**REPUBLIC DU CAMEROUN REPUBLIC OF CAMEROON**

***Paix--Travail--Patrie Peace--Work--Fatherland***

**----------------** -----------------

UNIVERSITE DE DOUALA THE UNIVERSITY OF DOUALA

--------------- -----------------

**ECOLE NATIONALE SUPERIEURE NATIONAL HIGHER POLYTECHNIC**

**POLYTECHNIQUE DE DOUALA SCHOOL OF DOUALA**

---------------- -----------------

B.P : 2701 Douala P.O Box : 2701 Douala

Tel : (237) 697 542 240 Phone : (237) 697 542 240

**Site web :** [**www.enspd-udo.cm**](http://www.enspd-udo.cm) **Email : contact@enspd-udo.cm**

Une image contenant texte, Emblème, logo, symbole

Description générée automatiquementUne image contenant texte, Police, logo, Graphique

Description générée automatiquement

***Exposé* d’ARCHITECTURE DE CONFIANCE**

**THEME : PROTECTION DES SYSTEMES INFORMATIQUES**

***Option* : RESEAU ET SECURITE INFORMATIQUE (RSI5)**

**Rédigé par :**

**DJILLA DJIMEGNE GEORGES**

**MAHAMAT NOUR MAHAMAT TAHIR**

**NDJIEGOUE NGUELEU SERENA CHARY**

**RAKHIS SOULEYMANE DJAZOUM**

**SOUS LA SUPERVISION DE : Dr NOUMSI**

**Année académique 2024 - 2025**

SOMMAIRE

**Introduction ………………………………………………………………………..… 4**

**Stratégies et moyens de protection ………………………………………………..… 5**

**Sécurité physique …………………………………………………………..…….. 5**

**Sécurité des réseaux ………………………………………………………….….. 5**

* Filtrage réseau **………………………………………………….…. 5**
* Accès à distance **…………………………………………..………. 7**
* Outils réseaux **…………………………………………………….** **10**

**Sécurité des données ……………………………………………………….…… 13**

**Sécurité logicielle ……………………………………………………………...… 16**

* Mise à jour **……………………………………………………..… 16**
* Licences **………………………………………………………..… 16**

**Sécurité de stockage ………………………………………………………..…… 17**

* Sécurité physique ………………………………………………… **17**
* RAID 10 ………………………………………………………..… **17**
* Redondance **………………………………………….…………… 17**
* Cloud **……………………………………………………...……… 17**
* Sauvegarde **…………………………………………………..…… 18**

**Gestion des identités et des accès ………………………………………….…… 18**

* Identification **…………………………………………………...… 18**
* Authentification **……………………………………………….…. 21**
* Droits d’accès **……………………………………………….…… 24**
* Outils de gestion d’identité et d’accès **…………………………**

**Sécurité de l’administration …………………………………………………… 26**

1. Actions d’administration **………………………………………… 26**
2. Comptes d’administration **……………………………………..… 27**
3. Système d’information d’administration **………………………… 29**
4. Réseau d’administration **……………………………………….… 31**
5. Protocoles d’administration **……………………………..……… 32**
6. Outils d’administration **…………………………………….…… 32**

**Sensibilisation humaine ……………………………………………………..… 33**

* Sensibilisation **…………………………………………...……… 33**
* Formation **……………………………………….………….…… 34**

**Conformité et réglementation ………………………………………………… 34**

* Les normes de sécurité **…………………………………….…… 34**
* La législation en vigueur **…………………………………..…… 35**

**Mise en œuvre de la technique du cloisonnement …………………………… 35**

1. Cloisonnement du système **……………………………………… 35**
2. Cloisonnement physique **………………………………… 36**
3. Cloisonnement logique chiffré **………………………..… 36**
4. Cloisonnement logique simple **………………………..… 36**
5. Cloisonnement du réseau **……………………………………...… 37**
6. Cloisonnement physique **………………………………… 37**
7. Cloisonnement logique chiffré **………………………...… 37**
8. Cloisonnement logique simple **…………………………… 38**
9. Cloisonnement du stockage **……………………………………… 38**
   1. Cloisonnement physique **……………………………….… 38**
   2. Cloisonnement logique chiffré **…………………………… 39**
   3. Cloisonnement logique simple **…………………………… 39**

**Enjeux futurs et défis …………………………………………………………………… 40**

**Audit du système ………………………………………………………………………… 41**

**Conclusion ……………………………………………………………………….………. 43**

**Bibliographie/Webographie ………………………………………………….………… 44**

**Introduction**

La protection en cybersécurité désigne l’ensemble des mesures mises en place pour sécuriser les systèmes informatiques, les réseaux et les données contre les menaces et attaques malveillantes. Elle vise à garantir la confidentialité, l’intégrité et la disponibilité des informations et des infrastructures numériques.

Avec des dommages estimés à 10 500 milliards de dollars d’ici fin 2025, le domaine de la cybersécurité est devenu l’un de secteur le plus couteux. Pourtant, malgré ces chiffres alarmants, 68 % des organisations jugent leurs budgets de sécurité insuffisants face à des menaces désormais industrialisées. Alors que les systèmes d’information se complexifient (cloud hybride, IoT, IA), les menaces évoluent vers des attaques ciblées, automatisées et polymorphes. Dans un environnement réglementaire strict et face à des ressources limitées, **comment construire une sécurité des SI à la fois résiliente, adaptative et alignée avec les objectifs des entreprises** ? Comment concilier innovation technologique, contraintes opérationnelles et réponse à des adversaires toujours plus agiles ? Répondre à ces interrogations semble impossible pour certains mais pas pour nous. Bien que le risque zéro n'existe pas, nous pensons qu’avec la collaboration des utilisateurs d’un SI, il est possible de concevoir un SI hautement sécurisé. Ou améliorer considérablement la sécurité d’un SI existant.

Ainsi, tout au long de notre travail, nous allons proposer un guide complet pour la protection des SI. Que vous voulez construire votre SI ou que vous cherchez à améliorer votre SI existant, nous croyons fort que vous êtes au bon endroit : ce guide peut être appliquer à n’importe quel SI quelques soient sa taille et son importance.

1. **Stratégies et moyens de protection**
2. **Sécurité physique**

La sécurité des SI comment d’abord par la sécurité physique du site. Cela consiste à prendre des dispositions pour assurer la sécurité des personnels et des équipements, garantir la confidentialité des données et contrôler les accès aux salles stratégiques afin de contrecarrer les risques liés au vandalisme ou à l’incendie. Dans notre cas, nous recommandons les mesures suivantes :

* Délimiter le site avec un mur ou des grillages ;
* Mettre des vigiles aux entrées principaux ;
* Mise en place d’un dispositif de surveillance du site par des caméras ;
* Mise en place d’un dispositif de contrôle d’accès biométrique aux principales entrées et dans les salles ;
* Mise en place d’un système de contrôle d’accès par niveau ;
* Mise en place d’un dispositif anti incendie dans les locaux stratégiques comme la salle des serveurs ;

1. **Sécurité des réseaux**

La sécurité d’un réseau informatique peut être vue sous un angle avec 3 phase : la segmentation du réseau, le filtrage du réseau et la gestion des accès au réseau. Nous allons parler de la segmentation de façon détaillés dans la partie (Cloisonnement page 35). Nous évoquerons ici le filtrage du réseau et les accès au réseau notamment les accès à distances.

1. **Le filtrage réseau**

Le filtrage du réseau est une démarche visant à autoriser ou interdire des actions (flux) en fonction de règles préétablies ou construites automatiquement. L’objectif est de s’assurer que seuls sont autorisés les flux réseau nécessaires au bon fonctionnement du SI ou à sa sécurité, en filtrant ces flux. Pour mettre en œuvre le filtrage réseau, il est recommandé de suivre une démarche en 4 étapes :

* **Point de filtrage** : Le but ici est déterminer les points de filtrage. C’est-à-dire déterminer qui doit communiquer avec qui et comment cette communication doit se faire. En général, les interconnexions entre les systèmes et entre les sous-systèmes sont les points de filtrage principaux et les équipements d’extrémité sont donc des points de filtrage secondaires.
* **Besoin de filtrage** : Les flux réseau sont filtrés et autorisés relativement au ***besoin de fonctionnement*** du SI. Ce besoin tient compte des flux nécessaires au service métier rendu par le SI et de ceux nécessaires à sa sécurité. Le besoin de fonctionnement peut être exprimé en termes fonctionnels par les équipes responsables de la conception de chaque SI. Nous devons répertorier précisément les communications strictement nécessaires (ou ***besoin de fonctionnement***) entre le SI et les autres systèmes, et entre les sous-systèmes du SI, pour formaliser les besoins de filtrage.

**Les règles du filtrage**: Une fois les besoins de filtrage établis, il faut les décliner en une liste de règles techniques de filtrage, règles qui seront ensuite implémentées dans les dispositifs de filtrage. Nous devons établir et tenir à jour une liste des règles de filtrage en vigueur et des règles supprimées depuis moins d’un an. Cette liste constitue la matrice de flux globale. Cette liste doit préciser pour chaque règle :

* La date et le motif de la mise en œuvre, de la modification ou de la suppression de la règle ;
* Un historique daté des modifications de la règle ;
* Les modalités techniques de mise en œuvre de la règle, notamment le point de filtrage (le dispositif de filtrage) concerné ;
* Les critères techniques de filtrage réseau : adresses réseau, protocoles, numéros de ports, modes d’inspection, etc.

Le respect de ce formalisme permet de revoir plus facilement les règles lors des analyses a posteriori. En effet, pour que le filtrage soit efficace, il faut que sa formalisation soit maintenue dans le temps pour :

* Supprimer les règles devenues obsolètes ;
* Vérifier que tous les éléments attendus sont bien précisés et pertinents : raisons de Création, modification ou suppression des règles, éléments techniques ;
* Tracer les fusions et les optimisations de règles pour des raisons techniques ou de performance ;
* **Mise en œuvre du filtrage**: Après avoir formalisé les règles de filtrage, il faut les mettre en œuvre à l’aide de dispositifs techniques de filtrage, afin de n’autoriser effectivement que les flux nécessaires et d’interdire tous les autres. Les dispositifs incluant une fonction de filtrage peuvent être de natures différentes :
  + Pare-feu réseau ;
  + Pare-feu local d’un serveur ou d’un poste de travail ;
  + Liste de contrôle d’accès (***ACL***) sur un routeur ;
  + Serveur mandataire (***proxy***) effectuant une rupture de flux ;
  + Diode garantissant l’uni directionnalité d’un flux ;
  + Etc.

