Politique de sécurité et Cryptographie

I. Politiques de sécurité : Elaboration et mise en œuvre de politiques de sécurité, gestion des mots de passe, contrôle d'accès

Il s'agit de définir des règles et des procédures pour protéger les systèmes informatiques contre les menaces. Cela inclut la gestion des mots de passe (choisir des mots de passe forts et les renouveler régulièrement) et le contrôle d'accès (limiter l'accès aux ressources sensibles aux seules personnes autorisées).

1. Elaboration et mise en œuvre de politiques de sécurité

Une **politique de sécurité** établit des règles pour protéger les personnes, les biens et les informations contre les menaces. Elle définit les responsabilités de chacun, les comportements acceptables, ainsi que les procédures à suivre en cas de violation. Son objectif est de réduire les risques d'accès non autorisé et de protéger contre les attaques, la perte de données, le vol et la fraude.

2. En quoi consiste la mise en œuvre des politiques de sécurité ?

Elles consistent à :

- **Comprendre les risques et identifier les vulnérabilités :** Les organisations doivent **évaluer les risques** en analysant leur environnement, leurs actifs et les menaces potentielles pour identifier les vulnérabilités exploitables. Cette analyse permet de déterminer les mesures à prendre pour atténuer les risques. Elles doivent aussi considérer les conséquences d'une violation de sécurité, notamment les pertes financières, l'atteinte à la réputation, la perturbation des services et les implications juridiques.
- **Culture de sécurité :** est essentielle pour un environnement sûr. Elle repose sur des règles claires, la formation des employés aux bonnes pratiques et la mise à disposition des ressources nécessaires. Elle inclut aussi la sensibilisation à la sécurité, la réalisation d'audits et la mise en place de contrôles efficaces.
- **Assurer la sécurité des biens et des personnes :** Les organisations doivent **identifier et traiter les risques** pouvant entraîner des blessures ou des dommages. Un audit permet d'évaluer l'environnement et détecter les dangers potentiels. Après cette analyse, elles hiérarchisent les

risques selon leur impact, garantissant un traitement prioritaire des plus critiques et une allocation efficace des ressources.

- **Elaboration d'une politique de sécurité globale** : Une **politique de sécurité globale** doit couvrir tous les aspects de la protection : physique, réseau, données et personnel. Elle doit aussi prévoir des procédures de réponse aux incidents et de mise en œuvre des contrôles pour garantir une défense efficace contre les menaces.
    - **Mots de passes** : Définir des règles strictes sur la création, la gestion et le renouvellement des mots de passe pour garantir leur sécurité.
    - **Contrôle d'accès** : Établir des principes de gestion des droits d'accès, en fonction des rôles et responsabilités des utilisateurs.
- **Etapes clés de la mise en œuvre d'une politique de sécurité** : La **mise en œuvre d'une politique de sécurité** passe par plusieurs étapes clés : révision de la politique existante, désignation d'une équipe dédiée, formation du personnel et mise en place des contrôles nécessaires. L'équipe de sécurité veille à l'application des règles et à la gestion des incidents en coordination avec l'ensemble de l'organisation.
    - **Mots de passes** : Utiliser des gestionnaires de mots de passe et imposer des critères de robustesse (longueur, complexité, expiration).
    - **Contrôle d'accès** : Mettre en œuvre l'authentification multi-facteurs et des systèmes limitant l'accès aux seules personnes autorisées.
- **Audits et surveillance de la sécurité** : Les organisations doivent effectuer **des audits de sécurité réguliers** pour vérifier le respect des politiques et l'efficacité des contrôles. Ces audits permettent d'identifier les failles et d'y remédier rapidement. En parallèle, des systèmes de surveillance doivent être mis en place pour détecter toute activité suspecte ou tentative de violation.
    - **Mots de passes** : Vérifier régulièrement l'application des règles de sécurité et repérer les faiblesses éventuelles.
    - **Contrôle d'accès** : Surveiller les connexions suspectes et auditer les accès aux ressources sensibles.
- **Formation et sensibilisation** : La **formation et la sensibilisation** assurent que tous les membres de l'organisation comprennent et appliquent les règles de sécurité. Cela passe par des sessions de formation sur les procédures, des campagnes de sensibilisation et éventuellement des incitations pour encourager le respect des bonnes pratiques.
    - **Mots de passes** : Former les employés à l'importance des mots de passe sécurisés et aux risques liés au partage d'identifiants.

