Prérequis

Ce chapitre s'adresse aux lecteurs disposant de notions de base en informatique et en réseaux. Une compréhension préalable des protocoles fondamentaux et des architectures client-serveur sera utile pour mieux appréhender les concepts abordés ici.

Objectifs

L'objectif principal de ce chapitre est d'introduire les concepts essentiels de la sécurité informatique. Ce chapitre n'a pas pour vocation de couvrir l'intégralité du domaine de la cybersécurité, qui est vaste et en constante évolution. Il vise plutôt à **poser des bases solides**, en mettant l'accent sur les notions fondamentales que vous devrez maîtriser dans le cadre de la certification CEH.

Vous apprendrez à maîtriser la terminologie clé, à comprendre les modèles de sécurité fondamentaux comme la triade CIA (*Confidentiality, integrity, availability* - Confidentialité, Intégrité, Disponibilité) et le modèle AAA (Authentification, Autorisation, Audit). Vous serez également en mesure d'identifier les principales menaces et vulnérabilités, et de saisir l'importance des politiques et procédures pour une gestion efficace de la sécurité.

A. Terminologie clé en cybersécurité

1. Menaces, vulnérabilités, attaques

En cybersécurité, un terme revient souvent : la **menace**. Il désigne tout potentiel événement capable de nuire à un système informatique ou d'exploiter une vulnérabilité. Les menaces peuvent être intentionnelles, comme les attaques menées par des hackers, ou accidentelles, telles que les erreurs humaines.

Ensuite, il y a la **vulnérabilité**, une faiblesse ou une faille présente dans un système qui peut être exploitée par une menace pour causer des dommages ou accéder à des informations de manière non autorisée. Les vulnérabilités résultent souvent de bugs de programmation, de configurations incorrectes ou de la non-application de correctifs.

La notion d'**attaque** fait référence à toute initiative visant à compromettre la confidentialité, l'intégrité ou la disponibilité d'un système. Ces attaques sont souvent classifiées selon leur nature, leur cible ou leur mécanisme d'exploitation. Par exemple, les attaques par force brute, visant à contourner des mécanismes d'authentification en devinant les mots de passe, en sont une illustration courante.

2. Surface d'attaque et gestion des risques

La surface d'attaque désigne **l'ensemble des points d'entrée potentiels** qu'un attaquant peut exploiter pour accéder à un système. Cela inclut des éléments tels que les interfaces utilisateur, les API, les ports réseau ouverts ou encore les configurations mal sécurisées. Plus cette surface est grande, plus le risque d'exploitation augmente. Une réduction de la surface d'attaque passe par la suppression des points d'entrée inutiles, la segmentation réseau et l'adoption de contrôles d'accès stricts.

Le risque en cybersécurité est une combinaison de la probabilité qu'une menace exploite une vulnérabilité et de l'impact potentiel de cette exploitation. Une évaluation efficace des risques repose sur l'identification des actifs critiques, la compréhension des menaces pertinentes et l'analyse de leur impact potentiel. Cette approche permet aux organisations de prioriser leurs efforts en matière de cybersécurité et de concentrer leurs ressources sur les zones les plus vulnérables.

B. Modèles de sécurité (CIA, AAA)

Les modèles de sécurité constituent des cadres théoriques pour établir des stratégies de protection des systèmes d'information. Ils permettent d'articuler les différents aspects de la sécurité en garantissant à la fois la protection des données, la gestion des accès et la surveillance des activités. Parmi ces modèles, la **triade CIA** et le **modèle AAA** sont les plus répandus et largement appliqués dans les environnements professionnels.