**NB :** Si toutes ces approches sont intéressantes, il est néanmoins fortement recommandé d’utiliser des dispositifs spécialement conçus pour effectuer une fonction de filtrage afin d’avoir l’assurance que ce filtrage est effectivement bien réalisé. Voici quelques recommandations à prendre en compte :

* + Il est recommandé de limiter le nombre de fonctions portées par ses pares-feux ;
  + Il est préférable de ne pas recourir à un routeur avec des listes de contrôles d’accès (ACL) pour remplir une fonction de filtrage. En effet, les ACL fonctionnent avec un mode « sans état » et ne peuvent donc pas servir à filtrer efficacement une session. Il est recommandé de choisir des pare-feux mettant en œuvre un suivi dynamique des sessions (pare-feux dits avec état ou *stateful*) et d’activer cette fonctionnalité ;
  + Il est recommandé de mettre en œuvre des mécanismes de filtrage reposant sur le principe des ***listes d’autorisation***, en décrivant spécifiquement ce qui est autorisé et en interdisant par défaut tous les autres flux ;

Les dispositifs de filtrage fonctionnent selon deux principes :

* ***Une liste d’autorisation*** (*allow list* ou encore liste blanche) : on décrit les flux qui sont spécifiquement autorisés et tous les autres sont strictement interdits ;
* ***Une liste d’interdiction*** (*deny list* ou encore liste noire) : on décrit les flux qui sont spécifiquement interdits et tous les autres sont autorisés par défaut ;

La liste d’autorisation a l’avantage d’être plus explicite dans ce qui est autorisé et donc de ne pas limiter les flux potentiellement malveillants à une liste prédéfinie. Ainsi, une attaque qui ne serait pas encore connue sera quand même bloquée. En revanche, cette approche demande de bien connaître son besoin de fonctionnement et de faire évoluer sa matrice de flux au fur et à mesure de l’évolution du besoin.

1. **Accès à distance**

De nombreux systèmes d’information sont accessibles à distance, pour répondre à divers cas d’usage :

* Service offert au grand public ou à des utilisateurs externes ;
* Service offert à des utilisateurs internes mais répartis sur plusieurs sites ;
* Nomadisme et *télétravail****;***
* Maintenance à distance ;
* Etc.

Maintenir le niveau de sécurité lorsque le SI est accédé à distance, depuis ou à travers des ressources non maîtrisées est une tâche importante. Les accès à distance sont associés à des cas d’usage différents, entre autres :

1. **Accès publics au SI :** Dans le cas des accès publics à un SI, l’accès se fait à partir et à travers des environnements (poste, site, réseau) que l’entreprise ne maîtrise pas et qu’il ne peut donc considérer comme étant de confiance. On rencontre ce cas pour des applications Web ouvertes au public ou à des utilisateurs connus mais externes. Les services hébergés sur des SI ouverts au public présentent la particularité d’être accessibles depuis des équipements dont le niveau de sécurité n’est pas maîtrisé par l’entreprise. Cependant, la politique d’accès au SI peut imposer des mesures concernant la sécurité des communications et l’authentification des utilisateurs, et enfin nécessiter de se protéger sans présupposer des caractéristiques des postes ou serveurs qui s’y connectent. Ainsi, la mise en œuvre de ***cloisonnement logique par le chiffre*** est limitée par l’absence de maîtrise du poste de l’utilisateur : l’entreprise r ne peut pas s’appuyer sur un logiciel client particulier pour imposer un tunnel IPsec ou ***TLS***. En revanche, il est possible de mettre en œuvre, à l’initiative du SI, du chiffrement applicatif (HTTPS par exemple) et l’authentification des utilisateurs.
2. **Accès nomades au SI :** Dans le cadre de ce travail, nous considérons l’utilisateur nomade comme un utilisateur légitime du SI ayant un poste de travail maîtrisé, mais accédant au SI depuis un site non maîtrisé et via un réseau non maîtrisé. L’utilisateur peut-être un employé ou un agent de l’entreprise, ou bien un prestataire mandaté par l’entreprise. Nous devons configurer le poste de travail nomade afin qu’il établisse toujours un tunnel authentifié et chiffré depuis le poste de travail jusqu’au SIE, ou à défaut, jusqu’au SI interne de l’entreprise. Il est recommandé de mettre en œuvre un tunnel reposant sur la technologie de ***VPN IPsec***, configuré conformément aux *recommandations de sécurité relatives à IPsec pour la protection des flux réseau*. Le tunnel doit couvrir l’ensemble des communications. Ainsi, l’utilisateur ne doit pas pouvoir désactiver temporairement le tunnel (pour se connecter au portail captif d’un hôtel par exemple), ni pouvoir accéder directement à Internet ou communiquer avec un équipement sur le réseau local (imprimante personnelle à domicile). Cependant, l’accès se fait toujours depuis un site non maîtrisé. Les mesures suivantes visent à mieux protéger le poste de l’utilisateur dans cette situation de nomadisme : renforcement de l’authentification, de la confidentialité et de l’intégrité des informations affichées ou stockées sur le poste.

* Nous devons nous assurer de l’identité de l’utilisateur nomade en l’obligeant à utiliser une ***authentification à double facteur*** sur le poste de travail. Lorsque des raisons techniques ou organisationnelles empêchent de mettre en place de l’authentification à double facteur pour les utilisateurs nomades, nous devons décrire ces raisons dans le dossier d’homologation du SI.
* Nous devons protéger la confidentialité et l’intégrité des mémoires de masse utilisées sur les postes de travail en les chiffrant intégralement (à la fois la partition système et les partitions de données).
* Il est fortement recommandé que l’entreprise fournisse aux utilisateurs en situation de nomadisme des filtres de confidentialité, afin de protéger la confidentialité des données relatives au SI.

1. **Accès internes au SI :** Les accès à distance dits « internes » couvrent les accès au SI depuis des équipements maîtrisés par l’entreprise (des postes de travail, des serveurs ou d’autres SI), localisés sur un site maîtrisé par l’entreprise, mais à travers un réseau qui n’est pas maîtrisé par l’entreprise. Ce cas couvre également un SI réparti sur plusieurs sites de l’entreprise. La présence d’un réseau non maîtrisé permettant d’accéder à un SI expose ce dernier à des accès illégitimes, et crée aussi un risque pour la confidentialité et l’intégrité des données échangées. Le vecteur d’attaque que constitue un réseau non maîtrisé doit donc être désactivé en mettant en œuvre un ***cloisonnement par le chiffre*** des communications réseau afin de se retrouver dans des conditions de sécurité équivalentes à celles d’un réseau maîtrisé par l’entreprise. Nous devons mettre en place un tunnel authentifié et chiffré dès lors qu’une communication liée au SI transite par un réseau non maîtrisé. Il est recommandé de mettre en œuvre un tunnel reposant sur la technologie de ***VPN IPsec***.
2. **Outils de protection réseau**

Plusieurs logiciels et matériels peuvent être utiliser pour accroitre la protection au sein d’un réseau. Nous pouvons citer :

1. **Pare-feu**

Un pare-feu (ou firewall en anglais) est un dispositif de sécurité réseau qui filtre le trafic entrant et sortant en fonction de règles prédéfinies. Son objectif est de protéger un réseau ou un système contre les accès non autorisés, les cyberattaques et les logiciels malveillants.

Les principales fonctionnalités d’un firewall sont les suivantes :

* **Filtrage du trafic** : Analyse les paquets de données (entrants et sortants) en fonction de règles de sécurité. Exemples de critères : adresse IP, port, protocole (TCP, UDP, etc.), type de trafic (HTTP, FTP, etc.) ;
* **Application des règles** : Autorise ou bloque le trafic en fonction des politiques de sécurité définies. Par exemple : Bloquer tout trafic entrant sur le port 22 (SSH) sauf pour une adresse IP spécifique ;
* **Journalisation** : Enregistre les activités du trafic pour analyse et audit ;
* **Protection contre les menaces** : Peut inclure des fonctionnalités avancées comme la détection d'intrusions, la prévention des attaques DDoS ou le filtrage de contenu ;

Aussi, il existe plusieurs types de firewall :

* **Pare-feu réseau (Network Firewall)** : Protège un réseau entier en filtrant le trafic entre différents segments réseau. Il est souvent utilisé entre un réseau interne et Internet ;
* **Pare-feu logiciel (Host-based Firewall)** : Installé sur un ordinateur ou un serveur pour protéger un système spécifique. Par exemple : Windows Defender Firewall ;
* **Pare-feu matériel (Hardware Firewall)** : Appareil dédié placé entre le réseau interne et Internet. Par exemple : Pare-feu Cisco ASA, Fortinet FortiGate ;
* **Pare-feu nouvelle génération (NGFW - Next-Generation Firewall)** : Combine les fonctionnalités d'un pare-feu traditionnel avec des technologies avancées comme :
  + - Filtrage applicatif (ex : bloquer Facebook) ;
    - Détection d'intrusions (IDS/IPS) ;
    - Analyse en temps réel des menaces ;
* **Pare-feu cloud (Cloud Firewall)** : Protège les applications et services hébergés dans le cloud. Par exemple : AWS WAF (Web Application Firewall);

1. **Logiciels antivirus**

Un **antivirus** est un logiciel conçu pour **détecter, prévenir et supprimer les programmes malveillants** (malware) sur un ordinateur ou un autre appareil. Il protège les systèmes contre les virus, les vers, les chevaux de Troie, les ransomwares, les logiciels espions et d'autres menaces. Il utilise sa base de données virale pour vérifier les signatures des fichiers et des programmes.

Les principales fonctionnalités d’un antivirus sont les suivantes :

* **Détection des menaces** : Identifie les logiciels malveillants en utilisant des **signatures** (bases de données de menaces connues) et des **techniques heuristiques** (détection de comportements suspects).
* **Analyse en temps réel** : Surveille en permanence les fichiers, les téléchargements, les emails et les activités du système pour détecter les menaces ;
* **Suppression des menaces** : Nettoie les fichiers infectés, met en quarantaine les menaces ou les supprime définitivement ;
* **Mises à jour automatiques** : Met à jour régulièrement la base de données des signatures pour détecter les nouvelles menaces ;
* **Protection supplémentaire** : Certains antivirus incluent des fonctionnalités comme :
  + Pare-feu intégré ;
  + Protection contre le phishing ;
  + Contrôle parental ;
  + Gestion des mots de passe ;

1. **IDS**

Un IDS (**Intrusion Detection System),** ou système de détection d'intrusion en français est une technologie utilisée pour surveiller et analyser le trafic réseau et/ou les activités système à la recherche de comportements suspects ou d'anomalies qui pourraient indiquer une tentative d'intrusion ou une attaque informatique. Il y a deux types d’IDS :

1. **IDS basés sur le réseau (NIDS)** : Surveille le trafic réseau pour détecter des activités suspectes ou malveillantes. Par exemple ***Snort*** ;
2. **IDS basés sur l'hôte (HIDS)** : Surveille les activités d'un seul système ou d'un ordinateur pour détecter des comportements anormaux. Par exemple ***OSSEC***;

Les principales fonctionnalités d’un IDS sont les suivantes :

* **Surveillance en temps réel** : Analyse en continu du trafic ou des activités système ;
* **Analyse des signatures** : Compare les activités observées avec une base de données de signatures connues de menaces ;
* **Détection des anomalies** : Identifie les écarts par rapport au comportement normal défini ;

1. **IPS**

Un **IPS** (Intrusion Prevention System, ou Système de Prévention des Intrusions en français) est un dispositif de sécurité réseau conçu pour détecter et bloquer les menaces en temps réel. Contrairement à un **IDS** (Intrusion Detection System), qui se contente de surveiller et d'alerter, un IPS agit activement pour empêcher les attaques avant qu'elles ne causent des dommages.

