Cybersecurity reference guide

Manuel d'utilisation

Cybersecurity reference guide

Table des matières

Cybersecurity reference guide

Présentation

Présentation

L'objectif de ce guide est de fournir une base commune et de servir de référence pour les composants liés à la cybersécurité produits par Axis. Il s'agit de descriptions, de modèles et de structures simplifiés à partir de conférences NIST, SANS, ISO et RSA, ainsi que de documents de diverses organisations de la communauté de la cybersécurité.

Liens vers d'autres documents 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*

Définition de la cybersécurité

Basée en partie sur la définition du NIST :

La cybersécurité est la protection des systèmes et services informatiques contre les cyberattaques. Les pratiques de cybersécurité comprennent des processus de prévention des dommages et de restauration des ordinateurs, des systèmes et services de communications électroniques, des communications filaires et électroniques, ainsi que des informations stockées afin de garantir leur disponibilité, leur intégrité, leur sécurité, leur authenticité, leur confidentialité et leur non-répudiation.

Types d'organisation

Les biens, les ressources, l'exposition et la cybermaturité diffèrent d'une organisation à l'autre. En suivant la pratique recommandée, *les contrôles CIS (anciennement appelés contrôles de sécurité critiques)* définissent trois profils de profils d'analyse.

- **Groupe d'implémentation SANS 1 (IG1)**

  Dans la plupart des cas, une entreprise IG1 est généralement de petite à moyenne taille avec une expertise informatique et de cybersécurité limitée pour assurer la protection des biens et du personnel informatiques.

- **Groupe d'implémentation SANS 2 (IG2)**

  Une entreprise IG2 emploie des personnes responsables de la gestion et de la protection de l'infrastructure informatique. Ces entreprises gèrent généralement plusieurs services dont les profils de risque varient en fonction de la fonction et de la mission. Les petites unités d'entreprise peuvent supporter des charges en matière de conformité réglementaire.

- **Groupe d'implémentation SANS 3 (IG3)**

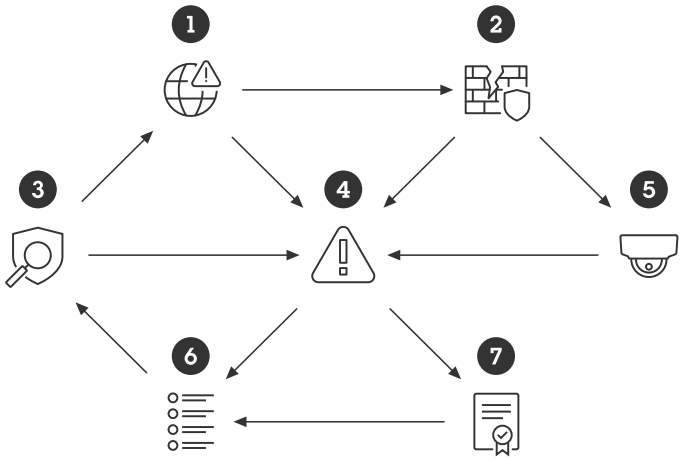
  Une entreprise IG3 emploie généralement des experts de la sécurité spécialisés dans différents domaines de la cybersécurité (par exemple, la gestion des risques, les tests de pénétration, la sécurité des applications). Les biens et données IG3 contiennent des informations ou des fonctions sensibles soumises à des dispositions réglementaires et de conformité.

Terminologie

Terminologie

Terminologie

La carte de terminologie présente les relations entre les principaux termes spécifiques à la cybersécurité et qui sont utilisés dans le présent document.



- **(1) Les menaces** exploitent **(2) les vulnérabilités** en exposant **(5) des ressources** et en augmentant **(4) les risques**
- **(4) Les risques** ont une influence **(7) sur la politique** qui indique**(6) des exigences**
- **(6) Les exigences** sont gérées dans des **(3) commandes de sécurité** , qui font constamment face à des **(1) menaces** tout en atténuant **(4) les risques**

Risque

La cybersécurité consiste à gérer les risques au fil du temps. Les risques ne peuvent jamais être éliminés, mais uniquement atténués. Parfois, les gens confondent certains termes : risque, biens, menace, vulnérabilité ou impact négatif

Le glossaire de sécurité Internet RFC 4949 définit le risque comme une prévision de perte exprimée en tant que probabilité qu'une menace particulière exploite une vulnérabilité particulière avec un résultat nuisible particulier.