- **Contrôle d'accès** : Sensibiliser à la gestion des droits d'accès et aux bonnes pratiques pour éviter les failles humaines.

3. Conclusion

   La **mise en œuvre d'une politique de sécurité** est essentielle pour protéger une organisation contre les risques. Elle doit être complète et adaptée aux menaces identifiées. Chaque membre doit être informé de ses responsabilités et des procédures à suivre pour assurer une application efficace.

Source : Carinel

II. Cryptographie : Principes de base, chiffrement des données, certificats numériques et signatures électroniques

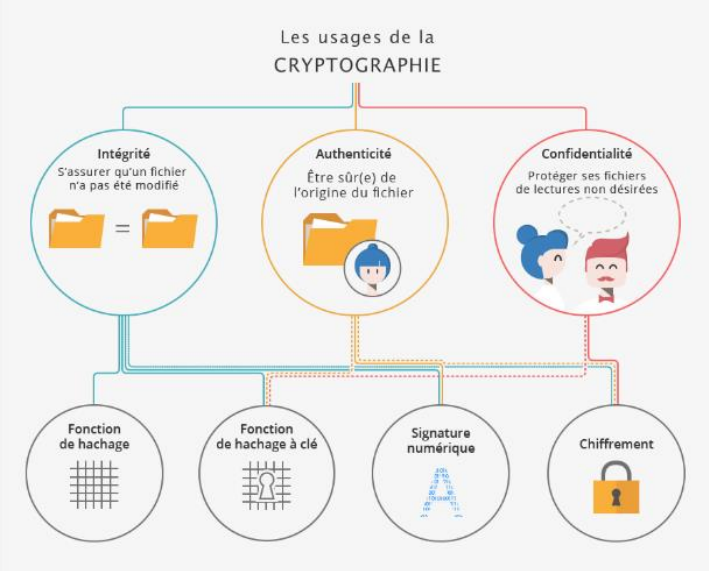
1. La cryptographie

La **cryptographie** est une discipline essentielle pour garantir la sécurité des données et des communications.

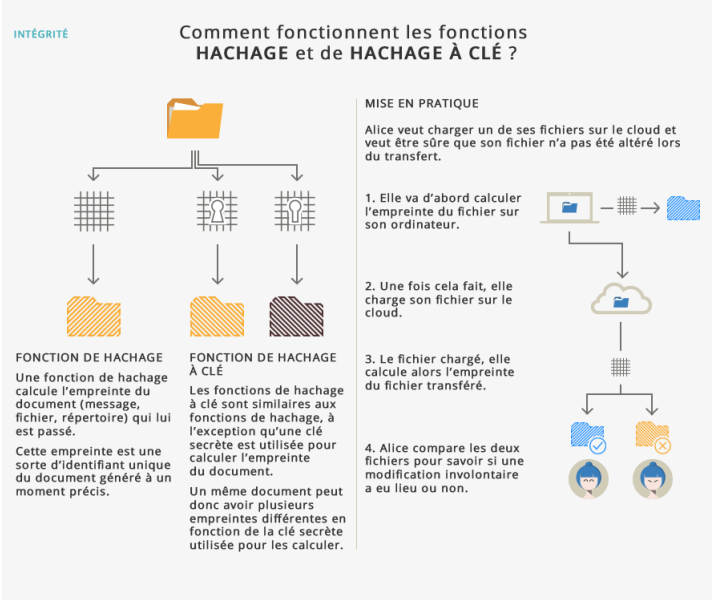
2. Ses principaux aspects

Voici ses principaux aspects :