* **Surveillance réseau :** Analyse en temps réel les paquets de données qui traversent le réseau ;
* **Détection des menaces :** Utilise des signatures (modèles d'attaques connues) et des analyses comportementales pour identifier les activités suspectes. Exemples de menaces détectées : exploitations de vulnérabilités, attaques DDoS, malware, etc.
* **Action préventive :** Bloque automatiquement les paquets malveillants, ferme les connexions suspectes ou modifie les règles de pare-feu pour empêcher l'attaque ;
* **Journalisation et reporting :** Enregistre les incidents et génère des rapports pour analyse ultérieure ;

1. **SIEM** (**S**ecurity **I**nformation **and E**vent **M**anagement**)**

Un **SIEM** ou Gestion des Informations et des Événements de Sécurité, est une solution logicielle qui permet aux organisations de surveiller, détecter et répondre aux menaces de sécurité en temps réel. Il centralise et analyse les données de sécurité provenant de diverses sources pour identifier les activités suspectes ou malveillantes. Ses principales fonctionnalités sont les suivantes :

* **Collecte des données :** Agrège les logs et événements de sécurité provenant de multiples sources (pare-feu, antivirus, serveurs, applications, etc.) ;
* **Corrélation des évènements :** Analyse les données pour identifier des schémas ou des anomalies qui pourraient indiquer une attaque. Par exemple plusieurs tentatives de connexion échouées suivies d'une connexion réussie ;
* **Alertes en temps réel :** Notifie les équipes de sécurité en cas de détection d'activités suspectes ;
* **Analyse et investigation**: Fournit des outils pour investiguer les incidents (recherche dans les logs, visualisation des événements) ;
* **Conformité et reporting**: Génère des rapports pour démontrer la conformité aux réglementations (RGPD, PCI-DSS, ISO 27001) ;
* **Automatisation des réponses**: Intègre des actions automatisées pour répondre aux menaces (ex : bloquer une adresse IP, désactiver un compte utilisateur) ;

1. **Monitoring**

Le monitoring informatique ou [supervision informatique](https://www.nowteam.net/supervision-informatique/)est la surveillance permanente de votre système dans un but préventif. Il permet d’être alerté en cas de fonctionnements anormaux détectés sur votre système d’information. Le monitoring permet une surveillance de nombreux aspects de votre système informatique : le fonctionnement général, le débit, la sécurité, l’utilisation des ressources, le contrôle des flux etc.

1. **Sécurité des données**

La protection de données est une étape clé dans la réussite d’une entreprise. Pour cela, nous devons mettre une stratégie robuste et multicouches pour la protection de ces données. Il s’agit de :

1. **Evaluer les risques**

La toute première action que nous devons faire est l’évaluation des risques. Les objectifs sont les suivants :

* Identifier les données sensibles (informations clients, propriété intellectuelle, données financières, etc.) ;
* Analyser les menaces potentielles sur ces données (cyberattaques, fuites internes, pertes matérielles) ;
* Évaluer l'impact d'une violation de données sur l'entreprise ;

Une fois que nous avons ces informations, nous pouvons enfin se lancer dans l’élaboration des politiques de sécurité.

1. **Mise en place des politiques de sécurité**

Ces politiques doivent être en adéquation avec les menaces identifiées dans l’étape précédente. Elles vont servir des directives pour l’ensemble des utilisateurs du SI. Elles sont :

* Élaboration d’une politique de sécurité des données (accès, utilisation, stockage, partage) ;
* Sensibilisation des employés aux bonnes pratiques (mots de passe forts, vigilance face aux phishing) ;
* Imposition des règles strictes pour les appareils personnels utilisés au travail (BYOD) ;

1. **Sécuriser les accès**

En plus des mesures sur la gestion des accès, nous allons ajouter une mesure de plus au niveau des accès des employés :

* Utiliser l'authentification multi-facteur (MFA) pour renforcer la sécurité des comptes ;

1. **Chiffrement de données**

Chiffrer les données ne doit pas être une option pour les entreprises mais une obligation. Etant donné qu’il est impossible d’avoir une sécurité complète (100%), nous partons du principe les données peuvent tomber sur des mauvaises mains. Pour cela nous pouvons :

* Chiffrer les données sensibles, aussi bien en transit (emails, transferts) qu'au repos (stockage sur serveurs ou cloud) ;
* Utiliser des protocoles sécurisés comme HTTPS, SSL/TLS pour les communications ;

1. **Sauvegarder régulièrement les données**

L’un des objectifs fondamentaux de la sécurité est la disponibilité. Ainsi il faut toujours sauvegarder les données pour pouvoir les récupérer en cas de panne ou du crash du SI. Pour cela il faut :

* Mettre en place des sauvegardes automatiques et régulières en utilisant la règle de 3-2-1 (3 copies, 2 supports différents, 1 copie hors ligne) ;
* Stocker les sauvegardes dans des emplacements sécurisés et hors site ;
* Tester régulièrement la restauration des données pour s'assurer de leur intégrité ;

1. **Protéger le réseau et le système**

Nous devons mettre en place des mesures pour empêcher l’intrusion dans le réseau et dans le système. Pour cela nous pouvons :

* Installer des pares-feux et des logiciels antivirus ;
* Segmenter le réseau pour limiter la propagation des menaces (cette partie sera évoquée plus en détails dans *le cloisonnement du réseau)* ;
* Mettre à jour régulièrement les logiciels et systèmes d'exploitation pour corriger les vulnérabilités ;

1. **Surveiller et détecter les menaces**

La surveillance du réseau et du système est très importante. Elle permet d’être alerté en cas des menaces et de prendre de prendre les mesures adéquates de riposte. Ainsi nous pouvons :

* Utiliser des outils de surveillance pour détecter les activités suspectes ;
* Mettre en place un système de gestion des événements et des informations de sécurité (SIEM) ;
* Auditer régulièrement les systèmes pour identifier les failles ;

1. **Prévoir un plan de réponse aux incidents**

Une entreprise qui se respecte doit avoir un plan de riposte aux incidents. Ce plan doit contenir les mesures à appliquer pour contenir les menaces, des protocoles à utiliser et les acteurs à impliquer : Il s’agit de :

* Élaborer un plan d'action en cas de violation de données ;
* Former une équipe dédiée à la gestion des crises ;
* Tester régulièrement le plan pour s'assurer de son efficacité ;

1. **Respecter les règlementations**

Il est très important de respecter les normes et les lois en vigueurs. Les normes permettent d’avoir un système cohérent et les lois permettent d’éviter des potentielles poursuites judiciaires. Pour cela, nous devons :

* Se conformer aux lois locales et internationales sur la protection des données (la loi N°2024/017 sur la protection des données personnelles au Cameroun, RGPD en Europe, CCPA en Californie, etc.) ;
* Mettre en place des procédures pour répondre aux demandes des autorités ou des clients concernant leurs données ;

1. **Collaber avec des experts**

Une entreprise aussi grande soit elle, doit impérativement collaber avec d’autres experts pour avoir une protection accrue de son système. L’objectif est d’être ouverte et avertie aux autres solutions. Il peut s’agir de :

* Faire appel à des experts en cybersécurité pour des audits et des conseils ;
* Souscrire à des assurances cyber-risques pour limiter les impacts financiers en cas d'incident ;

1. **Sécurité logicielle**

Les logiciels peuvent être source d’intrusion dans le système. Nous pouvons scinder la sécurité des ces derniers en deux :

1. **Mise à jour**

Une mise à jour est une opération qui vise à corriger une ou plusieurs vulnérabilités découvertes sur un logiciel, un firmware ou même un matériel. Pour garantir la sécurité de notre système, nous devons surveiller constamment les fabricants et prendre acte le plus vite possible des mesures qu’ils publient. Ainsi, nous devons faire :

* + Les mises à jour importantes ou critiques corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement ;
  + Les mises à jour de version apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant ;

1. **Gestion des licences**

Les logiciels crackés sont souvent source de piratage. En effet, ces derniers peuvent contenir des portes dérobées (***backdoor)*** qui peuvent être utilisées par les attaquants pour transformer notre machine en un ***zombie.*** Pour éviter ce genre d’incident, il faut :

* Télécharger des logiciels gratuits uniquement à partir des sites officiels ;
* Faire analyser les logiciels avec des outils adaptés comme ***Checkmarx*** ou ***Veracode*** pour s’assurer de leurs fiabilités ;
* Interdire le téléchargement et l’utilisation des logiciels crackés ;
* Payer toujours les licences des logiciels qui sont payants uniquement à partir des sites fiables ;
* Renouveler constamment les licences (annuellement par exemple) ;

1. **Sécurité de stockage**

La sécurité du stockage vise en grande partie à assurer la disponibilité des ressources même en cas d’incident comme la panne d’un serveur ou un incendie. Pour cela, nous pouvons mettre en œuvre les mesures suivantes :

1. **Sécurité physique de la salle des serveurs**

La première mesure de sécurité est l’isolation de la salle des serveurs. Elle doit être dotée de :

* D’un dispositif de contrôle d’accès biométrique ou par badge ;
* D’un système anti incendie pour protéger les serveurs de la flamme ;

1. Utilisation des serveurs dotés de la technologie du RAID 10 ;

Le **RAID 10** (aussi appelé RAID 1+0) est un niveau de stockage combinant les avantages du **RAID 1** (mirroring/miroir) et du **RAID 0** (striping/entrelacement). Il offre à la fois redondance et performances accrues. Les avantages de cette technologie sont les suivantes :

* Haute disponibilité : Redondance grâce à la duplication des données ;
* Performances élevées : Débit amélioré par l’entrelacement ;
* Récupération simplifiée : En cas de panne d’un disque, il suffit de remplacer le disque défectueux et de resynchroniser la paire miroir ;

Bien le RAID 10 permet d’utiliser seulement 50% de la capacité initiale des disques, nous conseillons fortement sa mise en œuvre.

1. **Redondance des serveurs**

La redondance des serveurs est un moyen sur de récupération des données. Elle consiste à installer un ou plusieurs serveurs physiques ou virtuels et de dupliquer sur eux la fonction des serveurs principaux. Ainsi, en cas de dysfonctionnement du serveur principal, nous pouvons récupérer les données du système et relancer celui-ci par la suite.

1. **Stockage à distance**

La solution de stockage à distance (cloud) est la solution la plus sure pour la sauvegarde des données. Elle, avec le cloud, nous n’avons pas besoin de nous occuper à gérer les équipements et leur sécurité. Ni même les protocoles qui vont avec. Il nous faut seulement une connexion internet sécurisée et un poste de travail pour accéder à tout moment à nos données. Ainsi, il serait regrettable de n’est pas profiter de cette technologie. Il y a plusieurs types de cloud. Donc en tant qu’entreprise, nous devons choisir le cloud privé et exiger au fournisseur des mécanismes de sécurité plus accru.

