Cybersecurity reference guide

Manual do usuário

Cybersecurity reference guide

Sumário

Cybersecurity reference guide

Introdução

Introdução

O objetivo deste guia é fornecer uma linha de base comum e servir como referência para materiais relacionados à segurança cibernética produzidos pela Axis. Esses são descrições, modelos e estruturas simplificadas baseadas em conferências NIST, SANS, ISO e RSA, bem como materiais de várias organizações da comunidade de segurança cibernética.

Links para outros materiais da Axis:

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

Definição de segurança cibernética

Baseado em parte na definição do NIST:

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.

Tipos de organizações

Organizações diferentes possuem ativos, recursos, exposição e maturidade cibernética diferentes. Ao seguir a prática recomendada, *os controles CIS (anteriormente conhecido como Controles de Segurança Crítica)* definem três perfis organizacionais.

- **Grupo de Implementação de SANS 1 (IG1)**

  Na maioria dos casos, uma empresa IG1 é geralmente pequena a média, com experiência limitada em TI e segurança cibernética para se dedicar à proteção de ativos de TI e pessoal.

- **Grupo de Implementação de SANS 2 (IG2)**

  Uma empresa IG2 emprega indivíduos responsáveis por gerenciar e proteger infraestruturas de TI. Geralmente, essas empresas oferecem suporte a vários departamentos com perfis de risco diferentes baseados na função e na missão no trabalho. Unidades de pequenas empresas podem ter cargas de conformidade regulatórias.

- **Grupo de Implementação de SANS 3 (IG3)**

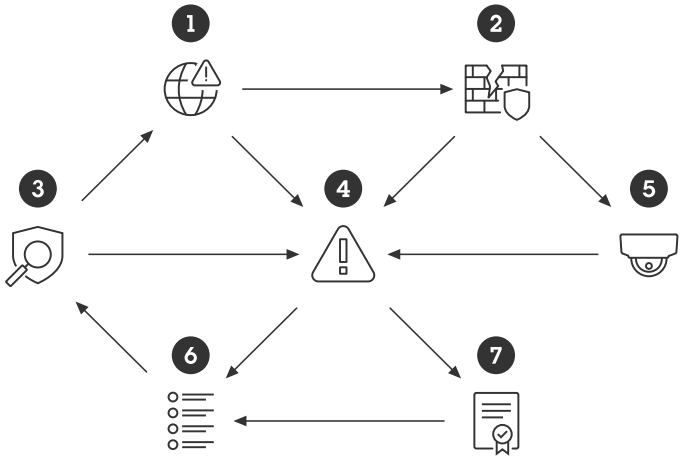
  Uma empresa IG3 normalmente emprega especialistas em segurança especializados em diferentes facetas da segurança cibernética (por exemplo, gerenciamento de riscos, testes de penetração, segurança de aplicativos). Ativos e dados IG3 contêm informações ou funções sensíveis sujeitas a supervisão regulatória e de conformidade.

Terminologia

Terminologia

Terminologia

O mapa da terminologia mostra as relações dos termos-chave de segurança cibernética específicos que são discutidos neste documento.



- **(1) Ameaças** exploram **(2) vulnerabilidades** expondo **(5) ativos** e aumentando **(4) riscos**
- **(4) Riscos** influenciam **(7) políticas** e indicam **(6) requisitos**
- **(6) Requisitos** são abordados em **(3) controles de segurança**, que enfrentam constantemente **(1) ameaças** enquanto mitigam **(4) riscos**

Risco

Segurança cibernética tem tudo a ver com o gerenciamento de riscos ao longo do tempo. Os riscos nunca podem ser eliminados, mas somente minimizados. Às vezes, as pessoas confundem os termos: risco, ativo, ameaça, vulnerabilidade ou impacto negativo

O Glossário de Segurança da Internet (RFC 4949) define o risco como uma expectativa de perda expressa como a probabilidade de uma ameaça específica explorar uma vulnerabilidade específica com um resultado prejudicial específico.

