Aspects organisationnels et légaux de la Cybersécurité
Introduction

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les réseaux, les applications et les données contre les attaques malveillantes, le vol, l'intrusion, les erreurs de conception et de programmation, etc.…

Elle peut être divisée en plusieurs catégories, dont les principales sont les suivantes :

Schématiquement, un réseau d'entreprise fait intervenir plusieurs composants (routeurs, commutateurs, concentrateurs, pare-feux, etc...) qui assurent la communication et l'échange de données entre les différents acteurs à l'interne comme à l'externe.

La sécurité des réseaux

- Ce système est exposé à des **défaillances techniques** (pannes), des **intrusions** (hackers, logiciels malveillants…) ou tout simplement des **défauts de manipulation**. Or les données collectées, stockées et échangées au sein du réseau d'entreprise sont souvent confidentielles et/ou de nature personnelle.
- Sécuriser ce réseau revient donc à **optimiser l'état et le fonctionnement** de ses composants afin de se prémunir des attaques informatiques et des incidents liés à un mauvais usage.
- La sécurisation du réseau d'entreprise passe également par le **choix de bonnes solutions et technologies, et l'entretien régulier** de ces dernières.

Réseau en entreprise : panne informatique et erreur humaine coûtent cher

CNIL.

Sécurité : Protéger le réseau informatique interne

https://www.cnil.fr/fr/securite-proteger-le-reseau-informatique-interne

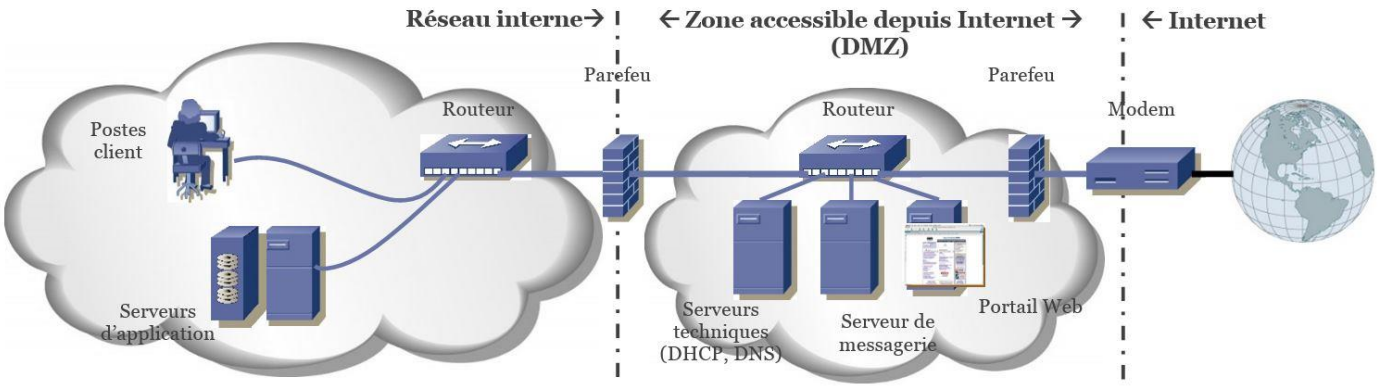


Figure 1: Exemple de mise en œuvre d'une DMZ

La gestion de la sécurité des applications consiste à DEVELOPPER, CORRIGER, AJOUTER et TESTER des fonctionnalités au sein des applications, afin de limiter principalement :

- **Les bogues** qui pourraient, par exemple, corrompre ou encore ouvrir l'accès aux données manipulées.
- **Les vulnérabilités** face à des menaces telles que les accès et les modifications non autorisés.

La sécurité des applications et des développements

Voici différents types de sécurité des applications : *authentification, autorisation, chiffrement, journalisation et tests permettant de détecter des bogues éventuels.*

Enfin, une politique de sécurité commence dès l'étape **d'analyse et conception**, bien avant l'écriture d'un programme.

CNIL.

Guide RGPD du développeur

Le guide RGPD du développeur offre une première approche des grands principes du RGPD et des différents points d'attention à prendre en compte dans le déploiement d'applications respectueuses de la vie privée des utilisateurs.

https://www.cnil.fr/fr/guide-rgpd-du-developpeur

...