1. Modèle de sécurité CIA

Le modèle de sécurité **CIA** est un ensemble de principes fondamentaux qui guide la protection des informations et des systèmes informatiques. Il représente trois piliers essentiels : la Confidentialité, l'Intégrité et la Disponibilité.

a. Confidentialité

La confidentialité concerne la protection des **informations sensibles** afin d'empêcher leur accès non autorisé. Dans le domaine de la cybersécurité, cette notion implique la mise en place de mécanismes tels que le chiffrement des données, l'authentification de l'utilisateur et le contrôle d'accès. L'objectif est de garantir que seules les personnes ayant les autorisations appropriées peuvent accéder aux informations critiques. Le respect de ce principe est crucial pour maintenir la confiance des utilisateurs, notamment dans des secteurs comme la finance ou la santé.

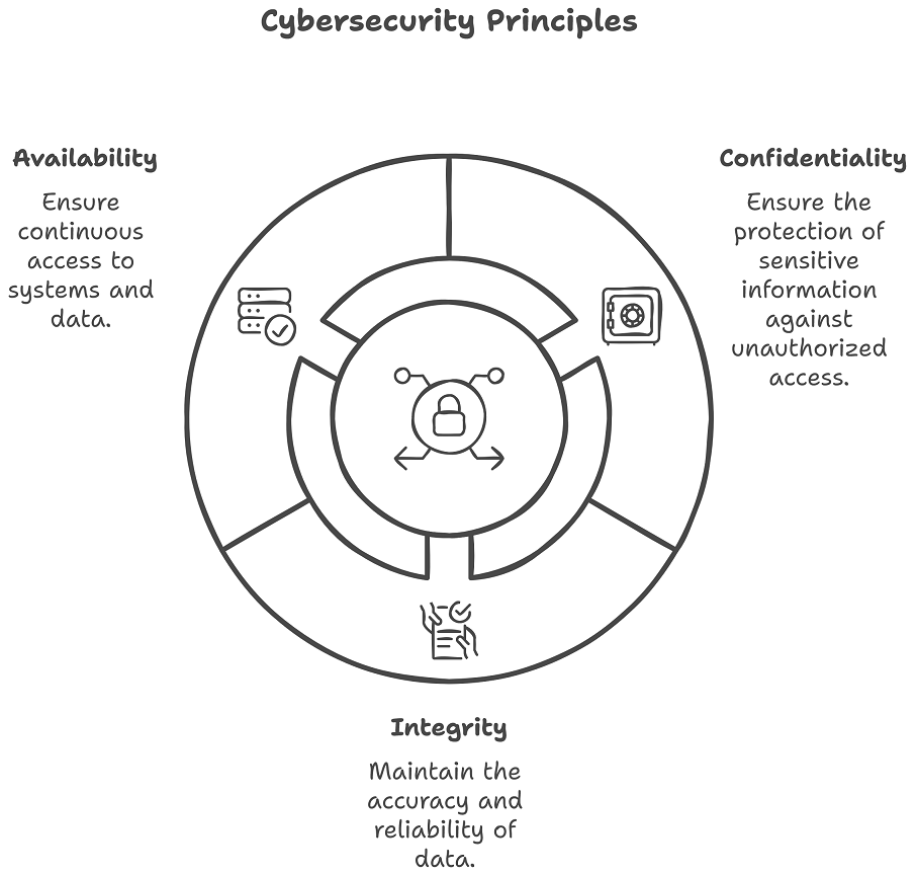
b. Intégrité

L'intégrité assure que les données ne sont modifiées que par des acteurs autorisés et que toute altération est détectable. Il est **essentiel** dans ce domaine de s'assurer que les informations ne sont altérées ni pendant leur stockage ni durant leur transmission. Des techniques telles que les signatures numériques et les hachages cryptographiques sont souvent utilisées pour garantir le maintien de l'intégrité des données. Un défaut dans ce principe peut entraîner des décisions erronées, fondées sur des informations incorrectes.

c. Disponibilité

La disponibilité concerne l'accessibilité des systèmes et des données par les utilisateurs autorisés lorsque cela est nécessaire. Il est impératif que les services soient disponibles de manière continue afin de garantir la continuité des activités. Des stratégies telles que les **sauvegardes régulières**, la mise en place de systèmes de redondance et la mise en place de solutions de sécurité en amont sont mises en œuvre pour préserver la disponibilité. L'impératif de disponibilité répond à la nécessité pour les utilisateurs de pouvoir accéder aux services à tout moment.