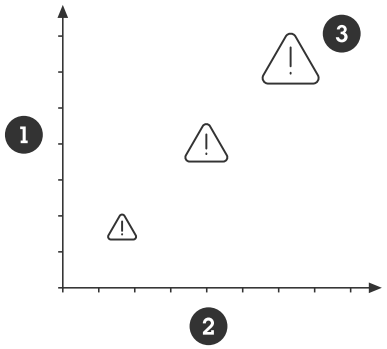
Il existe une version abrégée couramment utilisée : **Risque = Probabilité x Impact**

Cette formule est utilisée pour hiérarchiser les risques. La définition RFC inclut le terme « particulier » pour désigner menace, la vulnérabilité et le résultat nuisible. Chaque menace doit être considérée individuellement, à commencer par celle qui est la plus plausible et susceptible d'avoir l'impact négatif le plus élevé.

Le facteur de probabilité constitue un défi lors de l'évaluation d'un risque. Il est possible que des choses se produisent ou non. La probabilité qu'un adversaire exploite une vulnérabilité est souvent déterminée par la facilité d'exploitation (d'exposition) et par l'avantage potentiel pour l'adversaire d'exploiter cette vulnérabilité.

Il est possible de déterminer les risques avec les deux dimensions suivantes : utiliser la probabilité qu'un risque se produise sur un axe et l'impact du risque, s'il se produit, sur l'autre axe. Cela donne une vision claire de l'impact potentiel et de la priorité que vous devez accorder à chaque risque.

Terminologie



1 ***Probabilité*** *de la plus faible à la plus élevée*
2 ***Impact négatif*** *du plus faible au plus élevé*
3 ***Niveaux de risque*** *du plus faible au plus élevé*

Valeur d'attaque = Avantages de l'attaque – Coût de l'attaque

L'ajout d'une protection augmente le coût de l'attaque et réduit ainsi la probabilité. Le coût d'une attaque correspond à la quantité de temps, de ressources, de compétences et de formation nécessaire à la réussite de l'attaque. Le risque de se faire prendre ou d'autres conséquences négatives fait également partie du coût de l'attaque.

L'évaluation des risques, processus d'analyse des risques dans le cyberespace, est identique à celle d'une protection physique. Les questions à se poser sont les suivantes :

1. Que voulez-vous protéger ?
2. Contre qui voulez-vous vous protéger ?
3. Quelle est la probabilité d'un impact négatif ?
4. Quelles sont les conséquences si vous échouez ?
5. Quelles stratégies devez-vous mettre en œuvre pour réduire les risques ?

La mise en œuvre de mesures de protection ou de contrôle de la sécurité entraîne un certain type de coût. Toutes les organisations ont des ressources financières limitées. Si vous ne connaissez pas les risques, il est difficile d'estimer le budget à consacrer à votre protection. Vous devrez toujours accepter les risques, mais cette décision doit être une décision délibérée basée sur les risques.

L'évaluation du possible impact négatif sur chaque type de bien est difficile et complexe. Dans de nombreux cas, les estimations sont subjectifs et l'analyse des impacts est souvent approximative. L'utilisation du modèle d'impact et des types de désignation ISO 27000 (c'est-à-dire des types Limité, Sérieux, Grave ou Catastrophique) peut vous aider à obtenir une vue d'ensemble rapide de vos priorités. Il propose un moyen simple d'établir une valeur plus exacte à partir de l'estimation du temps qui serait nécessaire pour se remettre d'un impact négatif, à savoir :

- **Limité** = plusieurs heures à plusieurs jours
- **Sérieux** = plusieurs jours à plusieurs semaines
- **Grave** = plusieurs semaines à plusieurs mois
- **Catastrophique** = plusieurs mois à plusieurs années, si c'est le cas

Biens

Alors que la protection physique se concentre sur la protection des personnes et des objets physiques, la cybersécurité se concentre sur la protection des biens de données et des ressources informatiques. Il existe trois principaux domaines :

- **Confidentialité** : communication d'informations ou de ressources

- **Intégrité** : destruction ou modification d'informations ou de ressources
- **Disponibilité** : accessibilité aux informations et aux ressources

Ces zones sont également appelées triade CIA. L'Operation Technology (OT) donne souvent la priorité à la facilité d'utilisation, tandis que l'Information Technology privilégie souvent la sécurité. Trouver le bon équilibre entre confidentialité, intégrité et disponibilité est souvent difficile.