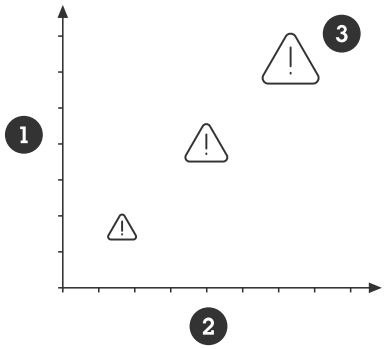
Uma versão resumida comumente usada é **Risco = Probabilidade x Impacto**

Essa fórmula é usada para priorizar riscos. A definição da RFC inclui o termo "particular" para ameaça, vulnerabilidade e resultados prejudiciais. Cada ameaça deve ser encarada individualmente, começando pela que é mais plausível e tem o maior impacto negativo.

Um desafio ao discutir risco é o fator de probabilidade. As coisas podem ou não acontecer. A probabilidade de um adversário explorar uma vulnerabilidade é muitas vezes determinada pela facilidade com que a vulnerabilidade é explorada (exposição) e pelo benefício potencial para o adversário explorá-la.

É possível traçar riscos com estas duas dimensões: Use a probabilidade de que um risco ocorra em um eixo e o impacto do risco, se ocorrer, no outro. Isso proporciona uma visão clara do impacto potencial e da prioridade que você precisa associar a cada risco.

Terminologia



1 ***Probabilidade*** *da menor para a maior*
2 ***Impacto negativo*** *do menor para o maior*
3 ***Níveis de risco*** *dos menores para os maiores*

Valor do ataque = Benefícios do ataque - Custo do ataque

Adicionar proteção aumentará o custo do ataque e, consequentemente, reduzirá a probabilidade. O custo do ataque está relacionado ao tempo, recursos, habilidades e sofisticação necessários para que o ataque seja bem-sucedido. O risco de ser pego ou outras consequências negativas também fazem parte do custo do ataque.

A avaliação de risco, que é o processo de análise de riscos no espaço cibernético, é a mesma da proteção física. As perguntas a serem consideradas são as seguintes:

1. O que você deseja proteger?
2. De quem você deseja proteger?
3. Qual é a probabilidade de um impacto negativo?
4. O quão ruins serão as consequências se você falhar?
5. Que estratégias você deve implementar para mitigar os riscos?

Implementar qualquer tipo de medida de proteção ou controle de segurança resulta em algum tipo de custo. Todas as organizações têm recursos fiscais limitados. Se você não sabe quais são os riscos, é difícil estimar o orçamento para sua proteção. Você sempre precisará aceitar riscos, mas essa decisão precisa ser uma decisão deliberada baseada em risco.

Estimar o potencial impacto negativo em cada tipo de ativo é difícil e complexo. Em muitos casos, as estimativas são subjetivas, e a análise de impactos é muitas vezes subestimada. Usar o modelo de impacto ISO 27000 e os tipos de designações — por exemplo, Limitado, Grave, Muito grave ou Catastrófico — pode ajudar a obter uma visão geral rápida para melhorar a priorização. Ele fornece uma maneira simples de estabelecer um valor mais exigente baseando-se na estimativa da quantidade de tempo que levaria para se recuperar de um impacto negativo, ou seja:

- **Limitado** = de horas a dias
- **Grave** = de dias a semanas
- **Muito grave** = de semanas a meses
- **Catastrófico** = de meses a anos, se de todo

Ativos

Embora a proteção física seja focada na proteção de pessoas e objetos físicos, a proteção de segurança cibernética é focada na proteção de ativos de dados e recursos de computador. Há três áreas principais:

- **Confidencialidade** : divulgação de informações ou recursos

- **Integridade**: destruição ou alteração de informações ou recurso
- **Disponibilidade**: acessibilidade a informações e recursos

Essas áreas também são conhecidas como tríade da CIA. A tecnologia de operação (OT) frequentemente prioriza usabilidade, enquanto que aqueles que trabalham com tecnologia da informação (TI) frequentemente priorizam a segurança. Encontrar o equilíbrio certo entre confidencialidade, integridade e disponibilidade é muitas vezes um desafio.

Ativos e recursos precisam ser classificados para determinar os níveis de proteção adequados. Nem todos os ativos de dados e recursos de computador são iguais em termos de impacto negativo. Elas são frequentemente classificadas da seguinte forma:

- **Publico**: o ativo está visando um consumidor público. Ou o impacto negativo será limitado se divulgado ao público.
- **Privado**: o ativo é privilegiado para um grupo específico/selecionado. Em geral, o impacto negativo se limita a uma organização específica, como uma empresa ou família.
- **Restrito**: o ativo é privilegiado para indivíduos selecionados dentro de uma organização.

