Partie 2 :

Principes, pratiques et processus de cybersécurité

Formateur : Azer Zairi
(azer.zairi@gnet.tn)

Partie 2 – Sections et objectifs

2.1 Le cube de la cybersécurité

Décrire les trois dimensions du cube de McCumber.

2.2 LA TRIADE CID

Décrire les principes de confidentialité, d'intégrité et de disponibilité.

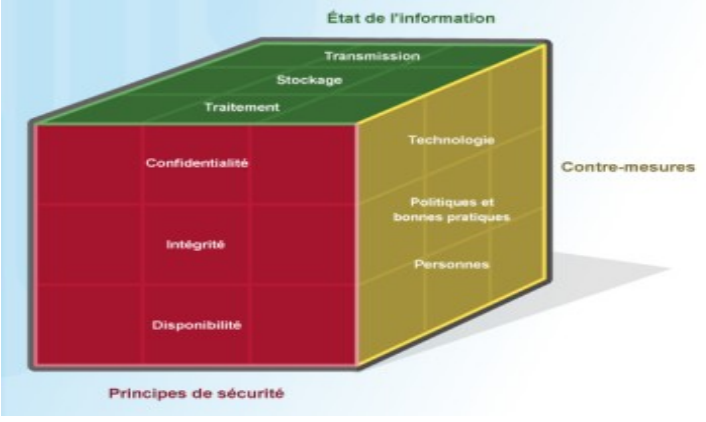
2.3 Les états des données

Expliquer la différence entre les trois états possibles pour des données.

2.4 Les mesures de cybersécurité

Comparer les différents types de contre-mesures en matière de cybersécurité.

2.1 Les trois dimensions



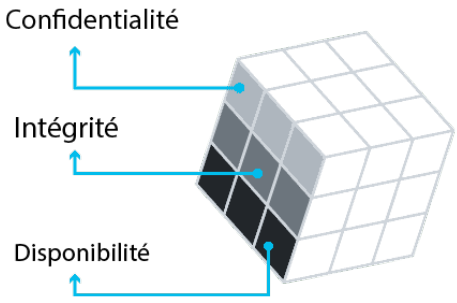
Le Cube de la cybersécurité

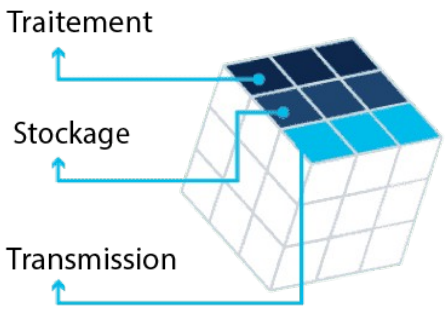
Le **Cube** de **cybersécurité** offre un **moyen utile** de réfléchir à la protection des données et inclut les **trois dimensions** de la **sécurité** des informations.

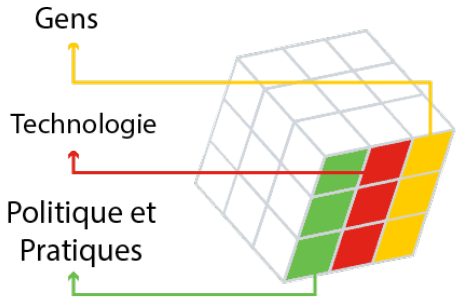
1. **Principes de sécurité** identifier les **objectifs** pour protéger le cyberespace.
- La **confidentialité** des données
- **Intégrité** des données
- **Disponibilité** des données

2. **États des données** représentent les trois états possibles des données.
- données **en transit**
- Data **au repos** ou en stockage.
- données **en cours de traitement**

3. **Mesures**
La troisième dimension du cube de la cybersécurité définit les piliers sur lesquels nous devons baser nos défenses en matière de cybersécurité afin de protéger les données et l'infrastructure dans le domaine numérique.
- **Technologie**
- **Politiques et bonnes pratiques**
- Améliorer l'éducation, la formation et la sensibilisation du **public**



