Perguntas e respostas sobre segurança cibernética

Manual do usuário

Perguntas e respostas sobre segurança cibernética

Para obter outras perguntas e respostas, visite o *banco de dados de perguntas* frequentes da Axis.

Perguntas e respostas sobre segurança cibernética

Questões gerais

Questões gerais

O que é segurança cibernética?

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

A segurança cibernética é sobre o gerenciamento de riscos por um período de tempo maior. Os riscos nunca podem ser eliminados, mas somente minimizados.

O que está geralmente envolvido no gerenciamento de segurança cibernética?

A segurança cibernética é sobre produtos, pessoas, tecnologia e processos contínuos.

Portanto, isso envolve **identificar** e avaliar vários aspectos da sua organização, incluindo a realização de um inventário de dispositivos, sistemas, software e firmware; estabelecimento de objetivos críticos, documentação de procedimentos e políticas de segurança, aplicação de uma estratégia de gerenciamento de riscos e desempenho contínuo de avaliações de riscos relacionadas aos seus ativos.

Ele envolverá a implementação de controles de segurança e medidas para **proteger** os dados, os dispositivos, os sistemas e as instalações que você identificou como prioridades contra ataques cibernéticos.

Também envolve desenvolver e implementar atividades que ajudam a **detectar** ataques cibernéticos para que você possa executar ações oportunas. Isso pode, por exemplo, envolver um sistema de SIEM (Security Information and Event Management) ou um sistema de orquestração de segurança, automação e resposta (SOAR) que gerencia dados de dispositivos de rede e software de gerenciamento, agrega dados de comportamento anormal ou ataques cibernéticos potenciais e analisa esses dados para fornecer alertas em tempo real. Os dispositivos Axis são compatíveis com os logs SYS e Remote SYS que são a fonte primária de dados para seu sistema SIEM ou SOAR.

O gerenciamento segurança cibernética também envolve o desenvolvimento e a implementação de procedimentos para **responder** a um incidente segurança cibernética assim que ele é detectado. Você deve considerar regulamentações locais e políticas internas, bem como requisitos para a divulgação de incidentes segurança cibernéticas. A Axis oferece um *AXIS OS Forensic Guide* que ajudará você a entender se um dispositivo AXIS foi comprometido durante um ataque de segurança cibernética.

Desenvolver e implementar atividades para manter planos para resiliência e **recuperar** ou restaurar quaisquer recursos ou serviços prejudicados devido a um incidente segurança cibernética também serão importantes. *O AXIS Device Manager*, por exemplo, facilita a restauração de dispositivos Axis com suporte a pontos de restauração, que são salvos instantâneos da configuração do sistema em um ponto no tempo. Na ausência de um ponto de restauração relevante, a ferramenta pode ajudar a retornar todos os dispositivos para seus Estados padrão e enviar modelos de configuração salvos através da rede.

Quais são os riscos de segurança cibernética?

Riscos de segurança cibernética (como definidos pelo Glossário de Segurança da Internet RFC 4949) são *uma expectativa de perda expressa como a probabilidade de uma ameaça específica explorar uma vulnerabilidade específica com um resultado prejudiciais específico.*

É importante definir políticas e processos de sistemas claros para obter uma redução de risco adequada a longo prazo. Uma abordagem recomendada é trabalhar de acordo com uma estrutura de proteção de TI bem definida, como o ISO 27001, o NIST ou semelhante. Embora esta tarefa possa ser muito complicado para organizações menores, até mesmo o mínimo de políticas e documentação de processos é melhor do que não ter nada.

Para obter informações sobre como avaliar riscos e priorizá-los, consulte *O Guia de Referência da Segurança Cibernética.*

Quais são as ameaças?

Uma ameaça pode ser definida como qualquer coisa que possa comprometer ou causar danos a seus ativos ou recursos. Em geral, as pessoas tendem a associar ameaças cibernéticas a hackers e malwares maliciosos. Na realidade, o impacto negativo muitas vezes

Questões gerais

ocorre devido a acidentes, mau uso intencional ou falha de hardware. Os ataques podem ser categorizados como oportunistas ou direcionados. A maioria dos ataques de hoje são oportunistas: Ataques que ocorrem somente porque há uma janela de oportunidade. Tais ataques usarão vetores de ataque de baixo custo, como phishing e sondagem. Aplicar um nível de proteção padrão reduzirá a maioria dos riscos relacionados a ataques oportunistas.

É mais difícil protegê-los contra invasores que visam um sistema específico com uma meta específica. Os ataques direcionados usam os mesmos vetores de ataque de baixo custo que os invasores oportunistas. No entanto, se os ataques iniciais falharem, eles são mais determinados e estão dispostos a gastar tempo e recursos para usar métodos mais sofisticados para atingir suas metas. Para eles, é amplamente o quanto o valor está em jogo.

Quais são as ameaças mais comuns e como elas podem ser abordadas?