Les biens et les ressources doivent être classés afin de déterminer les niveaux de protection appropriés. Les données et les ressources informatiques ne sont pas toutes égales en termes d'impact négatif. Elles sont souvent classées comme suit :

- **Public** : les biens ciblent un consommateur public. L'impact négatif est limité si les données sont livrées au public.
- **Privé** : les biens sont privilégiés pour un groupe spécifique/sélectionné. Généralement, l'impact négatif se limite à une organisation spécifique comme une entreprise ou une famille.
- **Restreint** : les biens sont privilégiés pour des personnes sélectionnées au sein d'une organisation.

La vidéo en direct au sein d'un système vidéo peut être classée comme publique, ce qui désigne à la fois le grand public et le public au sein d'une organisation. Mais, dans la plupart des cas, la vidéo en direct est classée comme privée, ce qui signifie qu'elle n'est accessible qu'à une unité de surveillance spécifique. En parallèle, la vidéo enregistrée, dans la plupart des cas, est classée comme étant à accès restreint, car certaines scènes peuvent être très sensibles. Les informations d'identification et les configurations sont également des données à classer comme restreintes.

Menaces

Une menace peut être définie comme tout ce qui peut compromettre ou endommager vos biens ou votre ressource. En général, les personnes ont tendance à associer les cybermenaces à des personnes malveillantes et des logiciels malveillants. En réalité, les impacts négatifs sont souvent dus à des accidents, des usages abusifs non intentionnels ou une panne matérielle.

Les attaques ne surgissent pas de bulle part. Il y a toujours une motivation à compromettre un système et ses ressources. Les attaques peuvent être classées comme opportunistes ou ciblées. En cybersécurité, les auteurs d'attaques sont également appelés adversaires qui peuvent avoir une intention malveillante.

La majorité des attaques d'aujourd'hui sont opportunistes : attaques qui se produisent simplement parce qu'une opportunité s'est présentée. Dans de nombreux cas, un agresseur opportuniste externe ne sait même pas qui est la victime. Ces agresseurs utilisent des vecteurs d'attaque peu coûteux tels que le hameçonnage et le sondage. Dans ce cas, ils n'ont pas la volonté de consacrer du temps et des ressources à une attaque ratée ; ils passent rapidement à leur prochaine tentative. L'application d'un niveau de protection standard atténue la plupart des risques liés aux attaques opportunistes. Il est plus difficile de se protéger contre les attaques ciblées, ces agresseurs qui ciblent un système spécifique avec un objectif spécifique. Les attaques ciblées utilisent les mêmes vecteurs d'attaque à faible coût que les attaques opportunistes. Toutefois, si les attaques initiales échouent, elles sont plus déterminées et prêtes à consacrer du temps et des ressources pour utiliser des méthodes plus sophistiquées pour atteindre leurs objectifs. Pour celles-ci, il s'agit en grande partie de savoir quelle est l'enjeu.

Adversaires courants (acteurs de menace)

- **Proches et parents** : personnes qui souhaitent s'immiscer dans votre vie personnelle
- **Employés** : ou personnes ayant accédé légitimement au système, soit par accident, soit par usages abusifs délibérés
- **Farceurs** : personnes qui considèrent qu'une intrusion dans des systèmes informatiques représente un défi stimulant
- **Hacktivistes** : personnes qui mènent des attaques contre des organisations pour des motifs politiques ou idéologiques
- **Cybercriminels** : personnes qui cherchent à gagner de l'argent par la fraude ou la vente d'informations de valeur
- **Concurrents industriels** : entités souhaitant bénéficier d'un avantage économique pour leurs entreprises ou leurs organisations
- **Cyberterroristes** : personnes ou entités qui effectuent une attaque destinée à déclencher une alarme ou un mouvement de panique, souvent pour des raisons idéologiques ou politiques.