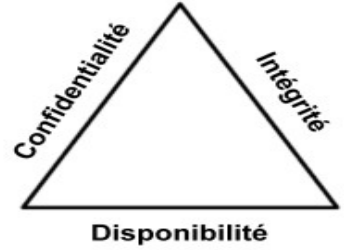




Les trois dimensions

Les principes de la sécurité

- La **première dimension** du cube magique de la cyber sécurité identifie les **objectifs** à protéger sur Internet.
- **Ces objectifs constituent les principes fondateurs de la cybersécurité.**
- Ces trois principes sont la **confidentialité**, l'**intégrité** et la **disponibilité**.
- Ces principes permettent aux spécialistes de la cybersécurité de **cibler ses efforts et d'établir des priorités** dans les mesures à prendre pour assurer la protection de ses ressources sur Internet.
- Ces principes sont définis par lles initiales CID (ou CIA en anglais).



Les trois dimensions

Les états des données

- La **deuxième dimension** du cube magique de la cybersécurité porte sur les problèmes liés à la protection des données sur Internet, quel que soit leur **état**.
- Les données peuvent se présenter sous **trois états** différents :

1) Données enregistrées ou **stockées**
2) Données en **transit**
3) Données en cours de **traitement**

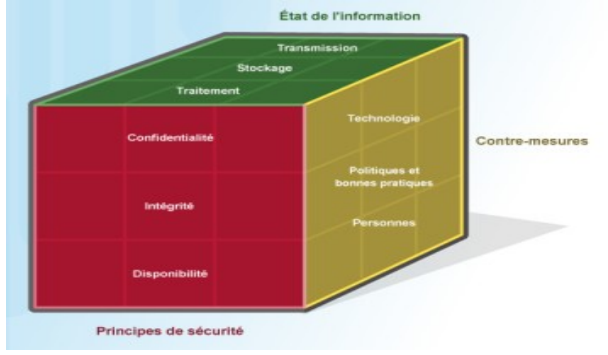
Le cube magique de la cyber sécurité

Les trois dimensions (suite)

Dispositifs de protection en cybersécurité

- La **troisième dimension** du cube magique de la cybersécurité définit les **types d'outils** utilisés pour la protection sur Internet.
- Autrement, **qui** appliquera la sécurité,

  par quel **moyen** et avec quelle **méthode** ou **démarche**
- Le cube magique identifie trois types d'outils :
  - **Technologies :** appareils et produits disponibles pour protéger les systèmes d'information et contrer les cybercriminels.
  - **Politiques et bonnes pratiques :** procédures et directives permettant aux citoyens du monde virtuel d'être protégés et de respecter les bonnes pratiques.
  - **Personnes :** informées et qualifiées, ils connaissent leur monde virtuel et les dangers qui le menacent.



2.2 LA TRIADE CID

LA TRIADE CID

Confidentialité

Le principe de confidentialité

- Le principe confidentialité consiste à **empêcher** la divulgation d'informations à des personnes, des ressources ou des processus non autorisés.
- Les entreprises doivent **former** leurs **collaborateurs** sur les **bonnes pratiques** permettant de **préserver** la **confidentialité** des **informations sensibles**
  - afin de **se protéger** eux-mêmes et leur entreprise **contre des attaques**.
- **Diverses méthodes** permettent de garantir la confidentialité des données, notamment le **chiffrement** des données, **l'authentification** et le **contrôle** d'accès.

Protection de la vie privée

- Les **entreprises collectent une grande quantité de données dont la majeure partie n'est pas sensible**,
  - car elles sont **accessibles publiquement**, comme les noms et les numéros de téléphone.
- Toutefois, parmi les données collectées, d'**autres peuvent être sensibles**.
- Les **informations sensibles** sont **protégées contre** les **accès** non autorisés afin de **protéger** un **individu** ou une **entreprise**.

