**II. Cadre Théorique : Sécurité des Infrastructures Numériques : Concepts Fondamentaux et Mise en Œuvre Pratique**

La sécurité des infrastructures numériques est un enjeu complexe qui exige une approche structurée et globale. Pour garantir une protection efficace, il est essentiel de s'appuyer sur des concepts fondamentaux de la sécurité et de les traduire en mesures concrètes. Cette partie théorique explore ces concepts clés, en mettant l'accent sur leur application pratique à travers le monitoring de sécurité, le contrôle d'accès réseau et l'optimisation des ressources, en complément de la partie I dédiée au monitoring.

**II.1 Concepts Fondamentaux de la Sécurité : La Triade CIA et le Modèle AAA au Service de la Protection**

Avant d'aborder les aspects pratiques, il est crucial de rappeler les principes fondamentaux qui sous-tendent toute démarche de sécurité informatique. Deux modèles conceptuels sont particulièrement pertinents : la Triade CIA et le modèle AAA.

**II.1.1 La Triade CIA : Confidentialité, Intégrité, Disponibilité – Les Objectifs Essentiels**

La **Triade CIA** définit les trois piliers fondamentaux de la sécurité de l'information :

* **Confidentialité :** Assurer que l'information est accessible **uniquement aux personnes autorisées**. Ce principe est crucial pour protéger les données sensibles contre la divulgation non autorisée. Des mécanismes comme le chiffrement et le contrôle d'accès contribuent à garantir la confidentialité.
* **Intégrité :** Garantir que l'information est **exacte, complète et non altérée** tout au long de son cycle de vie. L'intégrité protège contre la modification ou la suppression non autorisée des données. Les signatures numériques et les contrôles d'intégrité sont des exemples de mesures visant à préserver l'intégrité.
* **Disponibilité :** Assurer que les systèmes et les informations sont **accessibles et opérationnels** pour les utilisateurs autorisés **quand ils en ont besoin**. La disponibilité est essentielle pour garantir la continuité des services. La redondance et les plans de reprise d'activité sont des mesures clés pour assurer la disponibilité.

La Triade CIA constitue le cadre de référence pour définir les objectifs de sécurité et évaluer l'efficacité des mesures mises en place.

**II.1.2 Le Modèle AAA : Authentification, Autorisation, Auditabilité – La Gestion des Accès et des Actions**

Le **modèle AAA** décrit les fonctions clés pour une gestion sécurisée des accès et des actions au sein d'un système d'information :

* **Authentification :** **Vérifier l'identité** d'un utilisateur ou d'un système avant de lui accorder l'accès. L'authentification garantit que l'entité est bien celle qu'elle prétend être. Les mots de passe, l'authentification multi-facteurs et les certificats numériques sont des méthodes d'authentification.
* **Autorisation :** **Déterminer ce qu'un utilisateur authentifié est autorisé à faire**. L'autorisation définit les droits d'accès et les permissions en fonction du rôle et des besoins. Le principe du moindre privilège est essentiel pour une autorisation efficace.
* **Auditabilité :** **Tracer et enregistrer les actions** réalisées par les utilisateurs et les systèmes. L'auditabilité permet de conserver une preuve des activités, de détecter les anomalies et de faciliter les investigations en cas d'incident. La journalisation et les systèmes d'audit sont des mécanismes d'auditabilité.

Le modèle AAA est fondamental pour mettre en place une gestion des accès sécurisée et garantir la traçabilité des opérations.

**II.2 Mise en Œuvre Pratique : Monitoring, Contrôle d'Accès Réseau et Optimisation des Ressources au Service de la Sécurité**

Ces concepts fondamentaux de la sécurité trouvent une application concrète à travers divers mécanismes et outils. Dans le cadre de cette étude, nous nous concentrerons sur trois aspects essentiels, complémentaires à la partie I sur le monitoring général : le monitoring *de sécurité*, le contrôle d'accès réseau et l'optimisation des ressources.

**II.2.1 Monitoring de Sécurité : Traduire la Visibilité en Action Sécuritaire**

Le **monitoring de sécurité**, en complément du monitoring général abordé dans la partie I, se concentre spécifiquement sur les aspects liés à la sécurité. Il vise à **appliquer concrètement les principes de la Triade CIA et du modèle AAA** en :

* **Assurant la Confidentialité par la Détection des Fuites Potentielles :** Le monitoring de sécurité peut détecter des tentatives d'accès non autorisés à des informations sensibles, des transferts de données suspects ou des comportements anormaux qui pourraient indiquer une violation de la confidentialité.
* **Garantissant l'Intégrité par la Surveillance des Altérations :** Le monitoring de sécurité peut identifier des modifications suspectes de fichiers ou de configurations, des tentatives de sabotage ou des anomalies qui pourraient compromettre l'intégrité des données et des systèmes.
* **Maintenant la Disponibilité par la Détection des Menaces et des Pannes :** Le monitoring de sécurité permet de détecter les attaques par déni de service (DoS), les pannes de systèmes ou les problèmes de performance qui pourraient affecter la disponibilité des services et des ressources.
* **Renforçant l'Auditabilité par l'Enregistrement des Evénements de Sécurité :** Le monitoring de sécurité collecte et archive les logs de sécurité, fournissant une **preuve** des événements et facilitant les audits et les investigations en cas d'incident, conformément au principe d'auditabilité du modèle AAA.