☞*Pour faciliter la mémorisation du modèle de sécurité CIA :*



2. Modèle de sécurité AAA

Le modèle AAA (*Authentication, Authorization, Accounting*), est un cadre détaillé visant à sécuriser les environnements informatiques en vérifiant les identités et les permissions des utilisateurs tout en surveillant leurs actions.

a. Authentification

L'authentification est le **processus de vérification de l'identité d'un utilisateur**. Elle est réalisée à l'aide de différentes méthodes, telles que les mots de passe, les cartes à puce, ou les données biométriques comme les empreintes digitales. Ce processus est essentiel pour empêcher l'accès non autorisé aux systèmes informatiques. L'implémentation de l'authentification multifactorielle (MFA) est de plus en plus répandue car elle combine plusieurs méthodes pour renforcer la sécurité.

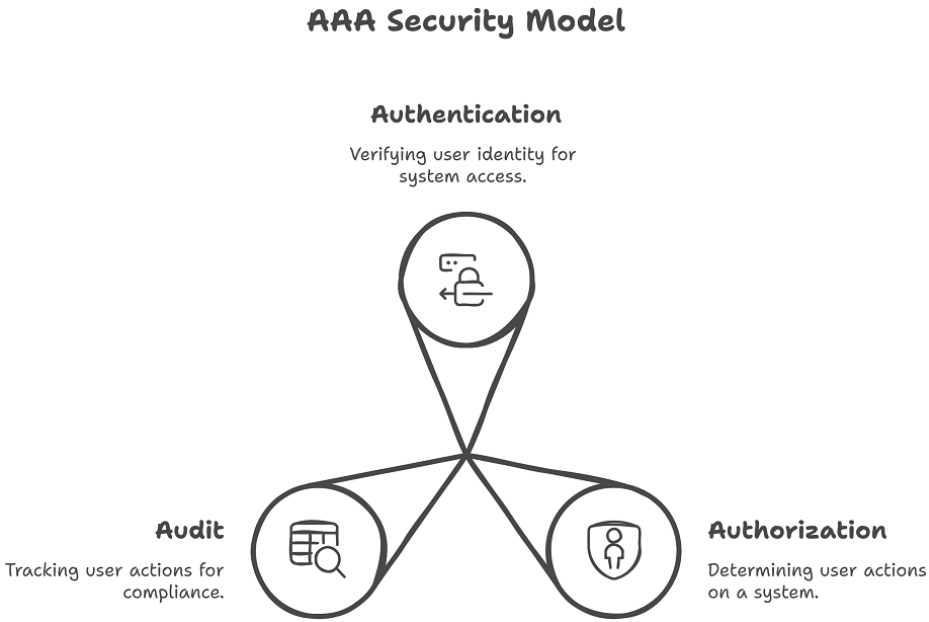
b. Autorisation

L'autorisation intervient après l'authentification et **détermine les actions qu'un utilisateur peut effectuer sur un système ou une ressource donnée**. Ce processus garantit que les utilisateurs ne peuvent accéder qu'aux informations et effectuer les actions pour lesquelles ils ont été expressément autorisés. L'application correcte de l'autorisation protège contre l'escalade de privilèges et minimise les risques internes liés à des droits d'accès excessifs.

c. Accounting (journalisation)

La journalisation est le processus qui consiste à **suivre et à enregistrer les actions des utilisateurs** pour assurer la conformité et identifier les anomalies potentielles notamment via un **audit**. Il agit comme un filet de sécurité en fournissant une piste d'audit qui peut être utilisée pour reconstituer des événements et identifier des comportements malveillants. Un audit efficace permet d'optimiser les stratégies de sécurité en détectant et en corrigeant les vulnérabilités au sein du système.