O vídeo ao vivo em um sistema de vídeo poderia ser classificado como público, o que se refere tanto ao público em geral quanto ao público dentro de uma organização. Mas, na maioria dos casos, o vídeo ao vivo é classificado como privado, o que significa que ele só é acessível para uma unidade organizacional específica. Enquanto isso, o vídeo gravado, na maioria dos casos, é classificado como restrito, pois pode haver cenas que poderiam ser muito sensíveis. Credenciais e configurações também são dados que devem ser classificados como restritos.

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 ocorre devido a acidentes, mau uso intencional ou falha de hardware.

Os ataques não surgem do nada. Há sempre alguma motivação para comprometer um sistema e seus ativos. Os ataques podem ser categorizados como oportunistas ou direcionados. Na segurança cibernética, os agressores também são conhecidos como adversários que podem ter más intenções.

A maioria dos ataques de hoje são oportunistas: Ataques que ocorrem somente porque há uma janela de oportunidade. Em muitos casos, um agressor externo oportunista nem sabe quem é a vítima. Esses agressores usarão vetores de ataque de baixo custo, como phishing e sondagem. Nesses casos, eles não têm a determinação de gastar tempo e recursos em um ataque fracassado; eles rapidamente avançam para sua próxima tentativa. Aplicar um nível de proteção padrão reduzirá a maioria dos riscos relacionados a ataques oportunistas. É mais difícil oferecer proteção contra ataques direcionados – aqueles 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.

Adversários comuns (atores de ameaça)

- **Próximos e queridos**: pessoas que podem querer espionar sua vida pessoal
- **Funcionários**: ou pessoas que têm acesso legítimo ao sistema, seja por acidente ou uso indevido intencional
- **Pregadores de peças**: pessoas que acham que interferir com sistemas de computador é um desafio agradável
- **Hacktivistas**: pessoas que desejam atacar organizações por motivos políticos ou ideológicos
- **Criminosos cibernéticos** : pessoas interessadas em ganhar dinheiro por meio de fraudes ou da venda de informações valiosas
- **Concorrentes industriais**: entidades interessadas em obter uma vantagem econômica para suas empresas ou organizações
- **Terroristas cibernéticos** : pessoas ou entidades que realizam um ataque desenvolvido para causar alarme ou pânico, muitas vezes por razões ideológicas ou políticas
- **Estados-nação**: agentes de serviços de inteligência estrangeiros agindo para obter quilometragem econômica e política ou para infligir danos a sistemas de informação críticos

- **Indivíduos**: uma pessoa ou grupo específico agindo por conta própria, onde a motivação pode ser diferente daquelas listadas acima. Essa pessoa pode ser um jornalista investigativo, hacker do bem ou semelhante. Hackers do bem (também conhecidos como hackers éticos) podem representar uma ameaça se você priorizar esconder as falhas em vez de corrigi-las.

Vulnerabilidade

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

Vulnerabilidades de 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 de compensação. Por outro lado, se um invasor descobrir uma nova falha desconhecida, o risco de explorações dia zero bem-sucedidas aumenta, pois a vítima não teve tempo suficiente para proteger o sistema.

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 Vulnerabilidades e Exposições Comuns (CVE).

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

Política

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.

Controles de segurança

Controles de segurança são salvaguardas ou contramedidas empregadas para evitar, detectar, combater ou minimizar riscos à segurança de instalações físicas, informações, sistemas de computador ou outros ativos. Os processos de implantação de controles de segurança são frequentemente chamados de fortalecimento.

Compensar os controles de segurança são proteções alternativas que podem ser usadas quando não é possível aplicar o controle de segurança preferido ou quando o controle preferido pode não estar disponível ou ser muito caro.

Os controles de segurança precisam ser continuamente monitorados e atualizados como ameaças, valores, vulnerabilidades e mudanças de exposição ao longo do tempo. Isso requer definir e seguir políticas e processos.

O SANS Institute publicou uma *lista de controles CIS*, que é um conjunto recomendado de melhores práticas prioritárias de defesa cibernética. Para mostrar a diversidade dos controles de segurança, aqui está a lista na íntegra.