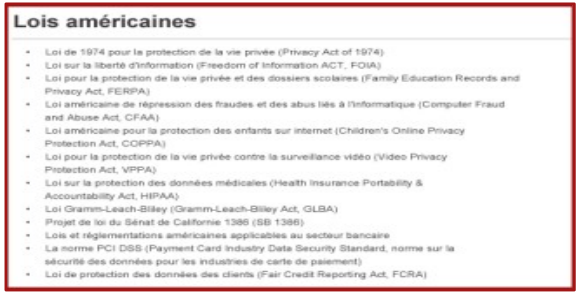
Remarque :
Selon la politique de l’entreprise, il faut différencier entre les données sensibles et les moyens sensibles

LA TRIADE CID

Confidentialité (suite)

Les notions de **confidentialité** et le **respect** de la **vie privée** peuvent sembler **similaires**, mais elles désignent des **réalités juridiques distinctes**.

- La **majorité des données privées est confidentielle**, mais **toutes les données confidentielles ne relèvent pas de la sphère privée**.
  - **L'accès** aux informations confidentielles est **permis après** avoir **confirmé** que **l'utilisateur** dispose des **autorisations** nécessaires.
  - Les **institutions financières**, les **hôpitaux**, les professionnels de **santé**, les cabinets **d'avocats** et les **entreprises** traitent des informations confidentielles.
- **Toute information confidentielle relève d'un statut non public.**
  - Préserver la confidentialité constitue un **devoir de nature éthique**.
- Le respect des informations privées s'attache à l'utilisation des données.
  - Lorsque des entreprises collectent des informations fournies par leurs clients ou leurs collaborateurs, elles doivent limiter l'utilisation de ces données à l'usage prévu.



LA TRIADE CID

Intégrité

Principe de l'intégrité des données

- L'intégrité représente **l'exactitude**, la **cohérence** et la **fiabilité** des **données** pendant tout leur cycle de vie.
- Les **méthodes utilisées** pour assurer l'intégrité des données comprennent le calcul de **hashs**, les **contrôles** de **validité** des données et les **contrôles d'accès**.

Importance de l'intégrité des données

- L'importance de l'intégrité des données varie selon l'utilisation qu'une entreprise fait de ces données.
  - ***Par exemple***, les réseaux sociaux ne vérifie pas, systématiquement, les données publiées par un utilisateur sur son profil.
- Les **banques** ou les **sociétés financières** attribuent une **importance** plus **élevée** à **l'intégrité** de leurs données
  - Les transactions et les comptes clients doivent être exacts.
- La **protection** de **l'intégrité** des données représente un **défi permanent** pour la plupart des entreprises.
  - La **perte** de **l'intégrité** des données peut rendre des ressources de données **entières non fiables**, voire **inutilisables**.

Vérification de l'intégrité

- Une vérification de l'intégrité permet de mesurer la cohérence d'un ensemble de données (un fichier, une image ou un enregistrement).
- Le **processus** de **vérification** de **l'intégrité** consiste à **exécuter** une opération appelée **fonction de hash** pour enregistrer l'état des données à un moment précis.

LA TRIADE CID

Disponibilité

On appelle **disponibilité** des données le principe selon lequel il est nécessaire **d'assurer** une **disponibilité en continu** des ressources à exploiter.

Certains **dysfonctionnements** et **attaques** peuvent **empêcher l'accès** aux systèmes et services d'information.

- **Plusieurs méthodes** existent pour **garantir** la **disponibilité**, notamment la **redondance** du système, les **sauvegardes** système, la **résilience renforcée** du système, la **maintenance** des équipements, la **mise à jour** des systèmes d'exploitation et des logiciels et l'élaboration de **plans de reprise** après un incident.
- Les **systèmes** à **haute disponibilité** reposent généralement sur **trois principes** de **conception** :
  - **éliminer les points de défaillance uniques**, **fournir des substitutions fiables** et **détecter les défaillances** dès qu'elles se produisent.