- **États** : agents des services de renseignements étrangers qui agissent soit pour obtenir des gains économiques/politiques, soit pour endommager des systèmes d'information critiques.
- **Particuliers** : personne ou groupe spécifique agissant seul lorsque la motivation peut différer de celle énumérée ci-dessus. Il peut s'agir d'un journaliste d'investigation, d'un pirate en chapeau blanc ou similaire. Les pirates en chapeau blanc (ou « hackers éthiques ») peuvent constituer une menace si vous privilégiez la dissimulation des défauts plutôt que leur correction.

Vulnérabilité

Tous les systèmes comportent des vulnérabilités. Les vulnérabilités offrent des possibilités d'attaque ou d'accès à un système. Elles peuvent être le résultat de défauts, d'exposition, de fonctionnalités ou d'erreurs humaines. Des personnes malveillantes peuvent chercher à exploiter les vulnérabilités connues, en associant souvent une ou plusieurs vulnérabilités. La majorité des violations réussies sont dues à des erreurs humaines, à des systèmes mal ou à des systèmes peu entretenus – souvent en raison de l'absence de politiques adéquates, de responsabilités non définies et d'une faible sensibilisation organisationnelle.

Vulnérabilités logicielles

Une API (interface de programmation d'applications) et des services logiciels peuvent comporter des défauts ou des fonctionnalités exploitables lors d'une attaque. Aucun fournisseur ne peut jamais garantir que ses produits n'ont pas de défauts. Si les failles sont connues, les risques peuvent être atténués au moyen de mesures de contrôle de sécurité de compensation. D'un autre côté, si un hacker découvre une nouveau défaut inconnu, le risque d'attaques Zero Day est accru, car la victime n'a pas eu le temps de protéger le système.

The Common Vulnerability Scoring System (CVSS) est un moyen de classer la gravité d'une vulnérabilité logicielle. Il s'agit d'une formule qui estime le degré de facilité d'exploitation et ses impacts négatifs. Le score est une valeur entre 0 et 10, 10 représentant la gravité la plus élevée. Vous trouverez souvent un numéro CVSS dans les rapports CVE (Common Vulnerabilities and Exposures) publiés.

Axis utilise le CVSS comme l'une des mesures visant à déterminer le niveau critique d'une vulnérabilité identifiée dans le logiciel/le produit

Politique

Il est important de définir des politiques et processus système clairs pour parvenir à une réduction adéquate des risques à long terme. L'une des méthodes recommandées consiste à mettre en place un cadre de protection ITbien défini, tel que ISO 27001, NIST ou similaire. Même si cette tâche peut sembler écrasante pour les petites organisations, il vaut nettement mieux disposer d'une documentation, même minimale, sur la politique et les processus.

Contrôles de sécurité

Les contrôles de sécurité sont les garde-fous ou les contremesures utilisés pour éviter, détecter, neutraliser ou minimiser les risques de sécurité touchant les propriétés physiques, les informations, les systèmes informatiques ou les autres biens. Les processus de déploiement des contrôles de sécurité sont souvent appelés renforcement.

Les contrôles de sécurité de compensation sont des protections qui peuvent aussi être utilisées lorsqu'il n'est pas possible d'appliquer le contrôle de sécurité préféré ou lorsque le contrôle préféré peut ne pas être disponible ou être trop coûteux.

Les contrôles de sécurité doivent être constamment surveillés et mis à jour, car les menaces, la valeur, les vulnérabilités et l'exposition évoluent au fil du temps. Pour ce faire, il est nécessaire de définir et de suivre des politiques et processus.

SANS Institute a publié une *liste des contrôles CIS*, ensemble recommandé de meilleures pratiques de cyberdéfense prioritaires. Voici la liste dans son intégralité pour illustrer la diversité des contrôles de sécurité.