Ainsi, nous recommandons d’héberger une partie des ressources non critiques de l’entreprise dans le cloud.

1. **Sauvegarde régulière**

Nous recommandons une sauvegarde de l’ensemble du système avec la règle de 3-2-1. Cette sauvegarde doit être régulière et périodique. Par exemple chaque soir à 23h. Elle doit se faire dans des serveurs physiques ou virtuels qui sont physiquement distincts. Ainsi, au cas où l’uns des serveurs de sauvegarde tombe en panne, nous pouvons toujours utiliser d’autres serveurs de sauvegarde pour accéder ou récupérer les données.

1. **Gestion des identités et des accès**

Cette section détaille les recommandations relatives à l’identification, à l’authentification et à la gestion des droits d’accès dans un SI. L’objectif ici est de pouvoir attribuer toute action effectuée sur un SI à un utilisateur ou à un processus automatique, en associant une identité à chaque personne ou processus, puis une identité à chaque action effectuée. On parle de la non-répudiation.

1. **Identification**

**L’identification** est une action d’un utilisateur ou d’un processus automatique consistant à communiquer une identité préalablement enregistrée dans le SI. **L’imputabilité** est la capacité d’attribuer une action de façon certaine à un utilisateur ou à un processus automatique.

1. **Utilisation de comptes individuels**

Voici un scenario qui nous permettra de bien comprendre l’importance de cette section.

**Scenario :** dans un SI, un compte nommé « Utilisateur » sert à se connecter à une application sensible. Ce compte est utilisé par quinze personnes qui appartiennent à la même équipe. À la suite d’un incident, une investigation amène à retrouver dans les journaux de l’application que le compte « Utilisateur » a effectué il y a quatre mois une action en lien avec l’incident. Il est cependant impossible de savoir exactement quelle personne de l’équipe a réalisé cette action. Cela laisse aussi le doute sur la possibilité qu’un attaquant utilise aussi le compte à l’insu de l’équipe.

Il est obligatoire d’attribuer un ***compte individuel*** à chaque utilisateur ou processus automatique qui accède au SI ou l’utilise. Un ***compte individuel*** correspond :

* Soit à un seul utilisateur (personne physique), identifiable par son nom ou par un identifiant unique ;
* Soit à un ***compte technique*** rattaché à un processus automatique (un programme, une application, un service, un script, etc.). Un ***compte technique*** ne doit pas pouvoir ouvrir une session interactive ;

Des cas particuliers peuvent imposer la création de comptes partagés. Cela empêche cependant la stricte imputabilité de chaque opération effectuée et est donc contraire à ce qui est exigé dans la recommandation. Par exemple :

* Les équipements n’offrant pas de mécanisme technique de gestion de comptes et n’utilisant qu’un seul compte, voire pas de compte du tout. Ils ne permettent donc pas de créer un compte pour chaque utilisateur ;
* Certaines activités nécessitent l’utilisation par plusieurs utilisateurs d’une session unique, simultanément ou séquentiellement, pour des raisons organisationnelles. Cela peut être le cas de personnes chargées d’accueil du public dans un bâtiment, de personnes entrant des données dans un laboratoire, etc.
* Les équipements qui doivent maintenir dans la durée une même session active (leurs activités sont interrompues par la fermeture de la session). Dans ce cas, les utilisateurs ne peuvent pas recourir à des sessions différentes, ouvertes avec leurs comptes individuels respectifs. C’est le cas sur des systèmes industriels dont le temps d’opération peut être plus long que la présence d’un utilisateur unique ;

Dans tous ces cas particuliers où l’imputabilité d’une action à un utilisateur unique n’est plus assurée par l’utilisation d’un compte individuel, nous devons mettre en place des mesures techniques ou organisationnelles permettant d’atteindre un niveau d’imputabilité équivalent. Ces mesures peuvent êtres :

* La limitation de la plage horaire pendant laquelle le compte peut ouvrir une session ;
* La limitation des équipements pouvant utiliser ces comptes ;
* La limitation de l’accès physique à ces équipements ;

Pour assurer la traçabilité de l’utilisation d’un compte partagé, il faut :

* Utiliser un cahier d’enregistrement décrivant précisément la date et l’heure de présence du personnel à un poste d’astreinte particulier ;
* Utiliser un bastion assurant la traçabilité entre une identité individuelle et le recours à un compte partagé ;
* Sur un système Unix, d’utiliser la commande ***sudo*** qui permet de savoir quel utilisateur a fait usage du compte root en consultant les journaux du système ;

La journalisation et la supervision des accès et des actions des comptes partagés contribuent à la détection des incidents de sécurité.

1. **Comptes inutilisés**

La protection des comptes des utilisateurs passe aussi par leur désactivation dès lors qu’ils ne sont plus utilisés. Il est impératif de désactiver sans délai les comptes individuels ou partagés qui ne sont plus nécessaires. Le scenario suivant nous prouve la nécessité.

**Scenario :** Un utilisateur ayant un compte actif sur le SI part à la retraite et son compte reste actif. Comme plus personne n’utilise ce compte, un attaquant a plus de temps pour découvrir son secret d’authentification et obtenir un accès à ce compte, et il a toute la liberté de l’utiliser sans être détecté par son détenteur légitime.

La désactivation d’un compte revient à la suspension globale des droits d’accès qui lui étaient attribués, voire à leur suppression. Cette désactivation doit être systématique pour tout compte qui n’a plus vocation à être utilisé. La simple désactivation d’un compte est parfois préférable à la suppression complète du compte, pour permettre de conserver la traçabilité des actions dans le temps, ou pour conserver des données liées au compte de l’utilisateur (clés de chiffrement, certificats, etc.). Dans ce cas, il est recommandé que de désactiver *complètement* le compte. Pour cela, nous pouvons appliquer des mesures techniques supplémentaires : modification du mot de passe par un nouveau mot de passe aléatoire, interdiction d’ouverture de session, suppression des droits et privilèges, déplacement dans une unité organisationnelle d’annuaire dédiée, etc.

La désactivation du compte peut aussi se faire en cas d’absence prolongée de la personne titulaire du compte : congé sabbatique, congé parental, congé maladie, etc. Le compte est alors réactivé au retour de son titulaire. Cette recommandation est aussi valable pour les comptes créés par défaut lors de l’installation d’un système et qui n’ont pas vocation à être utilisés ensuite. Enfin, cette recommandation s’applique également aux comptes inutilisés depuis un certain temps (par exemple un an).

1. **Revue de comptes**

Afin que ces recommandations soient efficaces, nous pouvons utiliser des outils d’audit automatiques en lien avec son annuaire. Nous devons aussi faire régulièrement des revues afin d’avoir une visibilité sur les comptes présents sur le SI. Il est recommandé de lier cette revue des comptes actifs avec une revue des droits d’accès.

1. **Authentification**

**L’authentification** est le processus ayant pour but de vérifier l’identité dont se réclame un utilisateur, un processus, une entité ou une machine. S’authentifier consiste à apporter la preuve de cette identité au moyen d’un ou plusieurs ***facteurs d’authentification***. L’authentification est donc précédée d’une ***identification***. L’objectif ici est de vérifier l’identité d’une personne physique ou d’un processus automatique avant de lui donner accès au SI.

1. **Secret d’authentification**

L’accès à une ressource d’un SI doit être conditionné à la connaissance ou à la possession d’un secret (mot de passe, code PIN, clé privée, etc.).

* **Sécurité du mécanisme d’authentification**

L’objectif est de mettre en œuvre un mécanisme d’authentification pour chaque compte. Pour cela nous devons protéger les accès aux ressources du SI, que ce soit par un utilisateur ou par un processus automatique, au moyen d’un mécanisme d’authentification impliquant au minimum un élément secret. Cette authentification peut être renforcée par l’emploi d’une ***authentification à double facteur*** s’appuyant sur plusieurs types de ***facteurs d’authentification***.

Le secret qui est utilisé dans le mécanisme d’authentification est un des moyens de s’assurer que l’utilisateur ou le processus automatique est bien celui qu’il prétend être : la compromission d’un secret peut conduire à ce qu’un attaquant utilise frauduleusement un compte. La confidentialité et l’intégrité des secrets doivent donc être particulièrement protégées. Pour ça nous devons définir et appliquer une politique de gestion des éléments secrets d’authentification, dont les mots de passe, en accord avec notre politique de sécurité du SI. Cette politique de gestion doit décrire les éléments secrets utilisés et les mécanismes de sécurité mis en œuvre pour les protéger. Par exemple, les mots de passe ne doivent pas être stockés en clair (en dehors des cas de séquestre dans un coffre-fort). Suivant les contextes, il est préconisé de ne stocker que des mots de passe chiffrés. L’utilisation d’algorithmes réversibles ou de simples empreintes sont à proscrire. Les mots de passe doivent être conformes à l’état de l’art (longueur du mot de passe et types de caractères) et de renouvellement, en tenant compte du niveau de complexité maximal permis par la ressource concernée.

* **Partage de secrets**

Si un élément secret d’authentification venait à être connu de personnes n’ayant pas ou plus le besoin de le connaître, alors l’élément ne peut plus être considéré comme étant secret. L’imputabilité n’est plus garantie. Nous pouvons appliquer les mesures suivantes pour assurer la confidentialité du secret :

* Interdiction du partage d’éléments secrets entre plusieurs utilisateurs ;
* Interdiction d’inscrire en clair un mot de passe sur un support accessible à d’autres personnes que celles qui ont besoin de connaître ce mot de passe ;

1. **Renforcement de l’authentification**

Certains cas nécessitent d’utiliser une authentification renforcée afin de s’assurer, avec un haut niveau de confiance, de l’identité de l’utilisateur.

**Compte privilégié :** Compte dont les droits d’accès permettent des actions qui ne sont pas autorisées à la majorité des utilisateurs de l’application ou du SI. C’est par exemple le cas d’un compte d’administrateur technique. Cela peut être aussi le cas d’un compte d’administrateur métier qui permet de définir les droits des autres utilisateurs dans une application. Il existe également des comptes de processus ou de service avec des privilèges élevés. Ces comptes sont des comptes privilégiés sans être des comptes d’administration.

Lorsque les éléments secrets d’authentification sont des mots de passe, les utilisateurs ne doivent pas les réutiliser entre plusieurs comptes, privilégiés ou non privilégiés. Il est fortement recommandé que le mot de passe d’un compte privilégié ne puisse pas être déduit d’un mot de passe d’un autre compte du même utilisateur. Certains utilisateurs, et notamment les administrateurs, peuvent être amenés à utiliser un nombre important de secrets, ce qui rend le respect des bonnes pratiques difficile à maintenir dans le temps. Le stockage des mots de passe dans un fichier, en clair ou avec un chiffrement faible, doit être proscrit. L’utilisation d’un coffre-fort de mots de passe est recommandée notamment dans ce cas.