Les entreprises garantissent la disponibilité des informations grâce aux **mesures** suivantes :

1. **Maintenance** des équipements
2. **Mise à jour** du système d'exploitation et des logiciels
3. **Test** des **sauvegardes**
4. **Plan** de **gestion** des **sinistres**
5. **Implémentation** de **nouvelles technologies**
6. **Surveillance** des **activités** inhabituelles
7. **Test** de vérification de la disponibilité

2.3 Les états des données

États des données

Données au repos

- Les données qui **ne sont pas en transit ou en cours de traitement** sont considérées comme des **données au repos.**
- Il y a plusieurs options de stockage à utiliser selon les besoins et le contexte :

Stockage à accès direct (DAS)	Il est connecté à un ordinateur. Par défaut, les systèmes ne sont pas configurés pour partager le stockage à accès direct avec les autres ordinateurs du réseau.
Réseau redondant de disques indépendants (RAID)	Ces solutions de stockage professionnelles utilisent plusieurs disques durs dans une matrice, qui est une méthode permettant de combiner plusieurs disques de sorte que le système d'exploitation les considère comme un seul disque. Un RAID permet de bénéficier d'une performance et d'une tolérance aux pannes améliorées.
Dispositif de stockage en réseau (NAS)	Il s'agit d'un dispositif de stockage connecté à un réseau qui permet le stockage et la récupération de données à partir d'un emplacement centralisé par les utilisateurs autorisés du réseau. Les périphériques NAS sont flexibles et évolutifs, ce qui signifie que les administrateurs peuvent augmenter leur capacité en fonction des besoins.
Réseau de stockage (SAN)	L'architecture SAN est un système de stockage en réseau. Les systèmes SAN se connectent au réseau à l'aide d'interfaces à haut débit, ce qui permet d'améliorer les performances et de connecter plusieurs serveurs à un référentiel de stockage sur disque centralisé.
Stockage dans le cloud	Le stockage cloud est une option de stockage à distance qui utilise l'espace disponible auprès d'un fournisseur de data center. Ce stockage est accessible à partir de n'importe quel ordinateur avec accès à Internet.

États des données

Défis relatifs à la protection des données stockées

- Pour **améliorer** la **protection** du **stockage** des données, les organisations peuvent **automatiser** et **centraliser** les **sauvegardes** de données.

Stockage à accès direct

- Le stockage à connexion directe (DAS) peut être l'un des types de stockage les plus difficiles à gérer et à contrôler.
- Il est, en effet, vulnérable aux attaques malveillantes sur l'hôte local.

Données au repos.

- Les données au repos incluent également les données de sauvegarde (quand elles ne sont pas en cours d'écriture ou en transit).
- Pour renforcer la sécurité et réduire les pertes de données, les entreprises doivent limiter les types de données stockées sur les périphériques de stockage à connexion directe.

Système de stockage réseau

- Il offre une option plus sécurisée.
- Ce type de stockage garantit de meilleures performances et une redondance accrue.

États des données

Méthodes de transmission des données

- Les données en **transit** sont des données en cours de **transmission**.
- Elles ne sont pas au repos ni en cours d'utilisation.
- Il existe de **nombreuses façons** de **transmettre** des données entre des appareils:
  - **Sneaker net:** Il utilise des **supports amovibles** pour déplacer physiquement des données d'un ordinateur à un autre.
  - **Les réseaux filaires:** Ils incluent des **supports** en **cuivre** et en **fibre optique** et peuvent desservir un réseau local (**LAN**) ou couvrir de grandes distances dans des réseaux étendus (**WAN**).
  - **Réseaux sans fil :** les données sont transmises par le biais **d'ondes radioélectriques**.
    - Les réseaux sans fil **augmentent** le **nombre d'utilisateurs** invités munis de dispositifs mobiles sur les réseaux des petits bureaux, des bureaux à domicile (SOHO) et des entreprises.

États des données

Les défis des données en transit

- Avec la **croissance** des **appareils mobiles** et sans fil, et **l'augmentation** des **quantités** de **données collectées** et **stockées** par les organisations, les **professionnels** de la **cybersécurité** sont **chargés** de **protéger** les **quantités massives** de **données** qui **traversent** quotidiennement leur **réseau**.