- Commande CIS n°1 : Inventaire et contrôle des ressources d'entreprise
- Commande CIS n°2 : Inventaire et contrôle des ressources logicielles
- Commande CIS n°3 : Protection des données
- Commande CIS n°4 : Configuration sécurisée des ressources et logiciels d'entreprise

Terminologie

- Commande CIS n°5 : Gestion de compte
- Commande CIS n°6 : Gestion du contrôle d'accès
- Commande CIS n°7 : Gestion continue des vulnérabilités
- Commande CIS n°8 : Gestion des journaux d'audit
- Commande CIS n°9 : Protections par e-mail et navigateur Web
- Commande CIS n°10 : Défenses contre les logiciels malveillants
- Commande CIS n°11 : Récupération des données
- Commande CIS n°12 : Gestion de l'infrastructure réseau
- Commande CIS n°13 : Surveillance et défense réseau
- Commande CIS n°14 : Sensibilisation à la sécurité et formation aux compétences
- Commande CIS n°15 : Gestion des fournisseurs de services
- Commande CIS n°16 : Sécurité des logiciels d'application
- Commande CIS n°17 : Gestion de la réponse aux incidents
- Commande CIS n°18 : Tests de pénétration

Le *Guide de renforcement AXIS OS* repose sur CIS.

Mesures de protection contre les menaces courantes

En comprenant et en contrant les menaces communes, vous pouvez atténuer la majorité des risques.

Usage abusif délibéré ou accidentel du système

L'équilibre entre l'exploitation et la sécurité d'un système est difficile. De nombreux systèmes sont renforcés pour des raisons pratiques, et non à des fins de sécurité. Cela crée des occasions d'usages abusifs délibérés ou accidentels. Les personnes ayant un accès légitime à un système sont l'une des menaces les plus courantes pour un système.

Exemples de menaces courantes :

- Les personnes peuvent accéder à des services (vidéo en direct ou enregistrée, par exemple) pour lesquelles elles n'ont pas d'autorisation
- Erreurs individuelles
- Des personnes peuvent essayer de corriger des problèmes, ce qui entraîne une réduction des performances système.
- Des personnes mécontentes peuvent provoquer des actes d'endommagement délibérés du système
- Des personnes sont exposées à l'ingénierie sociale
- Vols
- Ces personnes peuvent perdre ou déplacer des composants critiques (cartes d'accès, téléphones, ordinateurs portables, documentation, etc.)
- Les ordinateurs de ces personnes peuvent être compromis et infecter de manière non intentionnelle un système avec des logiciels malveillants

Les mesures de protection les plus fréquemment recommandées sont les suivantes :

- Politique et processus de compte utilisateur
- Schéma d'authentification d'accès suffisant
- Outils pour la gestion des comptes et des privilèges utilisateur au fil du temps
- Réduire l'exposition
- Formation à la cybersécurité

Comment Axis peut contribuer à contrer cette menace :

- Le manuel *AXIS OS Hardening Guide* décrit les contrôles de sécurité communs pour les menaces courantes d'un périphérique.
- Le manuel *AXIS Camera Station Hardening Guide* décrit les contrôles de sécurité les plus courants pour les systèmes vidéo.
- Les manuels *AXIS Device Manager* et *AXIS Device Manager Extend* permettent de gérer les contrôles de sécurité communs

Sabotage physique et vandalisme

La protection physique des systèmes informatiques est très importante du point de vue de la cybersécurité.

Exemples de menaces courantes :

- Les équipements exposés physiquement peuvent être sabotés
- Les équipements exposés physiquement peuvent être volés

- Les câbles exposés physiquement peuvent être déconnectés, redirigés ou coupés

Les mesures de protection les plus fréquemment recommandées sont les suivantes :

- Placer l'équipement réseau (serveurs et commutateurs, par exemple) dans des zones verrouillées
- Installer les caméras de sorte qu'elles soient difficiles d'accès
- Utiliser un boîtier de protection en cas d'exposition physique
- Protéger les câbles dans des murs ou des conduites

Comment Axis peut contribuer à contrer cette menace :

- Carte SD cryptée pour empêcher la lecture de vidéos si un utilisateur non autorisé peut éjecter la carte SD
- Détection de sabotage de l'affichage de la caméra
- Détection d'un boîtier ouvert

Exploitation des vulnérabilités logicielles connues

Tous les produits basés sur des logiciels présentent des vulnérabilités qui peuvent être exploitées. Ces éléments peuvent être classés comme connus ou inconnus. Toutes les vulnérabilités inconnues seront éventuellement connues ; ce n'est qu'une question de temps. La plupart des vulnérabilités sont à faible risque, ce qui signifie qu'elles sont très difficiles à exploiter ou que leur impact négatif est limité. Parfois, des vulnérabilités peuvent être découvertes et exploitées, ce qui a un impact négatif important. MITRE héberge une large base de données CVE (Common Vulnerabilities et Exposures) pour aider à atténuer les risques.