1. **Renouvellement du secret**

Les secrets d’authentification ont une grande valeur pour les attaquants, qui disposent de nombreux outils pour automatiser la recherche de ces informations. Face à cette menace, il est imprudent de considérer qu’un secret d’authentification peut être utilisé indéfiniment. En effet :

* Au cours de l’exploitation d’un SI, de plus en plus de personnes sont amenées à s’y connecter et donc à connaître des secrets d’authentification ;
* Plus la période de renouvellement d’un secret est longue, plus un attaquant a de temps pour découvrir ce secret ;

Pour cela nous devons renouveler régulièrement les secrets d’authentification. La fréquence de renouvellement doit être choisie en accord avec la direction et doit répondre à l’objectif de protection des SI concernés.

Lorsque la ressource ne permet pas techniquement de modifier l’élément secret d’authentification, l’opérateur doit mettre en place des mesures techniques et organisationnelles permettant de réduire les risques associés à ce secret fixe. Ainsi, nous devons décrire les raisons, les mesures et leurs justifications dans le dossier d’homologation du SI. Ces mesures concernent en particulier le contrôle d’accès physique à la ressource concernée ou la traçabilité (horaire, durée, etc.) des accès, afin de rattacher indirectement une action à une personne. Il convient de compléter cette approche par une protection de la méthode de renouvellement du secret, afin que le nouveau secret employé ne soit pas directement à la disposition de l’attaquant.

Nous devons aussi nous assurer que seuls les utilisateurs qui en ont la responsabilité peuvent modifier les éléments secrets d’authentification et peuvent accéder, si nécessaire, à ces secrets en clair. La possibilité de modifier un élément d’authentification d’un compte ne doit être accessible qu’aux personnes ayant légitimement ce rôle, comme l’utilisateur du compte, un administrateur, ou une personne chargée du support utilisateur.

Lorsqu’un mot de passe est modifié par une autre personne que l’utilisateur lui-même, alors l’utilisateur doit à nouveau changer le mot de passe lors de sa première connexion.

En plus du renouvellement régulier, certains cas particuliers demandent une modification ponctuelle et parfois immédiate des secrets d’authentification, en particulier des mots de passe :

* Lorsque ce sont des éléments définis par défaut ;
* Lorsqu’il s’agit d’un compte partagé et qu’une personne connaissant ce secret partagé n’en a plus besoin ;
* Lors de la première authentification après attribution d’un mot de passe temporaire à un compte d’utilisateur ;
* Lorsqu’il y a une suspicion de compromission ou une compromission avérée ;

Lorsque les conditions de sécurité protégeant un secret d’authentification ne sont plus réunies, il est fortement recommandé de renouveler immédiatement ce secret.

1. **Droits d’accès**

L’objectif ici est de s’assurer que les utilisateurs ont uniquement accès aux ressources et aux fonctions qui leur sont légitimement nécessaires.

* **Attribution des droits d’accès**

Nous devons définir les règles de gestion et d’attribution des droits d’accès aux ressources du SI, conformément à sa politique de sécurité. Cette politique doit préciser formellement la façon dont les droits d’accès au SI sont attribués et maintenus dans le temps. Il s’agit de :

* Définition de rôles métier et de profils techniques standards ;
* Cycle de vie des droits : modalités d’attribution, de modification et de suppression de droits ;
* Outillage technique associé ;
* Modalités de contrôle ;
* Etc.

Il est recommandé de recourir à une méthodologie définissant des rôles et des profils (par exemple suivant la méthodologie ***RBAC***), pour que l’attribution de droits d’accès soit systématique et non redéfinie manuellement au cas par cas, ce qui est souvent source d’erreur. Dans un annuaire, les rôles et profils sont souvent représentés par des groupes de comptes.

Aussi, nous ne devons attribuer à un utilisateur ou à un processus automatique que les droits strictement nécessaires à l’exécution des actions dont l’utilité est avérée. Il est recommandé qu’aucun droit ne soit attribué par défaut à un utilisateur ou à un processus automatique : c’est le ***principe du moindre privilège.***

Le principe du moindre privilège implique de limiter le niveau de droits qu’on attribue sur une ressource, mais aussi de ne donner accès qu’aux fonctions de cette ressource qui sont nécessaires. Pour cela, nous devons déterminer quels sont les droits d’accès unitaires disponibles sur une ressource (système, application, etc.), puis déterminer comment ces droits unitaires sont attribués à un compte donné ou à un groupe de comptes.

Nous devons également établir et tenir à jour la liste des comptes privilégiés. Toute modification d’un compte privilégié (ajout, suppression, suspension ou modification des droits associés) doit faire l’objet d’un contrôle formel destiné à vérifier que les droits d’accès aux ressources et fonctionnalités sont attribués selon le principe du moindre privilège et en cohérence avec les besoins du compte. La liste des comptes privilégiés doit faire partie de la cartographie globale du SI. Elle doit préciser, pour chaque compte, le niveau et le périmètre des droits d’accès associés, ainsi que les types de comptes sur lesquels portent ces droits (comptes d’utilisateurs, comptes de messagerie, comptes de processus, etc.). Cette liste doit être à jour, ce qui implique que chaque modification concernant un compte privilégié doit être tracée et validée. Enfin, il est important que la gestion des comptes privilégiés soit systématiquement intégrée aux processus d’arrivée, de départ ou de gestion interne du personnel (mutations, congés, etc.).

Concernant le contrôle formel des modifications des comptes privilégiés, il est recommandé qu’il soit fait par deux personnes, l’une ayant les connaissances métier suffisantes pour s’assurer que l’utilisateur est bien légitime et l’autre connaissant bien le fonctionnement technique de la ressource concernée.

* **Revue des droits d’accès**

De nombreuses attaques sont facilitées par le fait que des droits d’accès qui ont été attribués à un utilisateur (ou à un administrateur) ne suivent pas forcément l’évolution de la situation de cet utilisateur dans le temps. Ainsi, des droits attribués peuvent ne plus correspondre au strict besoin de l’utilisateur quelques mois ou quelques années plus tard. Nous devons faire une revue régulière des droits d’accès attribués, au moins tous les ans. Cette revue est également une opportunité pour détecter des comptes à désactiver. Cette révision porte sur les liens entre les comptes, les droits d’accès associés et les ressources ou les fonctionnalités qui en font l’objet. Cette revue des droits d’accès attribués aux utilisateurs et aux processus automatiques permet de s’assurer de l’efficacité de la procédure d’attribution de droits dans le temps et de corriger les éventuelles erreurs. La revue de droits peut faire intervenir les responsables hiérarchiques. Ces derniers sont les plus à même de juger de l’appartenance d’un utilisateur ou d’un processus automatique à un groupe particulier, ou des droits associés à ce groupe.

Lorsque la solution de gestion de droits est complexe (annuaire d’entreprise comme Active Directory, progiciel de gestion intégré), certains privilèges donnent le droit d’en attribuer d’autres, ou de contrôler certaines ressources permettant d’en acquérir d’autres. Dans ce cas, une analyse des chemins de contrôle et des chemins d’élévation de privilèges est recommandée, en recourant si nécessaire à des outils spécialisés.

* **Quelques outils pour la gestion des identités et des accès**

Il existe plusieurs outils de gestion d’accès sur le marché. Le choix du bon l'outil dépend des besoins spécifiques de l'organisation, de son infrastructure existante et des exigences de conformité. Nous pouvons citer :

* **Microsoft Entra ID** : Anciennement connu sous le nom d'Azure Active Directory, il offre une gestion complète des identités pour les environnements cloud et hybrides ;
* **Okta** : Une solution cloud indépendante qui fournit des services d'authentification et de gestion des identités pour diverses applications ;
* **IBM Security Identity Governance and Intelligence** : Conçu pour les grandes entreprises, il combine l'authentification des utilisateurs, l'application des politiques et la gouvernance des identités ;

1. **Sécurité de l’administration**

Cette section couvre les règles relatives aux comptes d’administration et aux systèmes d’information d’administration. L’objectif est d’identifier les actions susceptibles d’altérer le fonctionnement ou la sécurité du SI pour en garantir une utilisation légitime.

1. **Actions d’administration**

On parle d’action d’administration toute action d’installation, de consultation, de modification ou de suppression d’un composant d’un SI susceptible de modifier le fonctionnement ou la sécurité de celui-ci. Par définition, les actions d’administration sont des vecteurs d’attaque importants sur un SI, puisqu’un attaquant peut les utiliser pour compromettre le fonctionnement ou la sécurité du SI. Nous devons donc identifier précisément ce que sont les actions d’administration avant de protéger les comptes et les ressources associés à ces actions. L’identification des ***actions d’administration*** applicables au SI est recommandée, pour ensuite protéger l’accès à ces actions. Quelques exemples non exhaustifs d’actions d’administration :

* Installation de microcodes, de systèmes d’exploitation, de logiciels ;
* Configuration de matériels et de logiciels, et en particulier ceux relatifs à la sécurité du SI ;
* Gestion des comptes, des privilèges et des droits d’accès, par exemple à travers un annuaire ;
* Maintenance et supervision, dès lors que ces actions nécessitent des privilèges de même niveau que pour effectuer les actions d’administration ;
* Programmation d’un automate industriel ;

Il est parfois pertinent de distinguer l’administration *technique* de l’administration *métier*. Cette dernière correspond à la gestion fine des droits au sein d’une application métier particulière (permissions des utilisateurs au sein de l’application). Le périmètre d’action et les privilèges d’un administrateur métier sont limités à une application. Dans tous les cas, tous les comptes d’administration, techniques comme métiers, sont des ***comptes privilégiés***, soumis aux recommandations de cette section.

1. **Comptes d’administration**

Les comptes utilisés pour les actions d’administration sont particulièrement sensibles car ils donnent aux administrateurs :

* Des privilèges élevés sur les ressources à administrer ;
* Un accès aux outils d’administration ;
* La capacité de modifier le comportement des mesures de sécurité ;

L’objectif ici est de s’assurer de la légitimité d’une personne à exécuter des ***actions d’administration*** et garantir la traçabilité de ses actions en utilisant des comptes spécifiques : les ***comptes d’administration***.

* **Usages des comptes d’administration**

La protection des comptes d’administration commence par une définition précise de leur cadre d’utilisation, par leur identification et leur bonne gestion. L’administrateur doit disposer d’un ou plusieurs comptes d’administration dédiés, distincts de son compte utilisateur, pour effectuer des actions d’administration. Les comptes d’administration doivent être utilisés *exclusivement* pour des actions d’administration. En particulier, aucun ***compte d’administration*** ne doit être utilisé pour des actions bureautiques ou l’ouverture de sessions de travail sur des postes autres que ceux réservés aux actions d’administration.