- Pour protéger ces données, plusieurs défis doivent être relevés :

Protéger la confidentialité des données en transit	Les professionnels de la cybersécurité doivent prendre des mesures pour protéger les données en transit, telles que la mise en œuvre de VPN, l'utilisation de SSL et IPsec, ainsi que de diverses autres méthodes de chiffrement des données à transmettre.
Protéger l'intégrité des données en transit	Les professionnels de la cybersécurité déploient des systèmes d'intégrité des données qui testent l'intégrité et l'authenticité des données transmises afin de contrer ces actions. Ces systèmes incluent, par exemple, le hachage et la redondance des données.
Protéger la disponibilité des données en transit	Les professionnels de la sécurité des réseaux peuvent mettre en place des systèmes d'authentification mutuelle pour contrer ces actions. Les systèmes d'authentification mutuelle exigent que l'utilisateur s'authentifie auprès du serveur et demandent au serveur de s'authentifier auprès de l'utilisateur.

États des données

Données en cours de traitement

- Les données en cours de traitement font référence aux données en cours **d'entrée initiale**, de **modification**, de **calcul** ou de **sortie**.

Entrée	La protection de l'intégrité des données commence lors de la saisie initiale des données. Les organisations utilisent plusieurs méthodes pour collecter des données, chacune présentant une menace potentielle pour l'intégrité des données : saisie de données, numérisation de formulaires, téléchargement de fichiers et données collectées par des capteurs.Les perturbations au cours du processus d'entrée peuvent inclure un mauvais étiquetage et des formats de données incorrects ou mal assortis, des erreurs de saisie de données ou des capteurs du système déconnectés et/ou fonctionnant mal ou inopérants.
Modification	La modification des données est tout changement apporté aux données originales, comme les utilisateurs qui modifient manuellement les données, et les programmes qui traitent et modifient les données. Mais les modifications apportées aux données peuvent être involontaires ou malveillantes. Lorsque les données sont modifiées d'une manière qui les empêche d'être lisibles ou utilisables, on parle souvent de corruption des données.
Sortie	La sortie de données fait référence à la sortie de données vers des dispositifs de sortie, tels que des imprimantes, des écrans électroniques et des haut-parleurs.L'exactitude des données en sortie est essentielle, dans la mesure où elles fournissent des informations et influencent la prise de décision.

États des données

Données en cours de traitement (suite)

- **Pour protéger** les données en cours de traitement, la **conception** des systèmes doit être **parfaitement étudiée**.
- **Sinon**, les **résultats** pour les entreprises peuvent être **graves** et **coûteux** pour leurs **finances** ou même leur **réputation**.
- Il incombe aux **professionnels** de la **cybersécurité** de **concevoir** des **politiques** et des **procédures complètes** concernant
  - les **tests**,
  - la **maintenance**
  - et les **mises à jour**
- afin que les systèmes fonctionnent avec le **moins d'erreurs** possible.

2.4 Les mesures de cybersécurité

Les mesures de cybersécurité

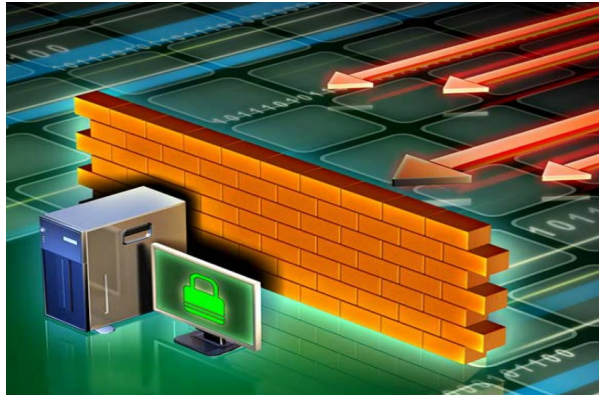
Les technologies

Des protections technologiques logicielles

- Les protections logicielles englobent les **programmes** et les **services** qui **protègent** les **systèmes d'exploitation**, les **bases** de **données** et les autres services exécutés sur les postes de travail, les appareils portables et les serveurs.
- **Les ressources d'une entreprise sont protégées à l'aide de plusieurs technologies logicielles**.

Des protections technologiques matérielles

- Les technologies matérielles sont des **appliances** (boîtiers) mises en œuvre au sein des installations réseau.
- Elles peuvent inclure : des appliances de **pare-feu**, des systèmes de détection d'intrusions (**IDS**), des systèmes de prévention des intrusions (**IPS**) et des systèmes de **filtrage** du contenu.