Ainsi, le monitoring de sécurité n'est pas seulement un outil de supervision technique, mais un **élément actif de la stratégie de sécurité**, permettant de traduire la visibilité sur l'infrastructure en actions concrètes pour protéger la confidentialité, l'intégrité et la disponibilité, et pour assurer l'auditabilité.

**II.2.2 Contrôle d'Accès Réseau : Appliquer l'Authentification et l'Autorisation au Périmètre du Réseau**

Le **contrôle d'accès réseau**, notamment à travers des mécanismes comme le portail captif, met en œuvre les principes d'**authentification et d'autorisation** du modèle AAA au niveau de l'accès au réseau. Il permet de :

* **Appliquer l'Authentification à l'Entrée du Réseau :** Le portail captif exige une **authentification** avant d'accorder l'accès au réseau, vérifiant l'identité des utilisateurs conformément au premier pilier du modèle AAA. Cela permet de contrôler qui accède au réseau et de limiter les accès non autorisés.
* **Mettre en Œuvre l'Autorisation par Politiques d'Accès :** Le portail captif permet de définir et d'appliquer des **politiques d'autorisation** spécifiques, par exemple en limitant l'accès à certains services ou en imposant des conditions d'utilisation, en accord avec le principe d'autorisation du modèle AAA. Cela permet de contrôler ce que les utilisateurs authentifiés sont autorisés à faire sur le réseau.
* **Renforcer la Confidentialité et l'Intégrité par un Accès Contrôlé :** En contrôlant l'accès au réseau, le portail captif contribue indirectement à la **confidentialité** et à l'**intégrité** des informations, en limitant les risques d'accès non autorisés et de compromission des données.

Le contrôle d'accès réseau, via le portail captif, est donc une application pratique des principes d'authentification et d'autorisation, permettant de sécuriser le périmètre du réseau et de contrôler les accès utilisateurs.

**II.2.3 Optimisation des Ressources Réseau : Contribuer Indirectement à la Disponibilité et à la Sécurité Globale**

L'**optimisation des ressources réseau**, et notamment la gestion de la bande passante, contribue indirectement à la sécurité, en particulier à la **disponibilité** et à la **résilience** des systèmes. En effet :

* **Améliorer la Disponibilité par la Priorisation du Trafic Critique :** La gestion de la bande passante permet de **prioriser le trafic** lié aux applications et services critiques pour la sécurité (outils de monitoring, systèmes de sécurité, communications d'urgence), garantissant leur disponibilité même en cas de congestion réseau, et contribuant ainsi au principe de disponibilité de la Triade CIA.
* **Renforcer la Résilience Face aux Attaques par Déni de Service :** Les mécanismes de limitation de débit et de gestion de la congestion peuvent aider à **atténuer l'impact des attaques DoS**, en préservant la disponibilité des services légitimes et en limitant la propagation des attaques.
* **Optimiser l'Utilisation des Ressources pour une Sécurité Plus Efficace :** Une gestion optimisée des ressources réseau permet de **garantir que les outils de sécurité disposent des ressources nécessaires** pour fonctionner efficacement (bande passante, latence), contribuant indirectement à l'efficacité globale de la sécurité.

Bien que la gestion de la bande passante ne soit pas une mesure de sécurité directe, elle apporte un **soutien indirect à la sécurité**, en particulier en termes de disponibilité et de résilience, en optimisant l'utilisation des ressources réseau.

**II.3 Conclusion du Cadre Théorique : Vers une Sécurité Intégrée et Proactive**

Ce cadre théorique a permis de poser les bases conceptuelles de la sécurité informatique, en rappelant les principes fondamentaux de la Triade CIA et du modèle AAA. Il a ensuite exploré comment ces principes se traduisent concrètement dans la mise en œuvre du monitoring de sécurité, du contrôle d'accès réseau et de l'optimisation des ressources, en complément de la partie I sur le monitoring général. Ces mécanismes, lorsqu'ils sont mis en œuvre de manière coordonnée, contribuent à construire une infrastructure numérique plus **sécurisée, résiliente et performante**, permettant de faire face aux défis de la sécurité à l'ère numérique de manière **intégrée et proactive**.