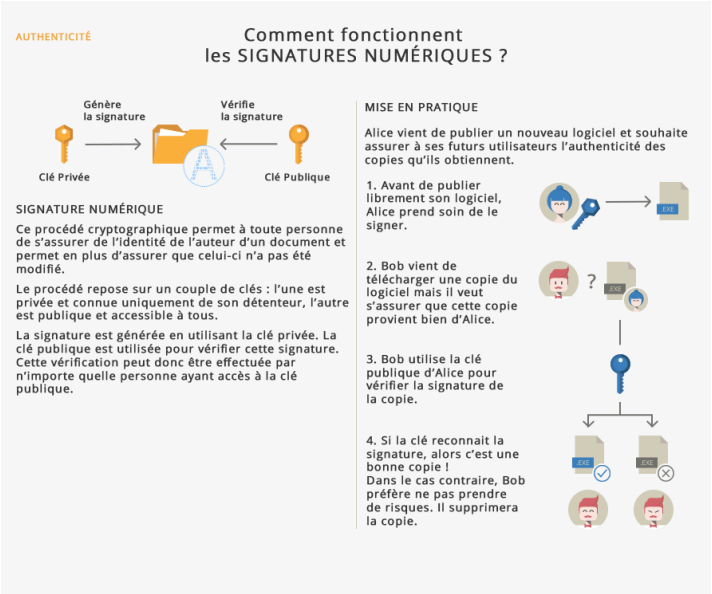
a) **Principes de base** : La cryptologie englobe la cryptographie (écriture secrète) et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie). Elle permet d'assurer la confidentialité, l'authenticité et l'intégrité des messages.



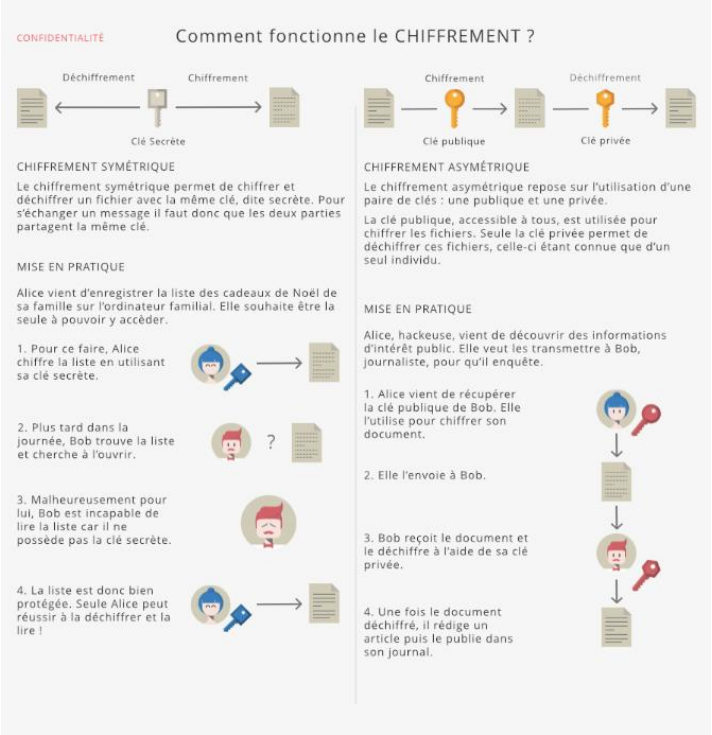
b) **Chiffrement des données** : Le chiffrement transforme un message en une forme illisible pour toute personne non autorisée. Il existe plusieurs types de chiffrement, comme le chiffrement symétrique (une seule clé) et asymétrique (deux clés : publique et privée).



c) **Certificats numériques** : Ils garantissent l'identité d'un utilisateur ou d'un site web en associant une clé publique à une entité vérifiée. Ils sont délivrés par des autorités de certification et permettent de sécuriser les échanges en ligne.



d) **Signatures électroniques** : Elles assurent l'authenticité et l'intégrité d'un document ou d'un message. Grâce à des algorithmes cryptographiques, elles permettent de prouver qu'un document n'a pas été altéré et qu'il provient bien de son auteur.