Les mesures de cybersécurité

Les technologies

Des protections technologiques basées sur le réseau

Les mesures technologiques peuvent aussi inclure des technologies basées sur le réseau.

- **Le réseau privé virtuel (VPN)** est un réseau virtuel sécurisé qui utilise le réseau public (c.-à-d., Internet).
  - La sécurité d'un VPN dépend du chiffrement du contenu du paquet entre les terminaux qui définissent le VPN.
- **Le contrôle d'accès au réseau (NAC)** exige un **ensemble** de **contrôles avant d'autoriser** un **appareil** à se **connecter à un réseau**.
  - Parmi les contrôles courants, on compte l'installation de mises à jour du système d'exploitation ou du logiciel antivirus.
- **La sécurité du point d'accès sans fil** inclut l'implémentation de l'authentification et du chiffrement.

Les mesures de cybersécurité

Les technologies

Des protections technologiques dans le cloud

- Les mesures technologiques peuvent aussi inclure des technologies basées sur le cloud.
- Les technologies dans le cloud déplacent la technologie de l'entreprise au fournisseur cloud.
- **Le logiciel proposé comme un service (SaaS)** permet aux utilisateurs d'accéder au logiciel d'application et aux bases de données.
- Les fournisseurs cloud gèrent l'infrastructure.
- Les utilisateurs stockent les données sur les serveurs du fournisseur cloud.
- **L'infrastructure sous forme de service (IaaS)** fournit des ressources informatiques virtualisées sur Internet.
- Le fournisseur héberge le matériel, les logiciels, les serveurs et les composants de stockage.
- **Les appliances de sécurité virtuelles** s'exécutent dans un environnement virtuel avec un système d'exploitation renforcé prêt à l'emploi s'exécutant sur du matériel virtualisé.

Les mesures de cybersécurité

Mise en œuvre de formations sur la cybersécurité

C'est pourquoi il est important pour les entreprises d'élaborer un **programme de sensibilisation à la sécurité**.

Certains collaborateurs font preuve d'un **comportement malveillant sans** même le **savoir**, simplement parce qu'ils **ne connaissent pas** les **procédures appropriées**.

Il existe plusieurs manières pour mettre en œuvre un programme de formation officiel :

- Sensibilisez les nouveaux collaborateurs à la sécurité lors de leur processus d'intégration
- Ajoutez la sensibilisation à la sécurité aux conditions requises pour un poste ou aux évaluations de performances
- Réalisez des sessions de formation en présentiel
- Organisez des cours en ligne

La sensibilisation à la sécurité doit être continue, car de nouvelles menaces et de nouvelles techniques font constamment leur apparition.

Les mesures de cybersécurité

Politiques et procédures de cybersécurité

- Une **politique** de sécurité est l'ensemble **d'objectifs** de **sécurité** d'une entreprise, incluant les **règles** de comportement des utilisateurs et des administrateurs et spécifiant la configuration système requise.
  - Ces objectifs, ces règles et ces exigences assurent ensemble la sécurité du réseau, des données et des systèmes informatiques d'une entreprise.
- **Les normes** permettent à l'équipe informatique de préserver la cohérence de fonctionnement du réseau.
  - Elles assurent la conformité des technologies requises par les utilisateurs et programmes spécifiques, ainsi que des programmes ou critères requis par une entreprise.
- **Les directives** sont une liste de suggestions expliquant comment opérer de manière plus efficace et sécurisée. Ils s'apparentent à des normes, mais sont plus flexibles et généralement pas obligatoires.
  - Des directives définissent la manière dont les normes sont développées et garantissent leur conformité aux politiques de sécurité générales.
- **Les documents de la procédure** sont plus longs et plus détaillés que les normes et les directives.
  - Les documents de la procédure englobent des informations sur l'implémentation qui contiennent habituellement des instructions pas-à-pas et des graphiques.

Les mesures de cybersécurité

Politiques

- Une **politique** de **sécurité définit** les **objectifs de sécurité**, les **règles** de **comportement** et les **exigences système** à respecter.