- Controle CIS 1: Inventário e controle de ativos corporativos
- Controle CIS 2: Inventário e controle de ativos de software
- Controle CIS 3: Proteção de dados
- Controle CIS 4: Configuração segura de ativos corporativos e software
- Controle CIS 5: Gerenciamento de contas
- Controle CIS 6: Gerenciamento de controle de acesso

Terminologia

- Controle CIS 7: Gerenciamento contínuo de vulnerabilidades
- Controle CIS 8: Gerenciamento de logs de auditoria
- Controle CIS 9: Proteções de email e navegador da Web
- Controle CIS 10: Defesas contra malware
- Controle CIS 11: Recuperação de dados
- Controle CIS 12: Gerenciamento da infraestrutura de rede
- Controle CIS 13: Monitoramento e defesa da rede
- Controle CIS 14: Treinamento em conscientização e habilidades de segurança
- Controle CIS 15: Gerenciamento de provedores de serviços
- Controle CIS 16: Segurança de software aplicativo
- Controle CIS 17: Gerenciamento de resposta a incidentes
- Controle CIS 18: Teste de penetração

O *Guia de Fortalecimento do AXIS OS* é baseado em CIS.

Medidas de proteção para ameaças comuns

Ao entender e combater as ameaças comuns, você pode mitigar a maioria dos riscos.

Mau uso deliberado ou acidental de um sistema

O equilíbrio entre usabilidade e segurança de um sistema é difícil. Muitos sistemas são endurecidos do ponto de vista da conveniência, não da segurança. Isso oferece oportunidades de uso indevido intencional ou acidental. Pessoas com acesso legítimo a um sistema são a ameaça mais comum a qualquer sistema.

Exemplos de ameaças comuns:

- Indivíduos podem acessar serviços (por exemplo, vídeo ao vivo ou gravado) aos quais não estão autorizados
- Indivíduos cometem erros
- Indivíduos podem tentar corrigir coisas que resultam em redução no desempenho do sistema
- Indivíduos descontentes podem roubar ou causar danos deliberados ao sistema
- Indivíduos são suscetíveis à engenharia social
- Indivíduos roubam
- Os indivíduos podem perder ou mover componentes críticos (cartões de acesso, telefones, laptops, documentação, etc.)
- Os computadores dos indivíduos podem ser comprometidos e infectar involuntariamente um sistema com malware

As medidas de proteção recomendadas mais comuns são:

- Política e processo de conta de usuário definidos
- Esquema de autenticação de acesso suficiente
- Ferramentas para gerenciar contas de usuário e privilégios ao longo do tempo
- Redução da exposição
- Treinamento em consciência cibernética

Como a Axis ajuda a combater essa ameaça:

- O *Guia de Fortalecimento do AXIS OS* descreve controles de segurança comuns para ameaças comuns a um dispositivo
- O *Guia de Fortalecimento do AXIS Camera Station* descreve controles de segurança comuns para sistemas de vídeo
- O *AXIS Device Manager* e o *AXIS Device Manager Extend* ajudam a gerenciar controles de segurança comuns

Sabotagem e o violação físicas

A proteção física para sistemas de TI é muito importante do ponto de vista da segurança cibernética.

Exemplos de ameaças comuns:

- Equipamentos fisicamente expostos podem ser adulterados
- Equipamentos fisicamente expostos podem ser roubados
- Cabos fisicamente expostos podem ser desconectados, redirecionados ou cortados

Medidas de proteção recomendadas comuns:

- Coloque os equipamentos de rede (por exemplo, servidores e switches) em áreas bloqueadas
- Monte as câmeras de um modo que seja difícil de acessá-las fisicamente
- Use uma caixa protetora quando exposta fisicamente
- Proteja os cabos em paredes ou conduítes

Como a Axis ajuda a combater essa ameaça:

- Cartão SD criptografado para impedir a reprodução de vídeo se um usuário não autorizado for capaz de ejetar o cartão SD
- Detecção de violação da visão da câmera
- Detecção de abertura da caixa

Exploração de vulnerabilidades de software conhecidas

Todos os produtos baseados em software possuem vulnerabilidades que podem ser exploradas. Elas podem ser categorizadas como conhecidas e desconhecidas. Eventualmente, todas as vulnerabilidades desconhecidas serão conhecidas; é só uma questão de tempo. A maioria das vulnerabilidades possui baixo risco, o que significa que são muito difíceis de explorar ou que o impacto negativo é limitado. Ocasionalmente, é possível que vulnerabilidades exploráveis capazes de causar impacto negativo substancial podem ser descobertas. O MITRE hospeda um grande banco de dados de CVE (vulnerabilidades e exposições comuns) para ajudar as pessoas a reduzirem os riscos.