Source : CNIL

III. <u>Réponse aux incidents de sécurité : Stratégie de détection, de réponse et de récupération après l'incident</u>

1. Principe de base d'une réponse aux incidents de sécurité

La réponse aux incidents est une méthodologie structurée visant à **identifier, minimiser les dégâts et résoudre rapidement** les cyberattaques. Une gestion efficace réduit l'impact sur l'organisation, garantit la conformité et protège sa réputation.

2. Quelles sont les étapes clés ?

Les étapes clés sont :

- **Préparation** : Former une équipe dédiée, établir un plan clair et organiser des exercices réguliers.
- **Identification** : Détecter et analyser les incidents pour en évaluer la portée et les impacts.
- **Confinement** : Limiter la propagation en isolant les systèmes touchés et en bloquant les accès suspects.
- **Éradication** : Supprimer la cause de l'incident (élimination des logiciels malveillants, correction des failles).
- **Récupération** : Restaurer les systèmes affectés, vérifier leur bon fonctionnement et prévenir de nouvelles attaques.
- **Leçons apprises** : Examiner l'incident, ajuster les stratégies et renforcer la sensibilisation des équipes.

3. Quelles sont les défis ?

- **Manque de ressources** : Certaines organisations disposent de peu de moyens dédiés à la réponse aux incidents.
- **Formation insuffisante** : Les équipes doivent être formées régulièrement pour gérer des attaques complexes.
- **Faible sensibilisation des employés** : De nombreuses failles sont causées par des erreurs humaines (ex. mots de passe faibles, phishing).

4. Peut-on sécuriser les interactions web ?

Face à la croissance des cybermenaces, il est crucial de protéger les sites et applications contre les **robots, le spam et les abus**. Friendly Captcha propose une alternative sécurisée et respectueuse de la vie privée aux captchas traditionnels, utilisée par des entreprises, gouvernements et start-ups.

Source : Friendly Captcha

IV. Outils et logiciels à utiliser

1. Politique de sécurité

- ISO 27001 Toolkit : Aide à structurer une politique de sécurité conforme aux normes internationales.
- ANSSI Guides : L'ANSSI propose des recommandations pour renforcer la sécurité numérique.
- Splunk : Plateforme d'analyse et de surveillance des événements de sécurité.
- Microsoft Defender for Endpoint : Solution de protection avancée contre les menaces.

2. Cryptographie

- OpenSSL : Outil open source pour le chiffrement et la gestion des certificats numériques.
- GnuPG (GPG) : Logiciel de chiffrement pour sécuriser les communications et les fichiers.
- BitLocker : Solution de chiffrement intégrée à Windows pour protéger les données.
- Progress MOVEit : Logiciel de transfert sécurisé de fichiers.
- CertMgr.exe : Outil Microsoft pour gérer les certificats numériques.
- VeraCrypt : Gratuit, compatible avec Windows, Linux et Mac, offre de nombreuses méthodes de chiffrement et peut chiffrer les partitions système
- ProxyCrypt : soit GitHub ou soit un autre site comme MDN Web Docs. Gratuit, offre une grande liberté dans la mise en place du chiffrement et protège contre les enregistreurs de frappe ou Keyloggers, mais demande des connaissances d'administration et est uniquement pour Windows.
- Folder Lock : Très facile à utiliser, peut chiffrer des partitions, mais est limité à Windows et ne permet pas de cacher les fichiers ou de chiffrer des partitions système.
- AxCrypt : Gratuit et Open Source, s'intègre directement à l'explorateur de fichiers de Windows, simplifie les opérations de chiffrement et de déchiffrement