Préparer son développement

Les principes de la protection des données personnelles doivent être intégrés aux développements informatiques dès les phases de conception afin de protéger la vie privée des personnes dont vous allez traiter les données, et de leur offrir ...

Sécuriser son environnement de développement

La sécurité des serveurs de production, de développement, d'intégration continue ainsi que les postes de travail des développeurs doit être une priorité car ils centralisent l'accès à un grand nombre de données.

Gérer son code source

Quelle que soit l'ampleur de votre projet, il est très fortement recommandé d'utiliser un outil de gestion de code source pour suivre dans le temps ses différentes versions.

Faire un choix éclairé de son architecture

Lors de la conception de l'architecture de votre application, vous devez identifier les données personnelles qui seront collectées et définir un parcours et un cycle de vie pour chacune d'entre elles. Le choix des supports de données (stockage ...

Sécuriser vos sites web, vos applications et vos serveurs

Tout site web, application ou serveur doit intégrer les règles élémentaires de sécurité à l'état de l'art, tant sur les communications que sur les authentifications ou son infrastructure.

Minimiser les données collectées

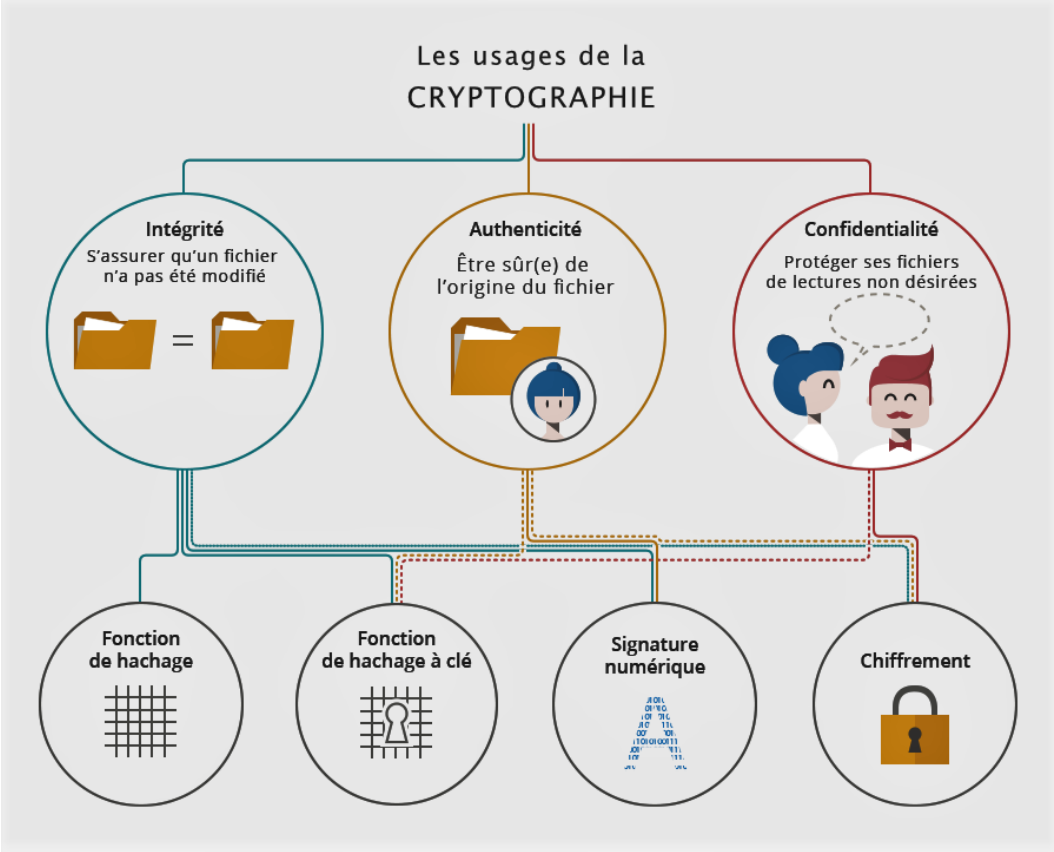
Vous ne devez collecter que les données personnelles qui sont adéquates, pertinentes et nécessaires au regard des finalités de votre traitement telles que définies au moment de la collecte.