Dans certains cas, l’administration d’une ressource ne peut pas techniquement être effectuée à partir d’un compte spécifique d’administration. L’opérateur doit alors atteindre par d’autres moyens l’objectif de protection des actions d’administration : traçabilité et supervision des actions d’administration, actions d’administration effectuées exclusivement par des administrateurs, limitation des adresses IP, etc. Par exemple sur certains équipements, toutes les opérations sont accessibles à tous les utilisateurs, sans notion de privilège. Dans d’autres cas, les équipements ne gèrent pas de comptes.

L’utilisation d’un compte sur un élément de SI laisse potentiellement des traces qui peuvent être utilisées par un attaquant pour compromettre le compte associé. L’utilisation des comptes d’administration doit donc être limitée aux équipements pour lesquels l’administrateur a des actions à réaliser. Un compte d’administrateur ne doit donc pas servir à ouvrir une session bureautique sur un poste de travail. Ainsi, cette spécialisation et la réduction de l’usage des comptes d’administrations contribuent à diminuer la probabilité qu’ils soient compromis. Les actions non relatives à l’administration (navigation sur Internet, messagerie, bureautique, accès applicatifs métier, etc.) doivent être faites depuis un compte utilisateur et jamais depuis un compte d’administration. Les administrateurs disposent donc en général d’au moins deux comptes : un compte utilisateur et un ou plusieurs comptes d’administration, et les secrets d’authentification de tous ces comptes doivent être distincts. Par ailleurs, les comptes natifs d’administration, dits *built-in* (ex. : root, admin), présents par défaut sur les équipements lors de l’installation ne doivent pas être utilisés. Leur utilisation doit rester exceptionnelle et restreinte à un nombre d’administrateurs très limité. En effet, ces comptes ne permettent pas d’imputer de manière précise les actions effectuées sur les équipements. Cela rend aussi impossible la mise en œuvre d’un contrôle d’accès pertinent aux outils d’administration et la ségrégation des droits. Seule la création de comptes individuels d’administration peut répondre à ces besoins. Lorsqu’ils existent, les mots de passe par défaut des comptes natifs doivent être changés.

Nous devons créer un compte d’administration individuel pour chaque administrateur. Pour faciliter la gestion des droits d’administration (ajout, modification et suppression), il est recommandé de créer des groupes dans le ou les annuaires des comptes d’administration. Un groupe contient, en fonction du juste besoin opérationnel, l’ensemble des comptes d’administration devant disposer de droits d’administration homogènes sur une ou plusieurs ressources administrées. Les droits sur ces ressources sont ainsi octroyés aux groupes et non aux comptes.

* **Protection des comptes**

Les actions d’administration sont effectuées au moyen de ***comptes d’administration*** individuels, relatifs à des personnes physiques ou à des processus automatiques. Ces comptes sont vulnérables aux attaques classiques sur les comptes utilisateur, mais avec un impact potentiel plus important. La protection des comptes d’administration représente donc un enjeu important et demande la mise en œuvre de mesures particulières.

Les annuaires contribuant à identifier et authentifier les administrateurs sur les ressources administrées sont des éléments critiques. Leur prise de contrôle par un attaquant permet en effet de disposer de l’ensemble des privilèges sur le SI administré. Il est fortement recommandé que le ou les annuaires contenant les comptes d’administration soient protégés en confidentialité et en intégrité et ne soient pas exposés sur des environnements de moindre confiance. Il est recommandé de déployer un annuaire dédié au SI d’administration en tant qu’infrastructure d’administration. Celui-ci gère les comptes d’administration et le contrôle d’accès aux ressources administrées. Il est fortement recommandé que de s’assurer que les comptes utilisés pour l’administration technique du SI ne puissent être compromis en renforçant leurs mécanismes d’***authentification*** :

* Utilisation de mots de passe complexes ;
* Authentification à double facteur;
* Chiffrement ou hachage robuste des secrets d’authentification, lorsqu’ils sont en transit ou stockés ;
* Mécanismes de protection des mots de passe contre les attaques en ***force brute*** ;
* Mécanismes de protection contre le rejeu de mots de passe ;

Nous devons configurer les journaux de telle sorte qu’ils ne stockent aucune information sur les secrets utilisés pour l’authentification des comptes d’administration, que ce soit des éléments stockés en clair ou sous forme d’empreinte cryptographique. Par ailleurs, il est nécessaire de limiter au strict nécessaire les actions d’administration permises à un administrateur : chacun de ses comptes d’administration doit uniquement disposer des droits relatifs aux actions dont ce compte est responsable, et uniquement sur le périmètre dont ce compte est responsable : c’est le ***principe du moindre privilège***.

1. **Système d’information d’administration**

Les ressources matérielles et logicielles utilisées pour effectuer les actions d’administration constituent le ***SI d’administration***. L’objectif est de s’assurer de l’intégrité des ressources utilisées pour réaliser les ***actions d’administration*** et de la confidentialité des informations que ces ressources manipulent, avec un niveau de confiance à la hauteur des enjeux pour le SI administré. Ce SI particulier doit être considéré comme très sensible. Sans mesures de protection spécifiques, une compromission du SI d’administration a des conséquences majeures :

* L’attaquant a accès à tout ou partie des ressources d’administration, et contrôle alors les ressources administrées associées ;
* L’attaquant peut utiliser le SI d’administration pour contrôler les sources d’événement systèmes destinées à la journalisation, ou encore certains moyens de détection et de supervision, et réussir à masquer ses traces ; il est impossible de savoir exactement quelles ressources ont été compromises ;
* Il devient obligatoire de reconstruire intégralement l’ensemble du système d’information, les comptes et le SI d’administration ne pouvant plus être considérés comme une base saine de reconstruction ;

1. **Maitrise des ressources d’administration**

Les ressources utilisées pour administrer le SI sont des ressources critiques, dont le niveau de sécurité a un impact direct sur le niveau de sécurité du SI. Nous devons gérer et configurer les ressources matérielles et logicielles utilisées pour réaliser les ***actions d’administration***, ou les faire gérer et configurer par un prestataire mandaté pour réaliser ces actions. En aucun *cas* l’utilisation d’un équipement personnel ne doit être tolérée pour l’administration d’un SI. La gestion des équipements inclut notamment l’installation, le durcissement, le paramétrage, la personnalisation, la configuration des outils de sécurité, le maintien en conditions de sécurité, etc. L’objectif est d’avoir une maitrise des ressources.

1. **Un SI dédié à l’administration**

Afin d’éviter la compromission de son SI d’administration, nous devons dédier ce SI aux actions d’administration, le cloisonnement des ressources de moindre confiance, et filtrer les échanges avec ces ressources. Ces recommandations générales sont déclinées dans trois domaines :

* Le poste de travail de l’administrateur ;
* Le réseau utilisé pour se connecter aux ressources administrées ;
* Les outils et serveurs de rebonds utilisés pour administrer les ressources ;

1. **Poste d’administration**

Un poste de travail usuel dispose de nombreuses applications (suite bureautique, navigateur, messagerie et autres outils de communication, applications métiers) ayant des niveaux de sécurité rarement évalués et souvent faibles. De plus, ce poste de travail échange avec des réseaux d’un faible niveau de confiance comme Internet. Ce poste de travail usuel a donc une surface d’attaque importante, et il est très exposé. Face à un attaquant motivé, ou simplement par la multiplication des attaques automatiques auxquelles ce poste est exposé, la compromission de ce poste est très probable. Ainsi nous devons dédier des postes de travail physiques à l’exécution des actions d’administration. Ce poste doit être distinct du poste permettant d’accéder aux autres ***environnements de travail*** usuels accessibles sur le SI de l’entité (ressources métier, messagerie interne, gestion documentaire, Internet, etc.). Le poste de travail utilisé pour les actions d’administration sert à saisir et stocker de nombreux secrets liés aux SIE et à leur administration (identifiants, clés de chiffrement, fichiers de configuration, etc.). Ce poste est donc particulièrement sensible et doit être protégé en conséquence : il est désigné ***poste d’administration***. Nous pouvons par exemple mettre les mesures suivantes :

* Interdiction d’aller à Internet à partir de ce poste ;
* La restriction des droits d’administration du poste pour l’utilisateur ;
* La limitation des logiciels installés sur le poste ;
* L’utilisation de chiffrement pour les périphériques de stockage ;
* L’interdiction de reconnaissance des périphériques comme le téléphone et les clés USB pour éviter toute copie depuis ce poste ;

1. **Réseau d’administration**

Le réseau d’administration se définit comme le réseau de communication sur lequel transitent les flux internes au SI d’administration et les flux d’administration à destination des ressources administrées. Comme le poste d’administration, le réseau d’administration est un élément clé de la sécurisation du SI d’administration. Le principe de cloisonnement doit conduire à le séparer des autres réseaux de sensibilité moindre.

Nous devons déployer les ressources d’administration (ex. : postes d’administration, serveurs outils) sur un réseau physiquement dédié à cet usage. Afin de renforcer le contrôle d’accès au réseau d’administration, il est recommandé que les postes d’administration s’authentifient lorsqu’ils se connectent à ce réseau.

Lorsque nous ne pouvons pas dédier un réseau physique à l’administration et que, pour des raisons techniques, les flux d’administration circulent sur d’autres réseaux, nous devons alors déployer les ressources d’administration sur un réseau logique dédié à cet usage en mettant en œuvre des mécanismes de chiffrement et d’authentification de réseau, à savoir le protocole IPsec. En complément, des mécanismes de segmentation logique (VLAN) et de filtrage réseau sont recommandés pour limiter l’exposition du concentrateur VPN IPsec aux seuls postes d’administration. Il est recommandé de dédier une interface réseau physique d’administration sur les ressources administrées en s’assurant des prérequis suivants :

* Les services logiques permettant l’exécution des actions d’administration doivent être en écoute uniquement sur l’interface réseau d’administration prévue à cet effet ;
* Les fonctions internes du système d’exploitation ne doivent pas permettre le routage d’informations entre les interfaces réseau de production et l’interface réseau d’administration d’une même ressource. Elles doivent être désactivées (par exemple désactivation d’*IP Forwarding*) ;

À défaut d’une interface réseau physique d’administration, il est recommandé de dédier une interface réseau virtuelle d’administration sur les ressources administrées.

Il est aussi fortement recommandé de cloisonner et de filtrer le réseau d’administration, avec en particulier :

* Un filtrage interne au sein du SI d’administration, entre zones de confiance (postes d’administration, serveurs d’infrastructures, outils, les différents réseaux de ressources administrées) ;
* Un filtrage périmétrique à toutes les interconnexions du SI d’administration avec d’autres SI ;
* Un filtrage local sur chaque ressource administrée ;
* L’activation du PVLAN (Private VLAN**)** sur les commutateurs reliant les ressources administrées, pour interdire les flux entre ressources administrées à travers le réseau d’administration ;

1. **Protocoles d’administration**

Les protocoles utilisés pour administrer le SI contribuent eux aussi à la sécurité des flux d’administration. Le recours aux versions chiffrées de ces protocoles, lorsqu’elles existent, protège l’intégrité et la confidentialité des informations relatives à l’administration.

