecedor ao cliente final, assumam a responsabilidade de gerenciar esses riscos.

As preocupações relacionadas ao ciclo de vida de segurança dos dispositivos são importantes para o processo de aquisição. Um fabricante deve implementar medidas para reduzir os riscos de segurança cibernética antes mesmo que o produto chegue até o cliente, enquanto o produto estiver em serviço e quando o produto for desativado.

A seguir, apresentamos uma visão geral das tecnologias, ferramentas e orientações, bem como abordagens e processos, que a Axis apoia para atenuar os riscos ao longo de todo o ciclo de vida de um dispositivo Axis.

Os pilares da segurança: Axis Edge Vault, AXIS OS, Modelo de desenvolvimento de segurança Axis

Os pilares da segurança — hardware, software e abordagem

Protegendo a integridade do produto e reduzindo o risco de vulnerabilidades desde o início

Plataforma de segurança cibernética Axis Edge Vault
Essa plataforma baseada em hardware oferece suporte a recursos que protegem a identidade e a integridade do dispositivo contra acessos não autorizados, para que o dispositivo seja inicializado e integrado com segurança e para garantir que dados confidenciais, como chaves, sejam protegidos.

Sistema operacional, AXIS OS
O AXIS OS é executado em uma variedade de dispositivos Axis. Incorporando as melhores práticas de gerenciamento de vulnerabilidades do setor, o AXIS OS fornece a plataforma para lançar recursos e correções de segurança de software de forma rápida e eficiente em um grande número de produtos.

Modelo de desenvolvimento de segurança Axis (ASDM)
É uma metodologia aplicada pela Axis para reduzir os riscos de que produtos com vulnerabilidades de software sejam lançados. O ASDM garante que a preocupação com a segurança seja parte integrante do desenvolvimento dos componentes de software e envolva, entre outras medidas, avaliações de risco, elaborações de modelos de ameaças, análises de códigos, testes de penetração, programas de recompensas para a identificação de bugs e verificações e gerenciamento de vulnerabilidades.

Transparência
Fortalecer a confiança é uma parte importante do trabalho da Axis. A Axis é uma Autoridade de numeração de vulnerabilidades e exposições comuns (CVE). Nós publicamos e notificamos as partes interessadas sobre as vulnerabilidades, para que os clientes possam tomar as medidas adequadas. Além disso, nós publicamos uma lista de materiais de software (SBOM) do AXIS OS.

FABRICAÇÃO E DISTRIBUIÇÃO

Reduzindo os riscos de comprometimento dos componentes

- **Cadeia de suprimentos —** os componentes críticos são adquiridos diretamente junto a fornecedores estratégicos. A Axis trabalha em estreita colaboração com os parceiros de fabricação. Os processos de fabricação são monitorados, e os dados pertinentes são compartilhados ininterruptamente com a Axis, permitindo análises em tempo real e garantindo transparência.
- **Axis Edge Vault —** instalado em um dispositivo Axis durante a fabricação, o Axis Edge Vault inclui os seguintes recursos:
  - **Repositório de chaves seguro,** que envolve módulos de computação criptográfica (como elemento de segurança, Trusted Platform Module, Ambiente de execução confiável) para armazenamento inviolável de chaves.
  - **Firmware assinado,** que garante que o AXIS OS instalado seja original. Ele assegura que qualquer novo firmware baixado e instalado no dispositivo também seja assinado pela Axis.
  - **Inicialização segura,** que permite que o dispositivo verifique se o firmware tem a assinatura da Axis. Se o firmware não for autorizado ou tiver sido alterado, o processo de inicialização é interrompido e o dispositivo para de funcionar. A combinação de firmware assinado, inicialização segura e configuração padrão de fábrica no dispositivo oferece proteção contra modificações maliciosas durante o envio do produto.
  - **ID do dispositivo Axis,** um certificado exclusivo do dispositivo, com chaves correspondentes que podem comprovar a autenticidade do produto Axis. Com base no protocolo IEEE 802.1AR, o ID do dispositivo Axis possibilita a identificação e a integração à rede de forma segura.
  - **Sistema de arquivos criptografados**, que protege as configurações e informações específicas do cliente contra extração ou violação quando elas estão armazenadas no sistema e enquanto o dispositivo não está em uso, como ocorre quando o produto está em trânsito entre um integrador de sistemas e o cliente final, por exemplo.

IMPLEMENTAÇÃO

Abordando os riscos da integração de produtos comprometidos ou inadequadamente protegidos à rede, o que pode resultar em acesso não autorizado, extração de dados confidenciais e transferência de dados alterados entre pontos de extremidade da rede

> **Configurações padrão de fábrica:** execute uma redefinição para as configurações padrão de fábrica no dispositivo antes de configurá-lo. Isso garante que o dispositivo esteja completamente livre de qualquer software ou configuração indesejada, pois o único software remanescente será o AXIS OS — e suas configurações padrão.