Mau uso deliberado ou acidental de um sistema

Pessoas com acesso legítimo a um sistema são uma das ameaças mais comuns a qualquer sistema. Eles podem acessar serviços aos quais não estão autorizados. Eles podem roubar ou causar danos deliberados para o sistema. As pessoas também podem cometer erros. Ao tentar corrigir as coisas, elas podem reduzir inadvertidamente o desempenho do sistema. As pessoas também são suscetíveis à engenharia social. ou seja, os truques que tornam os usuários legítimos fornecem informações confidenciais. Os indivíduos podem perder ou remover componentes críticos (cartões de acesso, telefones, laptops, documentação, etc.). Os computadores das pessoas podem ser comprometidos e infectar involuntariamente um sistema com malware.

As proteções recomendadas incluem ter uma política de conta de usuário e um processo definidos, ter um esquema de autenticação de acesso suficiente, com ferramentas para gerenciar contas de usuário e privilégios ao longo do tempo, reduzindo a exposição e treinamento de conscientização cibernético.

A Axis ajuda a combater essa ameaça com *guias* de fortalecimento e ferramentas como o *AXIS Device Manager* e *AXIS Device Manager Extend*.

Sabotagem e o violação físicas

Equipamentos expostos fisicamente podem ser violados, roubados, desconectados, redirecionados ou cortados.

As proteções recomendadas incluem a colocação do engrenagem de rede (por exemplo, servidores e switches) em áreas bloqueadas, as câmeras de montagem para que sejam difíceis de alcançar, usando a caixa protegida quando exposta fisicamente e protegendo os cabos em paredes ou canalizações.

A AXIS ajuda a combater essa ameaça com *gabinetes protetores* para dispositivos, parafusos resistentes a violações, câmeras com a capacidade de criptografar cartões SD, detecção de violação de exibição da câmera e detecção para uma caixa aberta.

Exploração de vulnerabilidades de software

Todos os produtos baseados em software possuem vulnerabilidades (conhecidas ou desconhecidas) que podem ser exploradas. A maioria das vulnerabilidades possui baixo risco, mostrando que é muito difícil de explorar ou que o impacto negativo é limitado. Ocasionalmente, talvez haja vulnerabilidades descobertas e exploráveis com impacto negativo significativo. O MITRE hospeda um grande banco de dados de CVE (vulnerabilidades e exposições comuns) para ajudar outras pessoas a reduzirem os riscos.

As proteções recomendadas incluem um processo contínuo de aplicação de patches que ajuda a minimizar o número de vulnerabilidades conhecidas em um sistema, minimizando a exposição da rede para facilitar a investigação e a exploração de vulnerabilidades conhecidas e o trabalho com subdomínios confiáveis que trabalham de acordo com políticas e processos que minimizam as falhas e que fornecem patches e são transparente sobre vulnerabilidades críticas descobertas.

A AXIS lida com a ameaça com o *Axis Security Development Model*, o que visa minimizar vulnerabilidades exploráveis no software Axis, e com a *Política de Gerenciamento de Vulnerabilidades da Axis*, que identifica, corrige e anuncia vulnerabilidades que os clientes precisam conhecer para tomar as medidas apropriadas. (A partir de abril de 2021, *A AXIS é uma Autoridade de Enumeração de Vulnerabilidades e Exposições Comuns* para produtos da Axis, permitindo que adaptem nossos processos ao processo padrão de mercado da MITRE Corporation.) A Axis também oferece *guias de fortalecimento* com recomendações de como reduzir a exposição e adicionar controles para reduzir o risco de exploração. A Axis oferece aos usuários *duas trilhas de software de dispositivo diferentes* para manter o sistema operacional de um dispositivo Axis atualizado:

1. O curso ativo oferece atualizações de software de dispositivo que oferecem suporte a novos recursos e funcionalidades, bem como correções de erros e patches de segurança.

Questões gerais

2. O suporte a longo prazo (LTS) fornece atualizações de software de dispositivo que oferecem suporte a correções de erros e patches de segurança, minimizando os riscos de problemas de incompatibilidade com sistemas de outros fabricantes.

Ataque de cadeia de suprimentos

Um ataque de cadeia de suprimentos é um ataque cibernético que procura danificar uma organização visando elementos menos seguros na cadeia de suprimentos. O ataque é obtido através de comprometimento de software/sistema operacional/produtos e atrai um administrador para instalá-lo no sistema. Um produto pode ser comprometido durante a remessa para o proprietário do sistema.

As proteções recomendadas incluem possuir uma política para instalar software somente de fontes confiáveis e verificadas, verificando a integridade do software ao comparar o checksum de software (Digest) com a soma de verificação do fornecedor antes da instalação, verificando entregas de produtos quanto a sinais de violação.