Les flux d’administration étant particulièrement sensibles, il est fortement recommandé que l’entreprise utilise une version sécurisée des protocoles d’administration permettant de protéger la confidentialité et l’intégrité de ces flux. Le cas échéant, les protocoles non sécurisés doivent être explicitement désactivés ou bloqués.

1. **Administration de plusieurs SI**

Le SI d’administration utilisé pour le SI peut aussi servir à administrer d’autres SI. Pour rappel, un poste d’administration peut disposer d’outils installés localement ou, de manière non exclusive, accéder à des serveurs outils d’administration. Un administrateur peut disposer d’un poste unique pour l’administration de différentes zones de confiance (par exemple, un SI et d’autres SI), aux conditions suivantes :

* La sécurisation du poste d’administration doit être en phase avec les besoins de sécurité de la zone de confiance administrée la plus exigeante ;
* Les serveurs outils accessibles depuis le poste d’administration ne doivent pas être mutualisés pour l’administration de deux zones de confiance distinctes (en d’autres termes, un serveur outils reste dédié à une unique zone de confiance et est cloisonné) ;
* Les éventuels outils installés sur le poste d’administration ne doivent pas permettre un rebond entre deux ressources administrées de deux zones de confiance distinctes ;
* L’accès aux différentes zones de confiance depuis le SI d’administration doit respecter le cloisonnement, physique ou logique, entre zones de confiance (en d’autres termes, deux pares-feux physiques ou un pare-feu configuré avec deux DMZ sont déployés en périphérie du SI d’administration, pour respecter le cloisonnement des zones de confiance) ;
* Outils d’administration

1. **Sensibilisation humaine**

La faiblesse d’un système informatique repose en grande partie sur les utilisateurs : on dit que l’humain est le maillon le plus faible de la chaine d’un SI. Ainsi, quelques soient les mesures de sécurité mises en œuvre, sans la collaboration des utilisateurs elles sont vaines. Pour pallier à ce problème, il faut passer par deux étapes qui sont intrinsèquement liées :

1. **Sensibilisation**

La première étape consiste à sensibiliser les utilisateurs du SI sur l’importance de la politique de sécurité mise en place ainsi que les potentielles conséquences de leurs actes irréfléchis. Nous pouvons par exemple :

* Leurs demander de suivre à la lettre la politique de sécurité de l’entreprise ;
* Leurs demander de choisir un mot de passe fort qui répond aux exigences de la politique de sécurité ;
* Leurs demander de ne pas ouvrir ou télécharger les pièces jointes dans un email provenant d’une adresse inconnue ;
* Leurs demander de ne pas écrire leur mot de passe sur des papiers ;
* Leurs demander de vérifier toujours l’adresse des sites pour éviter le phishing ;
* Etc.

1. **Formations**

La formation des utilisateurs est la deuxième étape de la sensibilisation. Elle consiste à montrer aux utilisateurs le bon fonctionnement du SI pour assurer son adoption et son utilisation efficace. Elle doit se faire avec l’aval de tous les responsables des services. Une formation réussie doit suivre les points suivants :

* **Types d’utilisateurs :** Il s’agit de déterminer les différents groupes d’utilisateurs (débutants, intermédiaires et experts) ;
* **Objectifs de la formation :** Quels éléments enseigner aux apprenants (utilisation de base, fonctionnalités avancées ou résolution de problèmes) ;
* **Choix de la méthode :** En présentiel, à distance ou encore mixte ;
* **Contenu de la formation :** Il doit être simple et clair. Exemples concrets et utilisation des supports visuels ;
* **Exercices pratiques :** Illustration des concepts avec des exemples pratiques et des cas d’utilisation réels. Inclure des exercices pratiques pour permettre aux apprenants de mettre en pratique leurs connaissances ;
* **Evaluation des connaissances :** Il faut utiliser des quiz ou des examens pour vérifier la compréhension des apprenants (utilisateurs) ;

1. **Conformité et réglementation**
2. **Les normes**

Les normes de sécurité informatique sont des ensembles de règles, de bonnes pratiques et de cadres de référence conçus pour protéger les systèmes d'information contre les menaces et les vulnérabilités. Elles aident les organisations à structurer leur sécurité, à réduire les risques et à se conformer aux réglementations. Voici un aperçu des principales normes de sécurité informatique que nous devons acquérir :

* **ISO/IEC 27001**: Son objectif est d’établir un Système de Management de la Sécurité de l'Information (SMSI). Elle couvre la gestion desrisques, le contrôle d'accès, la gestion des incidents et la continuité des activités ;
* **ISO/IEC 27002 : Son objectif est de f**ournir des lignes directrices pour la mise en œuvre des contrôles de sécurité recommandés dans l'ISO 27001. Elle couvre les politiques de sécurité, la gestion des actifs, la sécurité physique et la gestion des accès ;
* **ISO/IEC 27005 :** L’objectif est de guider la gestion des risques liés à la sécurité de l'information ;
* **ISO/IEC 27032 : Son objectif est de fournir un cadre pour gérer la gestion des risques liés à la cybersécurité ;**
* **NIST Cybersecurity Framework (CSF) : Son objectif est de f**ournir un cadre pour gérer les risques de cybersécurité. Elle couvre l’identification, la détection, la récupération et la réponse ;
* **ISO/IEC 27035 : Son objectif est** de fournir des lignes directrices pour la gestion des incidents de sécurité. Elle couvre la gestion des incidents, la gestion des problèmes et la gestion des changements ;
* **ISO 22301 : Son objectif est d’é**tablir un Système de Management de la Continuité des Activités (SMCA). Elle couvre la planification, les tests, la gestion des crises et la reprise après sinistre ;

1. **La réglementation**

La réglementation est l’ensemble des règles qui garantissent les droits des personnes et des entreprises face vis-à-vis d’une situation donnée. Dans le domaine informatique, elle représente les lois et les arrêtés qui définissent les droits et devoirs des citoyens et des entreprises en matière de traitement, de la protection et la sauvegarde des données. Elle définit aussi les peines encourues en cas de non-respect des lois. Dans notre cas, nous devons nous du respect des législations suivantes :

* Le code pénal ;
* La loi **N° 2024/017 du 23/12/2024** sur a protection des données personnelles ;
* La loi **du 2010** sur la cybersécurité et la cybercriminalité ;
* Etc.

1. **Mise en œuvre de la technique du cloisonnement**
2. **Cloisonnement du système**
3. **Cloisonnement physique du système**

Dans le cas d’un cloisonnement physique, on suppose que la machine physique n’est utilisée que pour une fonction. Sa compromission ne touche donc que cette seule fonction. Tout autre système ou toute autre application est hébergé sur une machine physique différente.

**Exemple :** Un SI contient deux serveurs Web, l’un accessible depuis le réseau public et l’autre accessible uniquement depuis un réseau local. Leur différence d’exposition conduit à les cloisonner en deux sous-systèmes. Il est recommandé de les installer sur deux machines physiques différentes. Ainsi, la compromission d’une des machines ne peut s’étendre à l’autre que si elles sont toutes deux connectées au même réseau, d’où l’importance du cloisonnement réseau et du filtrage réseau.

1. **Cloisonnement logique chiffré du système**

Dans le cas d’un cloisonnement logique par le chiffre, plusieurs éléments sont mutualisés sur la même machine physique et un outil de chiffrement assure que la compromission d’un élément ne compromet pas la confidentialité et l’intégrité des données des autres systèmes.

**Attention :** Les exemples de cloisonnement par le chiffre au niveau système sont très rares. En effet, dès que l’information est accessible en clair sur un système par un processus qui y a légitimement accès, alors le cloisonnement ne repose plus sur le chiffre mais sur des mécanismes logiques de contrôle d’accès à la mémoire. Ce cas se rencontre fréquemment : chiffrement d’un disque (le disque est déchiffré lorsqu’il est monté au niveau du système d’exploitation), chiffrement d’une machine virtuelle sur le stockage (la machine virtuelle est déchiffrée avant d’être exécutée).

Un des rares exemples pertinents est celui du chiffrement homomorphe des données. Dans ce cas, les données sont chiffrées sur un premier serveur, puis manipulées sur un second serveur par un processus qui effectue des calculs sur ces données, sans les déchiffrer et donc sans les exposer aux autres processus partageant ce serveur.

1. **Cloisonnement logique simple du système**

Si nous décidons de mettre en œuvre un cloisonnement logique simple, nous devons déterminer quelles ressources nous souhaitons mutualiser sur une machine physique et quels mécanismes logiques assurent la fonction de cloisonnement.

Quelques exemples de mécanismes logiques permettant de cloisonner des applications partageant une même machine physique :

* Avoir plusieurs machines virtuelles, chacune hébergeant un système d’exploitation et une application, exécutées par un hyperviseur ;
* Avoir, au sein d’un même système d’exploitation, plusieurs espaces d’exécution (comme des conteneurs) dédiés chacun à une application ;
* Avoir des services différents, exécutés par des comptes distincts, au sein d’un même système d’exploitation ;

Dans ce cas, la machine physique et certaines couches logicielles (hyperviseur, OS, etc.) sont mutualisées entre plusieurs fonctions et la compromission de l’une de ces fonctions augmente les possibilités d’attaque des autres fonctions. Ce type de cloisonnement n’est pas recommandé pour des fonctions de niveaux de sensibilité ou d’exposition homogènes.

1. **Cloisonnement du réseau**
2. **Cloisonnement physique du réseau**

Pour un réseau, le cloisonnement physique est mis en œuvre en dédiant du matériel (câblage, équipements actifs comme les commutateurs et les pare-feux) à chaque sous-système à cloisonner. Cette solution est la plus sécurisée. Il peut s’accompagner :

* Soit de l’absence totale d’interconnexion du SI avec d’autres SI. On parle alors d’un SI isolé. L’expression anglaise *air-gapped* désigne également cette architecture ;
* Soit de l’existence d’interconnexions réalisées au moyen de diodes réseau permettant de garantir l’uni directionnalité du flux d’information, du SIE vers les autres SI (pour une protection en intégrité et en disponibilité du SIE). Le niveau d’assurance de la fonction d’uni directionnalité est dépendant de la technologie mise en œuvre au sein de la diode réseau ; par exemple une diode optique apporte *a priori* un niveau d’assurance supérieur à une diode mettant en œuvre un contrôle des flux par circuit logique programmable (FPGA) ;
* Soit finalement de la présence d’interconnexion avec un dispositif de filtrage tel qu’un pare-feu. Ce dernier cas relève alors d’un cloisonnement logique simple ;

1. **Cloisonnement logique chiffré du réseau**

Nous pouvons aussi utiliser le même réseau physique pour porter à la fois des flux de données d’un SI et ceux d’autres SI. Dans ce cas, il possible de cloisonner ces flux en mettant en œuvre un cloisonnement logique par le chiffre. Nous pouvons par exemple utiliser un même réseau physique pour transporter des tunnels ***VPN*** chiffrés et authentifiés pour des flux de sensibilités différentes, par exemple avec le protocole ***IPsec***.