- Une **politique** de sécurité **exhaustive** porte sur **plusieurs points** :
  - Elle montre **l'engagement** de l'entreprise envers la sécurité.
  - Elle définit les **règles** relatives au comportement attendu.
  - Il assure la **cohérence** des opérations du système et de l'acquisition, de l'utilisation et de la maintenance des logiciels et du matériel.
  - Elle définit les **conséquences** juridiques des infractions.
  - Elle garantit au personnel de sécurité le **soutien** de la direction.

- Les politiques de sécurité **informent** les **utilisateurs**, le **personnel** et les **responsables** des **exigences** de l'organisation, qui protègent les actifs technologiques et informationnels.

- Une politique de sécurité spécifie également les **mécanismes** requis pour répondre aux exigences en matière de sécurité.

Les mesures de cybersécurité

Politiques (suite)

Une politique de sécurité comprend habituellement :

Politiques d'identification et d'authentification	Spécifier les personnes autorisées qui peuvent avoir accès aux ressources du réseau et décrire les procédures de vérification pour ces utilisateurs.
Politiques de mot de passe	Assurez-vous que les mots de passe répondent aux exigences minimales et sont changés régulièrement.
Les règles de bon usage	Identifier les ressources et l'utilisation du réseau qui sont acceptables pour l'organisation. Elles peuvent également identifier les conséquences d'une infraction.
Politiques d'accès à distance	Identifier comment les utilisateurs distants peuvent accéder à un réseau et ce qui est accessible à distance.
Politiques de maintenance du réseau	Spécifier les systèmes d'exploitation des périphériques réseau et les procédures de mise à jour des applications de l'utilisateur final.
Politiques de traitement des incidents	Décrire comment les incidents de sécurité doivent être traités.

- La règle d'utilisation acceptable est l'une des composantes les plus courantes de la politique de sécurité.
- Cette règle définit les autorisations des utilisateurs au niveau des divers composants système.

Les mesures de cybersécurité

Standards

- Les **normes** aident le personnel informatique à **maintenir** une **cohérence** dans **l'exploitation** du réseau.
- Les politiques de sécurité informent les utilisateurs, le personnel et les responsables des exigences de l'organisation en matière de protection des technologies et des informations.
- La cohérence est l'un des principes de sécurité les plus importants.
- Chaque organisation développe des normes qui soutiennent son environnement opérationnel unique.
- La politique de mot de passe d'une entreprise en est un exemple.
  - **Par exemple**, la norme pourrait stipuler que les mots de passe doivent comporter un minimum de huit caractères alphanumériques majuscules et minuscules, dont au moins un caractère spécial.
  - En outre, la politique relative aux mots de passe peut spécifier que les utilisateurs doivent modifier leur mot de passe tous les 30 jours.
  - Un historique des 12 mots de passe les plus récents peut être conservé afin d'éviter que quiconque réutilise les mêmes mots de passe au cours d'une période de 12 mois.

Les mesures de cybersécurité

Conseils

- Les directives détaillent une liste de suggestions visant à effectuer les opérations de manière plus efficace et plus sécurisée.

- Des directives définissent la manière dont les normes sont développées et garantissent leur conformité aux politiques de sécurité générales.

- Outre les bonnes pratiques définies par l'entreprise, des directives sont disponibles auprès des sources suivantes :
  - Centre de ressources sur la sécurité informatique du National Institute of Standards and Technology (NIST).
  - Guides de configuration de la sécurité de l'Agence nationale de sécurité (NSA).
  - La norme Critères communs.

2.5 Résumé de la deuxième partie

Résumé de la deuxième partie

Résumé

- Au cours de ce chapitre, nous avons évoqué les trois dimensions du cube magique de la cybersécurité.
- La principale responsabilité d'un responsable de la cybersécurité est de protéger les systèmes et les données d'une entreprise.
- Nous avons expliqué comment chacune de ses trois dimensions apporte sa pierre à l'édifice.
- Au cours de ce chapitre, nous avons aussi expliqué comment les professionnels de la sécurité utilisent les contrôles pour identifier les technologies, les appareils et les produits nécessaires à la protection de l'entreprise.