Sécurité - CIA Triad

Difficulté : Débutant

Notions : Principes fondamentaux en cybersécurité.

I. Introduction

Lorsque l'on parle de cybersécurité, il est important d'en saisir les objectifs principaux.

Pour cela, il a été créé un acronyme mnémotechnique : la triade ***CIA***.

Il s'agit d'un modèle conceptuel où chaque lettre représente l'un des trois grands piliers de la cybersécurité :

- Confidentiality
- Integrity
- Availability

Soit en français : Confidentialité, Intégrité, Disponibilité.

Ces piliers sont d'une importance équivalente.

Source : Try Hack Me

Cela découle dune application des normes suivantes :

- ISO 27001
- NIST CSF
- ANSSI (PGSSI-S, RGS)

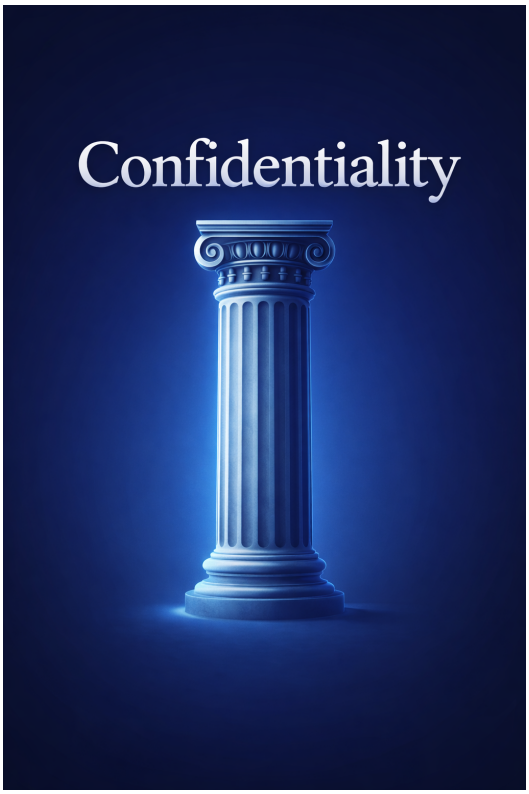
II. Confidentialité

Le premier principe est d'assurer la confidentialité des données.

Cette confidentialité assure que des données sensibles ne sont accessibles qu'aux personnes explicitement autorisées.

Si jamais cette confidentialité n'était pas maintenue, des personnes non autorisées, voire mal intentionnées, pourraient accéder à ces données et les exploiter. Ce qui entraînerait à minima une perte de confiance, voire des conséquences plus graves :

- Pertes financières
- Fuites de données personnelles
- Fuites de secrets industriels
- Poursuites judiciaires



Quelques exemples de perte de confidentialité de l'information :

- *Un employé partage son mot de passe à un collègue, celui-ci est entendu par une personne mal intentionnée qui accède ensuite au poste et vole des données confidentielles et personnelles. Elle pourra plus tard la faire chanter ou réutiliser contre elle ces informations.*
- *Des données sensibles concernant des secrets de fabrication pour un client ont fuité depuis une sauvegarde mal sécurisée. Cela entraîne des poursuites de la part du client mécontent que ses Propriété Intellectuelles aient été compromises.*
- *Les fiches de paye des salariés ont été rendues publiquement accessibles sur internet. Cela a entraîné des conflits internes et des mouvements de grèves qui ont déstabilisé le fonctionnement de l'entreprise.*

III. Intégrité

Le second principe est d'assurer l'intégrité des données.

Cette intégrité assure que les données n'ont pas été altérées. Que la confiance que l'on peut leur accorer reste pleine et entière.

Mais également que celles-ci sont précises et fiables.

Si jamais cette intégrité n'était pas maintenue, altérée par des personnes malveillantes, les données ne pourraient plus être considérées comme fiables.

Dans le meilleur des cas, ces données pourraient être relevées et corrigées, n'entraînant qu'une perte de temps.