☞*Pour faciliter la mémorisation du modèle de sécurité AAA :*



C. Principales menaces et vulnérabilités

1. Menaces ciblées et avancées

Certaines attaques ne sont pas aléatoires, mais soigneusement préparées pour viser des cibles précises. Ces menaces, dites **avancées ou ciblées**, représentent un grand danger pour les organisations car elles sont conçues pour contourner les défenses classiques.

a. Attaques ciblées

Les attaques ciblées sont menées par des acteurs ayant un objectif précis : obtenir un accès non autorisé à des données sensibles, perturber un service, ou espionner une activité. Ces campagnes sont souvent précédées d'une phase de reconnaissance durant laquelle les attaquants collectent un maximum d'informations sur leur cible (employés, infrastructures, technologies utilisées).

Ils peuvent ensuite exploiter des vulnérabilités techniques ou recourir à des méthodes de social engineering comme le phishing personnalisé. L'impact de ces attaques peut être sévère : perte de données, atteinte à la réputation, arrêt d'activité ou même fuite d'informations confidentielles.

b. Espionnage industriel

L'espionnage industriel est une forme spécifique de menace stratégique où des organisations adverses cherchent à accéder illégalement à des informations confidentielles ou propriétaires.

Les techniques de cyberespionnage incluent l'utilisation de chevaux de Troie pour infiltrer les systèmes, ainsi que le recours à des insiders, c'est-à-dire des employés ou associés ayant accès à des données précieuses, et qui peuvent être manipulés ou incités à les divulguer.

Les entreprises technologiquement avancées sont souvent ciblées dans un contexte d'espionnage industriel, car ces attaques peuvent fournir aux concurrents un avantage injuste sur le marché.

2. Vulnérabilités techniques

Les vulnérabilités techniques présentes dans le code des applications web offrent aux attaquants des points d'entrée privilégiés pour mener leurs activités malveillantes. Ces **vulnérabilités techniques** peuvent résulter d'erreurs de conception, de mauvaises pratiques de développement, ou d'un manque de mise à jour des composants.

a. Injections de code

Les injections de code, telles que les **injections SQL** et les attaques de type **Cross-Site Scripting (XSS)**, sont parmi les techniques les plus courantes et les plus nuisibles. Elles permettent aux pirates de manipuler directement le fonctionnement d'une application pour voler des données ou détourner des sessions.

Ces attaques exploitent des failles dans le traitement des entrées utilisateurs. Une application qui ne valide ni ne nettoie correctement les données d'entrée est susceptible d'être vulnérable aux injections de code. Un attaquant peut insérer des scripts malveillants qui seront exécutés par le navigateur de la victime, compromettant ainsi sa sécurité.

Renforcer la validation des données et utiliser des requêtes préparées sont des actions essentielles pour prévenir ces vulnérabilités.

b. Contrôle d'accès défaillant

Un contrôle d'accès inadéquat peut conduire à des **violations de sécurité** exploitables par des utilisateurs non autorisés. Un mauvais paramétrage ou une gestion défaillante des privilèges d'accès permet aux personnes malintentionnées d'accéder à des ressources restreintes.

Pour sécuriser une application web contre de tels risques, il est crucial de définir des niveaux d'accès appropriés, de vérifier constamment les droits des utilisateurs et d'utiliser des mécanismes robustes pour protéger les ressources sensibles. Par exemple, l'utilisation de politiques de gestion d'identités et d'accès (IAM) permet de mieux surveiller et restreindre l'accès aux informations critiques.

☞*Au fur et à mesure de ce livre, nous verrons ensemble comment fonctionnent ces vulnérabilités en détail.*

D. Politiques et procédures de sécurité

Pour protéger les systèmes d'information d'une organisation, les politiques et les procédures de sécurité sont des supports importants sur lesquels toute leur sécurité est basée. Ces politiques doivent être bien définies et acceptées par tous les membres de l'organisation afin de garantir la sécurité desdits systèmes. Cette section a pour but de vous donner les grandes étapes pour élaborer ces politiques et ainsi comprendre comment elles sont utiles.