Medidas de proteção recomendadas comuns:

- Um processo de patching contínuo ajuda a minimizar o número de vulnerabilidades conhecidas em um sistema.
- Minimize a exposição da rede para dificultar sondar e explorar vulnerabilidades conhecidas.
- Trabalhe com subfornecedores confiáveis que funcionam de acordo com políticas e processos que minimizam falhas, adotam processos para fornecer patches e fazer divulgações quando vulnerabilidades críticas são descobertas.

Como a Axis ajuda :

- O *Modelo de Desenvolvimento de Segurança da Axis* é uma estrutura que define os processos e ferramentas usados pela Axis para reduzir o risco de lançar produtos com vulnerabilidades de software.
- A *política de gerenciamento de vulnerabilidades da Axis* envolve identificar, corrigir e divulgar vulnerabilidades às quais os clientes precisam estar atentos para tomar as ações apropriadas. Desde abril de 2021, a AXIS é uma autoridade de enumeração (CNA) de vulnerabilidades e exposições comuns (CVE) para produtos da Axis, o que nos permite adaptar nossos processos ao processo padrão de mercado da MITRE Corporation. Isso, por sua vez, nos ajuda a prestar um suporte melhor aos nossos clientes.
- Os *guias de fortalecimento da Axis*, como o *Guia de Fortalecimento do AXIS OS*, fornecem recomendações sobre como reduzir a exposição e adicionar controles de compensação para reduzir o risco de exploração de falhas de software.
- As versões de firmware LTS (suporte de longo prazo) permitem que os clientes apliquem patches no sistema operacional dos dispositivos Axis, minimizando os riscos de problemas de incompatibilidade com sistemas de gerenciamento de vídeo de terceiros.

Ataque de cadeia de suprimentos

Um ataque de cadeia de suprimentos é um ataque cibernético que procura danificar uma organização direcionando elementos menos seguros na cadeia de suprimentos. Ele é usado principalmente quando outros vetores de ataque (por exemplo, engenharia social, ataques de firewall e interface) falham devido aos altos níveis de proteção do sistema. O ataque é obtido com o comprometimento de software/firmware/produtos e atraindo-se um administrador para instalá-lo no sistema. Um produto pode ser comprometido durante a remessa para o proprietário do sistema. Conseguir um ataque na cadeia de suprimentos com êxito requer habilidades, tempo e recursos.

As medidas de proteção recomendadas mais comuns são:

Medidas de proteção para ameaças comuns

- Adote uma política para instalar software somente de fontes confiáveis e verificadas.
- Verifique a integridade do software comparando a soma de verificação de software (digest) com a soma de verificação do fornecedor antes da instalação.
- Na entrega, verifique a embalagem ou o produto em busca de sinais de violação.

Como a Axis ajuda a combater essa ameaça:

- O software Axis é publicado com uma soma de verificação, permitindo que os administradores validem a integridade do software antes de instalá-la.
- O firmware assinado em um dispositivo Axis garante que o AXIS OS instalado seja verdadeiramente da Axis e garante que qualquer novo firmware baixado e instalado no dispositivo também seja assinado pela Axis.
- A inicialização segura em um dispositivo Axis permite que o dispositivo verifique se o firmware possui uma assinatura Axis. Se o firmware não for autorizado ou for alterado, o processo de inicialização será cancelado.
- O ID de dispositivo Axis compatível com IEEE 802.1AR é um certificado de fornecedor exclusivo da Axis que fornece uma forma do sistema verificar se o hardware dentro do gabinete é fornecido pela Axis.
- A criptografia do cartão SD e criptografia do sistema de arquivos impedem a extração de dados armazenados quando o cartão ou dispositivo é roubado.

Manual do usuário
Cybersecurity reference guide

Ver. M3.2
Data: Novembro 2023
Nº da peça T10201166