...

La sécurité des données

La sécurité des données veille à garantir principalement l'intégrité, l'authenticité et la confidentialité des données, qu'elles soient stockées ou en transit.

- **L'intégrité** désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.
- **L'authenticité** qui permet de s'assurer de la provenance d'un message.
- **La confidentialité** est définie comme « le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé.



CNIL.

Guide de la sécurité des données personnelles

https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

« La protection des données personnelles nécessite de prendre des "mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque »

Sensibiliser les utilisateurs

Authentifier les utilisateurs

Gérer les habilitations

Tracer les accès et gérer les incidents

Sécuriser les postes de travail

Sécuriser l'informatique mobile

Protéger le réseau informatique interne

Sécuriser les serveurs

Sécuriser les sites web

Sauvegarder et prévoir la continuité d'activité

Archiver de manière sécurisée

Protéger les locaux

Etc…

La sécurité « opérationnelle » comprend les REGLEMENTS liés au TRAITEMENT et à la PROTECTION des données.

La sécurité opérationnelle

- **Depuis l'entrée en application du « Règlement Général de la Protection des Données » (ou « RGPD »)** le 25 mai 2018, toutes les entreprises européennes doivent être en conformité avec ce texte, et ce quelle que soit leur taille.
- **Le RGPD est applicable à un très grand nombre d'opérations de traitement de données a caractère personnel**, telles que : *la collecte, l'enregistrement, la consultation, l'utilisation, la diffusion, l'effacement ou encore la destruction.*

CNIL.

Adopter les six bons réflexes

https://www.cnil.fr/fr/adopter-les-six-bons-reflexes

1 NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES POUR ATTEINDRE VOTRE OBJECTIF

Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.
Le principe de finalité limite la manière dont vous pourrez utiliser ou réutiliser ces données dans le futur et évite la collecte de données « au cas où ».
Le principe de minimisation limite la collecte aux seules données strictement nécessaires à la réalisation de votre objectif.

2 SOYEZ TRANSPARENT

Les administrés doivent conserver la maîtrise des données qui les concernent. Cela suppose qu'ils soient clairement informés de l'utilisation qui sera faite de leurs données dès leur collecte. Les données ne peuvent en aucun cas être collectées à leur insu. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits.

3 ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES ADMINISTRÉS

Vous devez organiser des modalités permettant aux administrés d'exercer leurs droits et répondre dans les meilleurs délais à ces demandes de consultation ou d'accès, de rectification ou de suppression des données, voire d'opposition, sauf si le traitement répond à une obligation légale (par exemple, un administré ne peut s'opposer à figurer dans un fichier d'état civil). Ces droits doivent pouvoir s'exercer par voie électronique à partir d'une adresse dédiée.

4 FIXEZ DES DURÉES DE CONSERVATION

Vous ne pouvez pas conserver les données indéfiniment.
Elles ne sont conservées en « base active », c'est-à-dire la gestion courante, que le temps strictement nécessaire à la réalisation de l'objectif poursuivi.
Elles doivent être par la suite détruites, anonymisées ou archivées dans le respect des obligations légales applicables en matière de conservation des archives publiques.

5 SÉCURISEZ LES DONNÉES ET IDENTIFIEZ LES RISQUES

Vous devez prendre toutes les mesures utiles pour garantir la sécurité des données : sécurité physique ou sécurité informatique, sécurisation des locaux, armoires et postes de travail, gestion stricte des habilitations et droits d'accès informatiques.
Cela consiste aussi à s'assurer que seuls les tiers autorisés par des textes ont accès aux données.
Ces mesures sont adaptées en fonction de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.

6 INSCRIVEZ LA MISE EN CONFORMITÉ DANS UNE DÉMARCHE CONTINUE

La conformité n'est pas gravée dans le marbre et figée.
Elle dépend du bon respect au quotidien par les agents, à tous les niveaux, des principes et mesures mis en œuvre. Vérifiez régulièrement que les traitements n'ont pas évolué, que les procédures et les mesures de sécurité mises en place sont bien respectées et adaptez-les si besoin.