A AXIS combate tal ameaça de várias formas. A AXIS publica o software com checksum para que os administradores validem a integridade antes de instalá-lo. Quando um novo sistema operacional de dispositivos (OS) é carregado, os dispositivos em rede Axis aceitam apenas o software de dispositivo assinado pela Axis. *Inicialização segura* nos dispositivos de rede Axis também garante que somente o sistema operacional assinado pela Axis execute os dispositivos. E cada dispositivo possui um ID de dispositivo exclusivo da Axis, o que fornece uma forma para o sistema verificar se o dispositivo é um produto Axis genuíno. Os detalhes sobre esses recursos de segurança cibernética estão disponíveis no whitepaper *Axis Edge Vault* (pdf).

Para obter mais detalhes sobre ameaças, consulte o *Guia de referência de segurança cibernética*.

O que são vulnerabilidades?

As vulnerabilidades fornecem oportunidades para que os adversários ataquem ou obtenham acesso a um sistema. Elas podem resultar de falhas, recursos ou erros humanos. Invasores mal intencionados podem parecer explorar qualquer vulnerabilidade conhecida, muitas vezes combinando uma ou mais. A maioria das brechas bem-sucedidas se deve a erros humanos, sistemas configurados insatisfatoriamente e sistemas de manutenção insatisfatórias – muitas vezes devido à falta de políticas adequadas, às responsabilidades indefinidas e à baixa conscientização da organização.

Quais são as vulnerabilidades do software?

Uma API de dispositivo (interface de programação de aplicativos) e serviços de software podem apresentar falhas ou recursos que podem ser explorados em um ataque. No entanto, nenhum fornecedor pode garantir que os produtos sejam isentos de falhas. Se as falhas são conhecidas, os riscos podem ser reduzidos através das medidas de controle de segurança. Por outro lado, se um invasor descobrir uma nova falha desconhecida, o risco aumenta, pois a vítima não teve tempo suficiente para proteger o sistema.

O que é o Sistema de Classificação de Vulnerabilidades Comuns (CVSS)?

O *CVSS (Common Vulnerability Scoring System)* é uma forma de classificar a gravidade de uma vulnerabilidade de software. É uma fórmula que aborda como é fácil explorar e o que pode ser o impacto negativo. A pontuação é um valor entre 0-10, com 10 representando a maior gravidade. Em geral, você encontrará um número de CVSS em relatórios publicados de Vulnerabilidade e Exposição Comuns (CVE).

A AXIS usa o CVSS como um dos indicadores para determinar a criticalidade de uma vulnerabilidade identificada pelo software/produto.

Perguntas e respostas sobre segurança cibernética

Perguntas específicas para a AXIS

Perguntas específicas para a AXIS

Quais treinamentos e guias estão disponíveis para me ajudar a entender mais sobre segurança cibernética e o que é possível fazer para proteger melhor os produtos e serviços de incidentes cibernéticos?

A página da web *Resources* (Recursos) oferece acesso a guias de fortalecimento (por exemplo, *Guia de Fortalecimento do AXIS OS*, *Guia de Fortalecimento do Sistema do AXIS Camera Station* e *Guia de Fortalecimento de Switches de Rede Axis*), documentos de políticas e muito mais. A Axis também oferece um curso de *aprendizado eletrônico* sobre segurança cibernética.

Onde posso encontrar o sistema operacional mais recente para meu dispositivo?

Vá para *device software* (software de dispositivo) e procure seu produto.

Como posso atualizar facilmente o sistema operacional em meu dispositivo?

Para atualizar seu software de dispositivo, é possível usar o software de gerenciamento de vídeo da Axis, como *AXIS Companion* ou *AXIS Camera Station*, ou ferramentas como o *Axis Device Manager* e *AXIS Device Manager Extend*.

Se houver interrupções nos serviços da Axis, como posso ser informado?

Visite *status.axis.com*.

Como posso ser notificado sobre uma vulnerabilidade descoberta?

Você pode assinar o *Axis Security Notification Service* (Serviço de Notificação de Segurança da Axis).

Como a AXIS gerencia vulnerabilidades?

Consulte a *Política de Gerenciamento de Vulnerabilidades da Axis*.

«»Como a AXIS minimiza as vulnerabilidades de software?

Read the article *Making cybersecurity integral to Axis software development*.

Como a Axis oferece suporte à segurança cibernética ao longo de um ciclo de vida de dispositivos?

Visite *A lifecycle approach to cybersecurity* (Uma abordagem de ciclo de vida da segurança cibernética).

Quais são os recursos de segurança cibernética integrados aos produtos AXIS?

Leia mais:

- *Axis Edge Vault*
- *AXIS OS*
- *Suporte à segurança cibernética ao longo do ciclo de vida do dispositivo*

Perguntas e respostas sobre segurança cibernética

Perguntas específicas para a AXIS

A AXIS possui certificação ISO, e com quais outras regulamentações a Axis se mantém em conformidade?

Visite a página de *Compliance* (Conformidade).

Como a Axis ajuda minha empresa a atender ao NIS 2?

Consulte o artigo no *NIS 2* (pdf).

Manual do usuário
Perguntas e respostas sobre segurança cibernética

Ver. M4.2
Data: Julho 2024
Nº da peça T10189380