Le chiffrement peut être appliqué depuis l’émetteur jusqu’au destinataire du flux, comme dans le cas d’un chiffrement applicatif type HTTPS. Le chiffrement peut aussi être appliqué uniquement sur une partie du trajet lorsque le flux traverse un réseau de moindre confiance, comme dans le cas d’un tunnel IPsec reliant deux réseaux à travers un réseau tiers. Les deux possibilités peuvent être combinées, réalisant du chiffrement multiple : par exemple, des commandes d’administration envoyées chiffrées par SSH transitant sur un réseau d’administration logique chiffré par IPsec.

1. **Cloisonnement logique simple du réseau**

Un cloisonnement logique d’un niveau de sécurité moindre peut être fait au niveau du réseau, sans chiffrement. Nous pouvons par exemple définir des réseaux logiques sur un même réseau physique au moyen de VLAN. Un cloisonnement par VLAN n’est cependant pas recommandé comme unique moyen de cloisonnement, puisque le cloisonnement repose alors sur la bonne configuration et la robustesse de l’ensemble des équipements traversés.

Appliqués à un réseau mutualisé, le principe de défense en profondeur et l’efficacité économique peuvent amener à combiner le cloisonnement physique, le cloisonnement par le chiffre et le cloisonnement logique simple pour répondre à différentes contraintes et menaces.

**Exemple :** Dans un SI, le réseau d’administration peut être physiquement distinct du réseau de production (cloisonnement physique). Au sein de ce réseau d’administration, plusieurs VLAN sont définis pour isoler des groupes de ressources administrées, et le mécanisme de PVLAN (*private VLAN*) est activé sur chaque VLAN pour empêcher le rebond entre les ressources administrées (cloisonnement logique simple). Enfin, l’administration des ressources se fait via des protocoles chiffrés (cloisonnement logique par le chiffre).

1. **Cloisonnement du stockage**
2. **Cloisonnement physique du stockage**

Un système de stockage peut être physiquement dédié à un serveur. C’est le cas pour des disques internes au serveur ou pour une baie à attachement direct (*direct-attached storage*). Le système de stockage peut être aussi partagé entre plusieurs serveurs. Ce système de stockage peut être un équipement de type serveur de stockage en réseau (*network-attached storage* ou NAS) ou bien un système composé d’un réseau spécialisé (*storage area network* ou SAN). Un système de stockage physique peut être commun à un ensemble de SI de même niveau de sensibilité : plusieurs SI du même opérateur, ou plusieurs SI sensibles.

Il est aussi possible de dédier une partie seulement d’un système de stockage à un SI, comme un ensemble de disques dédié à un SIE dans une baie pourtant mutualisée. Parce qu’il existe dans ce cas un composant mutualisé (ici, le contrôleur de la baie), l’efficacité du cloisonnement repose d’abord sur la robustesse du logiciel de ce composant. Il ne s’agit donc pas d’un cloisonnement physique, mais d’un cloisonnement logique simple, d’un niveau de confiance moindre.

1. **Cloisonnement logique chiffré du stockage**

Dans un cloisonnement logique par le chiffre, chaque sous-système dispose d’un espace logique chiffré au sein du système de stockage. Il est recommandé d’appliquer le chiffrement en amont du stockage, par les systèmes propriétaires des données, et non pas sur le système de stockage lui-même.

1. **Cloisonnement logique simple du stockage**

Pour un système de stockage, le cloisonnement logique simple consiste à contrôler l’accès à une ressource de stockage en fonction de critères logiques. Par exemple, on a :

* Le mécanisme de *zoning* permet de configurer quelles sont les ressources visibles ou accessibles aux hôtes dans un SAN. Il est mis en œuvre par les commutateurs du SAN ;
* Le mécanisme de *LUN masking* permet de configurer quelles unités logiques (LUN) sont accessibles aux contrôleurs hôtes de bus (*host bus adapters* ou HBA). Il est mis en œuvre par les contrôleurs des baies de stockage ;
* Le contrôle d’accès en lecture et en écriture aux partitions exposées par un NAS est lui aussi logique. Il s’appuie sur des éléments d’authentification présentés par les clients et est mis en œuvre par le serveur NAS ;

Le principe de défense en profondeur et l’efficacité économique peuvent amener à combiner plusieurs types de cloisonnement sur un système de stockage partagé : cloisonnement physique, cloisonnement logique par le chiffre et cloisonnement logique simple. Cette combinaison répond à des menaces variées. Par exemple :

* S’il est parfois difficile de justifier économiquement de dédier un système de stockage à chacun des SI, il peut être plus facile de déployer deux systèmes indépendants (SAN et baie) pour cloisonner physiquement d’un côté le stockage des SI sensibles de l’entité (dont les SIE) et de l’autre celui des SI moins sensibles ;
* Au niveau de chaque système de stockage physique, un premier niveau de segmentation est apporté par du cloisonnement logique simple par *zoning* et *LUN masking*. Chaque hôte n’a en théorie accès qu’aux unités logiques dont il a besoin ;
* Le chiffrement des données par les hôtes, en amont du système de stockage, complète le dispositif de protection en garantissant que les données en clair ne sont accessibles qu’à l’hôte qui les a chiffrées ;
* Si le chiffrement par les hôtes n’est pas possible, le chiffrement des données par la baie avant écriture sur les disques permet de se prémunir contre une fuite de données en cas de vol ou de perte des médias de stockage ;

1. **Enjeux futurs et défis**

Les enjeux futurs de la protection des données et de la cybersécurité seront marqués par des défis complexes, liés à l'évolution technologique, aux menaces sophistiquées et aux exigences réglementaires. Voici une analyse structurée des principaux enjeux :

### **Intelligence Artificielle (IA) et automatisation des attaques : les outils d’IA sont des outils à Double tranchant**. L'IA renforce les outils de détection (analyse comportementale, prédiction de menaces), mais les cybercriminels l'utilisent aussi pour automatiser des attaques (ex : phishing hyper-personnalisé, deepfakes). Ainsi nous nous attendons à des **cyberattaques autonomes** capables de s'adapter en temps réel ;

### **Informatique quantique et cryptographie :** Les ordinateurs quantiques pourront cracker des algorithmes de chiffrement asymétrique (RSA, ECC), compromettant la confidentialité des données. Il y a une menace sur le chiffrement actuel. Ainsi, il est indispensable de développer des algorithmes cryptographiques post-quantiques ;

### **Sophistication des cybermenaces** : Evolution des ransomwares, menaces étatiques, attaque par la chaine d’approvisionnement ;

1. **Expansion de l’IoT et des objets connectés**: Elargissement de la surface d’attaque ;
2. **Conformité règlementaire et confidentialité :** Régulations fragmentées, gestion des données sensibles et transparence des algorithmes ;
3. **Ingénierie sociale :** Exploitation de la confiance des utilisateurs, des menaces internes, éducation et sensibilisation ;
4. **Ethique et surveillance de masse :** Dilemme vie privée et sécurité, risque de dérive autoritaire ;
5. **Cyber-résilience et préparation aux crises :** Prévention et gestion des crises ;
6. **Collaboration internationale :** Partage de renseignements sur les menaces (*threat intelligence*) et Harmonisation des réglementations ;
7. **Audit du système**

L'audit de sécurité d'un système d'information (SI) est une vue à un instant T de tout ou partie du SI, permettant de comparer l'état du SI à un référentiel. L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du système. L'auditeur dresse également une série de recommandations pour supprimer les vulnérabilités découvertes.

Un audit de sécurité SI peut être réalisé pour répondre à des besoins différents, notamment :

* Evaluer le niveau de maturité du SI en termes de sécurité à la suite de la demande du commanditaire d’audit ;
* Vérifier l’efficacité de la politique de sécurité du SI mise en place ;
* Tester l’installation d’un nouvel élément dans le SI ;
* Analyser et réagir à la suite d’une attaque ;
* Tester la résistance du SI par la simulation des attaques dans des conditions réelles ;
* Passer un test pour un certificat (par exemple ISO 27001) ;
* Etc.

Les audits peuvent être classifiés en trois catégories :

* **Les audits internes** (appelés aussi audits de 1ère partie) sont réalisés pour les organismes souhaitant que leur système d’information soit examiné par rapport à des exigences de sécurité de système d’information. Ces audits sont établis par des auditeurs internes ou externes à l’organisme ;
* **Les audits externes** (appelés aussi audits de 2ème partie) sont commandités par des entités ayant un intérêt à l’égard de l’organisme audité, dans le but d’évaluer le niveau de sécurité du système d’information de ce dernier. Ces audits sont établis par des organismes d’audit externes ;
* **Les audits de certification** (appelés aussi audits de tierce partie) sont réalisés pour les organismes qui souhaitent faire reconnaître que la sécurité de leur système d’information est conforme aux exigences comme celles de l’ISO/CEI 27001. Ces audits sont établis par des organismes externes généralement accrédités ;

L’audit de sécurité SI représente une activité complexe qui couvre l’ensemble des composants du système d’information. Il consiste à évaluer le niveau de sécurité et à proposer les moyens de correction adaptés. Cette évaluation concerne les domaines suivants :

* Audit organisationnel et physique ;
* Politiques de sécurité de l’information ;
* Organisation de la sécurité de l’information ;
* Sécurité des ressources humaines ;
* Gestion des actifs ;
* Contrôle d’accès ;
* Cryptographie ;
* Sécurité physique et environnementale ;
* Sécurité liée à l’exploitation ;
* Sécurité des communications ;
* Acquisition, développement et maintenance des systèmes d’information ;
* Audit Technique de sécurité ;
* Audit des vulnérabilités infrastructure et système : phase de découverte des vulnérabilités et phase d’analyse des vulnérabilités ;
* Audit d’architecture réseau ;
* Audit de configuration ;
* Tests d’intrusion ;
* Audit applicatif ;

**Conclusion**

La sécurisation des SI repose sur une approche holistique et dynamique, intégrant des mesures techniques, organisationnelles et humaines. La protection des SI n'est pas un projet ponctuel, mais un processus continu nécessitant :

* Vigilance proactive face à l'évolution des menaces ;
* Adaptabilité aux nouvelles technologies (cloud, IoT, IA) ;
* Collaboration entre équipes techniques, dirigeants et gouvernements ;
* Éducation pour transformer les utilisateurs en première ligne de défense ;

Sans une approche équilibrée et anticipative, les risques de perturbations économiques, sociales et géopolitiques seront exponentiels. La cybersécurité doit donc être perçue non comme un coût, mais comme un investissement essentiel pour la pérennité et la crédibilité des organisations dans un monde hyperconnecté.

**Bibliographie/Webographie**

* RECOMMANDATIONS POUR LA PROTECTION DES SYSTÈMES D'INFORMATION ESSENTIELS (GUIDE ANSSI) du 18/12/2020
* <https://www.ibm.com/fr-fr/topics/identity-access-management>
* <https://www.microsoft.com/fr-ca/security/business/security-101/what-is-identity-access-management-iam>
* <https://www.silverfort.com/fr/blog/best-iam-tools>
* [www.deepseek.com](http://www.deepseek.com)