> **Verifique o firmware mais recente disponível para o dispositivo:** é possível que tenha se passado algum tempo entre a fabricação e a implementação. Portanto, é uma boa ideia conferir no site da Axis o firmware mais recente disponível, que contará com as últimas correções de bugs para o dispositivo específico.

> **ID do dispositivo Axis:** para garantir que apenas dispositivos Axis originais sejam implementados na rede, o ID do dispositivo Axis pode ser verificado usando autenticação IEEE 802.1X ou ao estabelecer uma conexão de rede segura por meio do protocolo HTTPS. Em uma rede IEEE 802.1X, o ID do dispositivo Axis pode ser utilizado para aumentar a segurança e reduzir o tempo de implementação.

> **Repositório de chaves seguro:** envolvendo módulos de computação criptográfica, o repositório de chaves seguro contém informações confidenciais, como o ID do dispositivo Axis e as chaves carregadas pelo cliente, impedindo acesso não autorizado e extração maliciosa de informações confidenciais, mesmo que o dispositivo seja comprometido.

> **Sistema de arquivos criptografados:** garante que nenhum dado armazenado no sistema de arquivos possa ser extraído ou violado quando o dispositivo não estiver em uso.

> **Guias para aumento do nível de proteção:** o Guia para Aumento do Nível de Proteção do AXIS OS, disponível no portal do AXIS OS, no site da Axis, define uma configuração básica para lidar com ameaças comuns, fornecendo as melhores práticas e orientações técnicas. Além disso, há um guia para aumento do nível de proteção do software de gerenciamento de vídeo AXIS Camera Station e também para os switches de rede Axis.

> **Guia do Verificador de Segurança do AXIS OS:** a Axis recomenda a realização de verificações de segurança dos dispositivos Axis para identificar possíveis vulnerabilidades ou configuração fracas. O Guia do Verificador de Segurança do AXIS OS oferece recomendações sobre como abordar algumas preocupações e descreve os "falsos positivos" mais comuns dos verificadores.

> **AXIS Device Manager:** essa ferramenta fornece configuração e gerenciamento eficientes dos dispositivos Axis localmente. A ferramenta possibilita o processamento em massa de tarefas de instalação e segurança, como gerenciamento de credenciais de dispositivos, implantação de certificados, desativação de serviços não utilizados e atualização do AXIS OS.

EM SERVIÇO

Abordando os riscos de execução de firmware com vulnerabilidades conhecidas, atualização de dispositivos usando firmware não autenticado ou falha nas configurações de segurança

> **Atualização de firmware:** é essencial garantir a segurança cibernética dos dispositivos Axis mantendo o firmware atualizado, usando o rastreamento ativo do AXIS OS ou o rastreamento de suporte de longo prazo (LTS). Fornecidas gratuitamente, as atualizações de firmware usando qualquer um dos tipos de rastreamento incluirão correções de segurança. O firmware assinado garante que somente firmware original da Axis possa ser instalado.

> **AXIS Device Manager Extend:** essa ferramenta, que complementa o AXIS Device Manager, permite o gerenciamento remoto dos dispositivos Axis e simplifica o dimensionamento de tarefas de manutenção, como atualizações de firmware.

> **Gerenciamento de vulnerabilidades:** a Axis fornece um serviço de notificação de segurança no qual você pode se inscrever para obter informações sobre vulnerabilidades e outros assuntos relacionados à segurança.

> **Guia Forense do AXIS OS:** o guia fornece orientações técnicas para a condução de análises forenses de dispositivos Axis em caso de ataque à segurança cibernética da rede e da infraestrutura de TI onde haja um dispositivo Axis instalado.

> **Vídeo assinado:** quando esse recurso é ativado em uma câmera compatível, assinaturas criptográficas são adicionadas ao stream de vídeo antes que ele seja transmitido pelo dispositivo, o que permite verificar se o vídeo foi violado ou não. Isso é particularmente importante em investigações ou processos judiciais.

DESATIVAÇÃO

Abordando o risco de dispositivos que não têm mais suporte e que têm vulnerabilidades conhecidas e não corrigidas, bem como o risco de dados confidenciais remanescentes nos dispositivos após o descarte

> **Data de fim do suporte do firmware:** a página da Web de suporte de muitos dos produtos em Axis.com mostra a data de fim do suporte do firmware do produto específico, permitindo que os clientes planejem a desativação e a substituição oportunas do produto.

> **AXIS Device Manager Extend:** oferece uma maneira fácil de rastrear o status da garantia de todos os dispositivos no sistema, incluindo informações sobre descontinuação e fim do suporte ao produto. Essas informações permitem preparar um dispositivo para desativação e eliminam os riscos associados a um dispositivo sem suporte.

> **Orientação:** o portal do AXIS OS no site da Axis fornece orientações sobre como desativar um dispositivo Axis. Redefinir o dispositivo para as configurações padrão de fábrica apagará todas as configurações e dados.

Para obter mais informações, visite: **www.axis.com/about-axis/cybersecurity**

© 2023 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC e VAPIX são marcas comerciais registradas da Axis AB em várias jurisdições. Todas as outras marcas comerciais pertencem aos respectivos proprietários.