Les mesures de protection les plus fréquemment recommandées sont les suivantes :

- Un processus de correctifs continu qui contribue à réduire le nombre de vulnérabilités connues dans un système.
- Une réduction de l'exposition au réseau afin de rendre plus difficile l'analyse et l'exploitation des vulnérabilités connues.
- Une collaboration avec des sous-fournisseurs de confiance qui appliquent des politiques et des processus qui réduisent les défauts, qui fournissent des correctifs et sont transparents sur les vulnérabilités critiques découvertes.

Comment Axis peut contribuer aider :

- Le *Modèle de développement de sécurité d'Axis* est un cadre qui définit les processus et les outils utilisés par Axis pour réduire le risque de publication de produits avec des vulnérabilités logicielles.
- La *politique de gestion des vulnérabilités d'Axis* implique d'identifier, de corriger et de réduire les vulnérabilités dont les clients doivent avoir connaissance pour prendre les mesures appropriées. Depuis avril 2021, Axis est approuvée en tant que CVE (Common Vulnerability and Exposures) Numbering Authority (CNA) pour les produits Axis, ce qui nous permet d'adapter nos processus au processus standard de l'entreprise MITRE.) Cela nous permet d'aider nos clients de manière plus efficace.
- *Les guides de renforcement de la sécurité Axis*, tels que *Axis OS Hardening Guide*, fournissent des recommandations sur la façon de réduire l'exposition et d'ajouter des contrôles de compensation pour réduire le risque d'exploitation des failles logicielles.
- Les versions de firmware LTS (assistance à long terme) permettent aux clients d'appliquer des correctifs au système d'exploitation des périphériques Axis tout en réduisant les risques d'incompatibilité avec les systèmes de gestion vidéo tiers.

Attaque de la chaîne d'approvisionnement

Une attaque de chaîne d'approvisionnement est une cyberattaque qui cherche à endommager une organisation en visant des éléments moins sécurisés de la chaîne d'approvisionnement. Elle est principalement utilisée lorsque d'autres vecteurs d'attaque (par exemple, l'ingénierie sociale, les attaques par hameçonnage et le sondage d'interface) échouent en raison de niveaux élevés de protection du système. Cette attaque s'effectue en compromettant les logiciels/ firmware/produits et en faisant pression pour qu'un administrateur les installe sur le système. Un produit peut ainsi être compromis lors de l'expédition vers le propriétaire du système. Pour réussir une attaque de la chaîne d'approvisionnement, il faut des compétences, du temps et des ressources.

Mesures de protection contre les menaces courantes

Les mesures de protection les plus fréquemment recommandées sont les suivantes :

- Disposer d'une politique d'installation des seuls logiciels à partir de sources fiables et vérifiées.
- Vérifier l'intégrité du logiciel par comparaison de la somme de contrôle du logiciel (digest) avec la somme de contrôle du fournisseur avant l'installation.
- Lors d'une livraison, vérifier l'intégrité du logiciel.

Comment Axis peut contribuer à contrer cette menace :

- Un logiciel Axis est publié avec une somme de contrôle, ce qui permet aux administrateurs de valider son intégrité avant de procéder à l'installation.
- Le firmware signé sur un périphérique Axis garantit que le système d'exploitation installé (AXIS OS) provient véritablement d'Axis et que tout nouveau firmware à télécharger et à installer sur le périphérique est également signé par Axis.
- Le démarrage sécurisé sur un périphérique Axis permet au périphérique de vérifier que le firmware comporte une signature Axis. Si le firmware n'est pas autorisé ou a été modifié, le processus de démarrage est interrompu.
- L'ID d'un périphérique Axis conforme à la norme IEEE 802.1AR est un certificat du fournisseur Axis propre au périphérique qui permet au système de vérifier que le matériel à l'intérieur du boîtier provient d'Axis.
- Le cryptage de carte SD et le cryptage de système de fichiers empêchent l'extraction des données stockées en cas de vol de la carte ou du périphérique.

Manuel d'utilisation
Cybersecurity reference guide

Ver. M3.2
Date : Novembre 2023
Référence T10201166