Dans des cas plus extrêmes, ces données altérées pourraient entraîner des conséquences plus graves :

- Communications erronées
- Prise de décision basées sur de fausses données
- Dommages collatéraux
- Perte de confiance
- Poursuites judiciaires

Quelques exemples de perte d'intégrité de l'information :

- *Des logs systèmes ont été modifiés pour effacer les traces d'une activité.*
- *Un rapport financier à été altéré, poussant le conseil d'administration à prendre de mauvaises décisions.*
- *Des enregistrements de base de données contenant les mélanges des préparations ont été modifiés, conduisant à une production de produits inexploitables voire dangereux.*

IV. Disponibilité

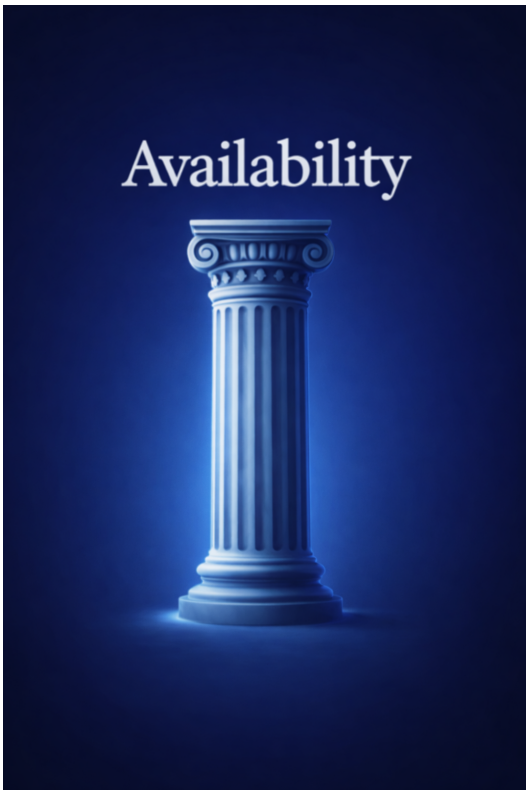
Le troisième principe est d'assurer la disponibilité des données et des services.

La disponibilité vise à assurer que les utilisateurs de la donnée ou du service puissent y accéder ***où*** ils en ont besoin et ***quand*** ils en ont besoin.

En fonction du secteur d'activité de l'entreprise, il peut même s'agir de l'élément fondamental qui en permet le fonctionnement.

Par exemple les secteurs bancaire ou hospitalier. Dans ces deux cas, une perte de service, même momentanée, pourrait avoir des conséquences dramatiques. Comme par exemple :

- Perte de production.
- Destruction de stocks.
- Pertes de vies humaines.
- Perte de confiance
- Poursuites judiciaires



Quelques exemples de perte de disponibilité des données :

- *Le cœur de réseau est tombé en panne, privant les utilisateurs de l'intégralité des services informatiques.*
- *Suite à une attaque par déni de service, les services de suivi de commandes ne sont plus disponibles.*
- *Une mise à jour a été effectuée sur un serveur de production, celle-ci a fait redémarrer le service.*

V. Conclusion

La triade **Confidentialité – Intégrité – Disponibilité** constitue le socle fondamental de toute démarche de sécurité informatique. Elle permet d’évaluer, structurer et prioriser les protections nécessaires pour garantir que les données restent accessibles aux bonnes personnes, exactes, et disponibles lorsque les utilisateurs en ont besoin.

Comprendre ces trois piliers, leurs risques et leurs interactions est essentiel pour analyser un système d’information, identifier ses vulnérabilités et mettre en place des mesures adaptées.

Dans les cours et les environnements professionnels, la triade CIA sert de référence pour aborder les normes, les bonnes pratiques et les stratégies de défense qui composent la cybersécurité moderne.

Voici un tableau récapitulatif qui résume les piliers, leurs objectifs et les risques auxquels ils permettent de faire face.

Pilier	Objectif	Risques
Confidentialité	Protéger les accès, gérer les permissions.	Fuite, espionnage, vol de donnée.
Intégrité	Garantir l'exactitude des données.	Altération, fraude.
Disponibilité	Assurer l'accès aux données.	Pannes, DDoS.

Revision #2
Created 2026-07-17 20:41:31 UTC by Olivier
Updated 2026-07-17 20:44:40 UTC by Olivier