1. Élaboration des politiques de sécurité

L'élaboration des politiques de sécurité est un processus stratégique qui définit les **règles** et **responsabilités** en matière de sécurité au sein d'une organisation. Ces politiques servent de guide pour les employés et les partenaires, leur indiquant comment protéger les ressources de l'entreprise.

☞*Ces politiques sont d'ailleurs essentielles pour que l'entreprise puisse être certifiée ISO/IEC27001.*

a. Identification des besoins

Le processus commence par l'identification des besoins de sécurité de l'organisation. Il faut effectuer une **analyse des risques** pour comprendre les vulnérabilités actuelles et potentielles. Cette analyse doit prendre en compte les actifs de l'organisation, la nature des menaces possibles et les conséquences d'une compromission. Une fois ces éléments évalués, ils permettent de **définir les priorités en matière de protection**.

b. Développement de la politique

Ensuite, une équipe dédiée, impliquant souvent des experts en **cybersécurité**, rédige la politique de sécurité. Celle-ci doit inclure des directives claires concernant l'utilisation des ressources informatiques, la gestion des mots de passe, le traitement des données sensibles et la réponse aux incidents. Les responsables de la création de la politique doivent garantir qu'elle est compatible avec les exigences réglementaires et légales. Une attention particulière doit être accordée à la clarté et à l'applicabilité des directives pour s'assurer qu'elles peuvent être suivies avec facilité.

c. Validation et communication

Une fois la politique rédigée, elle doit être validée par la direction et les parties prenantes clés. Cette validation est un **processus** critique pour s'assurer que la politique est alignée avec les objectifs de l'entreprise. Après approbation, la politique de sécurité doit être communiquée à tous les niveaux de l'organisation. Des sessions de formation peuvent être organisées pour s'assurer que chaque employé comprend et peut appliquer les politiques dans son travail quotidien.

2. Mise en œuvre des procédures de sécurité

Il est impératif que les procédures soient établies pour soutenir les politiques de sécurité établies. Les procédures fournissent des instructions détaillées sur la manière de réaliser les politiques en pratique, assurant ainsi leur efficacité.

a. Documentation et formation

Les procédures doivent être soigneusement documentées et intégrées dans les manuels de l'organisation pour être **facilement accessibles**. Ces documents incluent des instructions pas à pas sur l'exécution des tâches spécifiques de sécurité. Parallèlement, la formation des employés est essentielle pour garantir qu'ils sont compétents et capables d'exécuter ces procédures correctement. Les formations doivent être régulières et inclure des mises à jour sur les nouvelles menaces et les changements dans les politiques.

b. Surveillance et évaluation

Une fois mises en œuvre, les procédures de sécurité doivent être **constamment surveillées** et évaluées pour leur efficacité. Cela nécessite l'utilisation d'outils de surveillance pour observer et enregistrer l'activité du réseau, identifier les anomalies et générer des alertes en cas de menaces. De plus, des **audits de sécurité** réguliers doivent être effectués pour évaluer la conformité des procédures et identifier les domaines nécessitant des améliorations. Ce processus d'évaluation continue aide à améliorer les stratégies de sécurité et à s'adapter aux nouvelles menaces émergentes.

☞*Les entreprises font donc appel aux hackers éthiques à ce moment précis !*

c. Révision et mise à jour

Enfin, il faut revoir et mettre à jour régulièrement les politiques et procédures de sécurité. La révision doit être effectuée en fonction des résultats des évaluations, des nouvelles menaces identifiées, ou des changements dans l'organisation. Les mises à jour doivent être rapidement implémentées et communiquées à tous les membres de l'organisation, garantissant ainsi une protection continue contre un paysage des menaces en constante évolution.