Cybersecurity Q&As

Manuel d'utilisation

Pour toute autre questions, consultez la *base de données FAQ* d'Axis.

Cybersecurity Q&As

Questions générales

Questions générales

Qu'est-ce que la cybersécurité ?

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.

La cybersécurité consiste à gérer les risques sur une plus longue période. Les risques ne peuvent jamais être éliminés, mais uniquement atténués.

Qu'est-ce qui est généralement impliqué dans la gestion de la cybersécurité ?

La cybersécurité concerne les produits, les personnes, les technologies et les processus en cours.

Il s'agit donc **d'identifier** et d'évaluer divers aspects de votre organisation, y compris l'inventaire des périphériques, systèmes, logiciels et firmwares, l'établissement d'objectifs critiques ; la documentation des procédures et des politiques de sécurité ; l'application d'une stratégie de gestion des risques et l'établissement permanent de risques liés à vos biens.

Cela implique la mise en œuvre de contrôles de sécurité et de mesures visant à **protéger** les données, les périphériques, les systèmes et les installations que vous avez identifiés comme priorités contre les cyberattaques.

Cela implique également de développer et de mettre en œuvre des activités qui vous aideront à **détecter** les cyberattaques afin de pouvoir prendre des mesures en temps utile. Cela peut, par exemple, impliquer l'utilisation d'un système SIEM (Security Information and Event Management) ou d'un système SOAR (Security Orchestration, Automation and Response) qui gère les données des périphériques réseau et des logiciels de gestion, qui analyse les données relatives aux comportements anormaux ou les cyberattaques potentielles, puis analyse ces données pour fournir des alertes en temps réel. Les périphériques Axis sont connectés aux journaux SYS et aux journaux SYS distants, qui sont la principale source de données de votre système SIEM ou SOAR.

La gestion de la cybersécurité implique également l'élaboration et la mise en œuvre de procédures pour **répondre** à un incident de cybersécurité dès qu'il est détecté. Vous devez tenir compte des réglementations locales et des politiques internes, ainsi que des exigences de confidentialité des incidents de cybersécurité. Axis propose un guide *AXIS OS Forensic Guide* qui peut vous aider à comprendre si un périphérique Axis a été compromis lors d'une attaque de cybersécurité.

Il est également important de développer et de mettre en œuvre des activités pour maintenir la résilience et **récupérer** ou restaurer des fonctions ou des services déficients en raison d'un incident de cybersécurité. *AXIS Device Manager*, par exemple, facilite la restauration des périphériques Axis avec des points de restauration, qui sont des « instantanés » enregistrés de la configuration système à un moment donné. En l'absence d'un point de restauration approprié, l'outil peut aider à rétablir tous les périphériques à leurs états par défaut et à récupérer des modèles de configuration enregistrés via le réseau.

Quels sont les risques de cybersécurité ?

Les risques de cybersécurité (tels que définis par le glossaire de sécurité Internet RFC 4949) sont les prévisions de perte exprimées en tant que probabilité qu'une menace particulière exploite une vulnérabilité particulière avec un résultat nuisible particulier.

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.

Pour plus d'informations sur l'évaluation des risques et leur hiérarchisation, consultez le *guide de référence sur la cybersécurité*.

Quelles sont les menaces ?

Une menace peut être définie comme tout ce qui peut compromettre ou endommager vos biens ou vos ressources. 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

peuvent être classées comme opportunistes ou ciblées. La majorité des attaques d'aujourd'hui sont opportunistes : attaques qui se produisent simplement parce qu'une opportunité s'est présentée. De telles attaques utilisent des vecteurs d'attaque peu coûteux tels que le hameçonnage et le sondage. 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 personnes malveillantes 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.

Quelles sont les menaces les plus courantes et comment les traiter ?

Usage abusif délibéré ou accidentel d'un système

Les personnes ayant un accès légitime à un système sont l'une des menaces les plus courantes pour un système. Elles peuvent accéder à des services sur lesquels elles ne disposent pas d'autorisations. Elles peuvent provoquer des actes de vol ou d'endommagement délibérés du système. Ces personnes peuvent également faire des erreurs. En s'efforcent de résoudre les problèmes, elles risquent de réduire de façon considérable les performances du système. Ces individus sont également sensibles de pratiquer l'ingénierie sociale, c'est-à-dire des astuces qui permettent d'inciter les utilisateurs légitimes à fournir des informations sensibles. 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 protections recommandées comprennent la définition d'une politique et d'un processus de compte utilisateur, la création d'un système d'authentification d'accès suffisant, la gestion des comptes utilisateurs et des privilèges au fil du temps, la réduction de l'exposition et une formation sur la cybersécurité.

Axis aide à contrer cette menace avec *des guides de renforcement de la sécurité* et des outils tels que *AXIS Device Manager* et *AXIS Device Manager Extend*.

Sabotage physique et vandalisme

Les équipements exposés physiquement peuvent être sabotés, détournés, volés, déconnectés, redirigés ou coupés.

Les protections recommandées comprennent le placement des équipements réseau (par exemple, les serveurs et les commutateurs) dans des zones verrouillées, le montage de caméras de sorte qu'elles soient difficiles d'accès, l'utilisation d'un boîtier protégé lorsqu'elles sont physiquement exposées, et la protection des câbles dans des murs ou des conduits.

Axis aide à contrer cette menace avec un *boîtier de protection* pour les périphériques, des vis inviolables, des caméras capables de crypter les cartes SD, la détection de sabotage et la détection de boîtier ouvert.

Exploitation des vulnérabilités logicielles

Tous les produits basés sur des logiciels présentent des vulnérabilités (connues ou inconnues) qui peuvent être exploitées. 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 protections recommandées comprennent un processus de correctifs continu qui contribue à réduire le nombre de vulnérabilités connues dans un système, la réduction de l'exposition au réseau afin de rendre plus difficile l'analyse et l'exploitation des vulnérabilités connues, et la 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.

Axis répond à cette menace avec le *Modèle de développement de sécurité Axis*, qui vise à minimiser les vulnérabilités exploitables du logiciel Axis, ainsi qu'avec la *Politique de gestion des vulnérabilités Axis*, qui identifie, résout et annonce les vulnérabilités que les clients doivent connaître pour prendre les mesures appropriées. (En avril 2021, *Axis a été 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 .) Axis fournit également des *guides de renforcement de la sécurité* avec des recommandations sur la façon de réduire l'exposition et d'ajouter des contrôles pour réduire le risque d'exploitation. Axis propose aux utilisateurs *deux suivis différents du firmware* afin de maintenir à jour le firmware d'un périphérique Axis :

1. Le suivi actif fournit les mises à jour de firmware qui prennent en charge de nouvelles fonctionnalités, ainsi que des résolutions de bogues et des correctifs de sécurité.

2. Le suivi de support à long terme (LTS) propose des mises à jour de firmware qui prennent en charge les résolutions de bogues et les correctifs de sécurité tout en réduisant les risques d'incompatibilité avec des systèmes 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. 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.

Les protections recommandées comprennent une politique d'installation des seuls logiciels à partir de sources fiables et vérifiées, la vérification de l'intégrité du logiciel par comparaison de la somme de contrôle du logiciel (digest) avec la somme de contrôle du fournisseur avant l'installation, la vérification des livraisons de produits pour vérifier l'intégrité du logiciel.

Axis contre-attaque cette menace de plusieurs façons. Axis édite un logiciel avec une somme de contrôle pour permettre aux administrateurs de valider l'intégrité avant de procéder à l'installation. Lorsqu'un nouveau firmware doit être chargé, les périphériques en réseau Axis acceptent uniquement les firmware signés par Axis. Le *démarrage sécurisé* sur les périphériques en réseau Axis garantissent également que seul le firmware signé par Axis exécute les périphériques. Et chaque périphérique dispose d'un ID périphérique Axis unique, qui permet au système de vérifier que le périphérique est un produit Axis authentique. Les détails de ces fonctions de cybersécurité sont fournis dans le livre blanc *Cybersecurity features in Axis products* (pdf).

Pour plus d'informations sur les menaces, consultez le *guide de référence sur la cybersécurité*.

Que sont les vulnérabilités ?

Les vulnérabilités offrent des possibilités d'attaque ou d'accès à un système. Elles peuvent être le résultat de défauts, 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 et à des systèmes peu entretenus – souvent en raison de l'absence de politiques adéquates, de responsabilités non définies et d'une faible sensibilisation organisationnelle.

Quelles sont les 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. D'un autre côté, si un hacker découvre une nouveau défaut inconnu, le risque est accru, car la victime n'a pas eu le temps de protéger le système.

Qu'est-ce que CVSS (Common Vulnerability Scoring System) ?

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 Vulnerability and Exposure) 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.

Cybersecurity Q&As

Questions spécifiques à Axis

Questions spécifiques à Axis

Quelle formation et quels guides sont disponibles pour m'aider à en savoir plus sur la cybersécurité et ce que je peux faire pour mieux protéger les produits et services contre les cyber incidents ?

La page Web *Resources* web vous permet d'accéder à des guides de renforcement de la sécurité (par ex. *AXIS OS Hardening Guide*, *AXIS Camera Station System Hardening Guide* et *Axis Network Switches Hardening Guide*), des documents sur les règles, et bien d'autres. Axis propose également un cours *e-learning* sur la cybersécurité.

Où puis-je trouver le firmware le plus récent pour mon périphérique ?

Allez à *Firmware* et recherchez votre produit.

Comment puis-je facilement mettre à niveau le firmware sur mon périphérique ?

Pour mettre à niveau le firmware de vos périphériques, vous pouvez utiliser des logiciels de gestion vidéo Axis tels que *AXIS Companion* or *AXIS Camera Station*, ou des outils tels que *AXIS Device Manager* et *AXIS Device Manager Extend*.

En cas d'interruption des services Axis, comment puis-je en être informé ?

Visitez le site *status.axis.com*.

Comment puis-je être notifié d'une vulnérabilité découverte ?

Vous pouvez vous inscrire au *Service de notification de sécurité Axis*.

Comment Axis gère-t-il les vulnérabilités ?

Consultez la *Politique de gestion des vulnérabilités d'Axis*.

Comment Axis réduit-il les vulnérabilités logicielles ?

Lisez l'article *Intégrer la cybersécurité au développement des logiciels Axis*.

Comment Axis prend-il en charge la cybersécurité tout au long du cycle de vie des périphériques ?

Lisez l'article *Prise en charge de la cybersécurité tout au long du cycle de vie des périphériques*.

Quelles sont les caractéristiques des fonctions de cybersécurité intégrées aux produits Axis ?

En découvrir plus :

- *Fonctions de cybersécurité intégrées*
- *Caractéristiques de cybersécurité des produits Axis* (pdf)
- *Prise en charge de la cybersécurité tout au long du cycle de vie des périphériques*

Cybersecurity Q&As

Questions spécifiques à Axis

AXI est-il certifié ISO et à quelles autres réglementations se conforme Axis ?

Rendez-vous sur la page Web *Conformité*.

Manuel d'utilisation
Cybersecurity Q&As

Ver. M2.3
Date : Novembre 2023
Référence T10189380