CHAPITRE 1

Fiche savoirs technologiques 1

La typologie des risques et leurs impacts

I Définitions de vulnérabilité, menace et risque

Vulnérabilité	Menace	Risque
En informatique, une vulnérabilité est une faiblesse de la sécurité du système d'information (SI) qui peut affecter son fonctionnement normal.	Une menace est une cause intentionnelle ou non-intentionnelle qui peut entraîner des dommages sur le SI.	Un risque de sécurité du SI est la probabilité de l'exploitation d'une vulnérabilité du SI par une menace. Le niveau d'un risque est estimé en fonction de sa gravité et de la vraisemblance de son apparition.

Les objectifs de la sécurité informatique consistent à limiter les vulnérabilités du SI.

II La typologie des risques informatiques

1. La méthode EBIOS

> EBIOS Risk Manager : www.lienmini.fr/6988-104
> Fiche méthode 5, p. 211

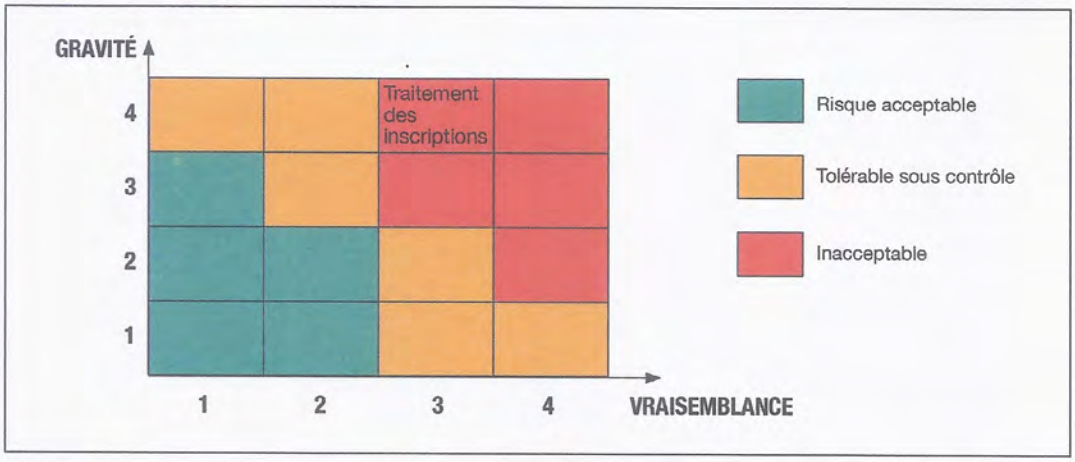
La méthode EBIOS Risk Manager (Expression des besoins et identification des objectifs de sécurité) développée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et retenue par la CNIL (Commission nationale de l'informatique et des libertés) permet d'identifier et de hiérarchiser les différents risques dans un contexte clairement défini.

Un risque est défini par l'ANSSI comme « un scénario qui combine un événement redouté et un ou plusieurs scénarios de menaces ». Un événement redouté désigne par exemple la possibilité d'atteindre des données avec des conséquences probables sur la vie privée des personnes concernées.

2. L'évaluation des risques

L'évaluation des impacts des risques informatiques est réalisée par le croisement de son niveau de vraisemblance et de gravité.

Exemple de cartographie des risques



La vraisemblance reflète la probabilité ou la possibilité que l'un des modes opératoires de l'attaquant aboutisse à l'objectif visé. Elle dépend des vulnérabilités des supports face aux menaces et des capacités des sources de risque à les exploiter.

La gravité évalue l'enjeu d'un événement redouté sur des « valeurs métier », c'est-à-dire stratégiques pour l'organisation (informations confidentielles, processus métier, matériels, logiciels, etc.).

Exemple de mesure de la gravité

Valeur métier	Évènement redouté	Impacts	Gravité
Facturation	Altération des informations sur les factures	• Impossibilité de recevoir un paiement • Perte de crédibilité • Impossibilité de remplir les obligations légales	G3 - Grave

III Les impacts des risques informatiques

L'ANSSI, au travers de sa méthode EBIOS, identifie différentes catégories d'impacts.

Impacts sur les missions et les services de l'organisation	Conséquences directes ou indirectes sur la réalisation des missions et services.
Impacts humains, matériels ou environnementaux	• **Impacts sur la sécurité ou sur la santé des personnes :** conséquences sur l'intégrité physique de personnes. • **Impacts matériels :** dégâts matériels ou destruction de biens supports. • **Impacts sur l'environnement :** conséquences écologiques à court ou long terme.
Impacts sur la gouvernance	• **mpacts sur la capacité de développement ou de décision :** conséquences sur la liberté de décider, de diriger, de mettre en œuvre la stratégie de développement. • **Impacts sur le lien social interne :** conséquences sur la qualité des liens sociaux au sein de l'organisation. • **Impacts sur le patrimoine intellectuel ou culturel :** conséquences sur les connaissances non-explicites accumulées par l'organisation sur le savoir-faire, les capacités d'innovation, les références culturelles communes.
Impacts financiers	Conséquences pécuniaires.
Impacts juridiques	Conséquences suite à une non-conformité légale, réglementaire, normative ou contractuelle.
Impacts sur l'image et la confiance	Conséquences sur l'image de l'organisation, la notoriété, la confiance des clients.

> Voir lexique BTS SIO, p. 221

CHAPITRE 1

Fiche savoirs technologiques 2

Les principes de la sécurité

La sécurité des systèmes d'information repose sur quatre principes fondamentaux :

I La confidentialité

La **confidentialité** vise à assurer que les données ne sont accessibles qu'aux seules personnes autorisées.

Exemple : la connexion d'un utilisateur au réseau de l'organisation par son identifiant et son mot de passe personnel ne donne accès qu'aux données qu'il est autorisé à consulter ou à modifier.

II La disponibilité

La **disponibilité** doit rendre les données accessibles et utilisables par les personnes autorisées sans interruption.

Exemple : la redondance des connexions réseaux permet d'accéder aux données de manière continue, même si une connexion est rompue.

III L'intégrité

Le principe d'**intégrité** s'assure que les données ne peuvent pas être modifiées pendant leur transfert, leur traitement ou leur stockage.

Exemple : des protocoles de cryptage, comme le protocole SSL, permettent de s'assurer que les données ne sont pas modifiées pendant leur transfert sur le réseau.

IV La preuve

Le principe de non-répudiation consiste à apporter la preuve non réfutable d'un acte malveillant. La non-répudiation est assurée par la combinaison de trois éléments : l'authentification, l'imputabilité et la traçabilité.

Authentification	Imputabilité	Traçabilité
L'authentification permet de s'assurer de la légitimité de la demande d'accès, et d'accorder les droits associés à celle-ci. La saisie d'un identifiant et d'un mot de passe peut être une solution d'authentification.	L'imputabilité désigne la possibilité d'attribuer la responsabilité d'un acte à une personne clairement identifiée.	La traçabilité permet de fournir un historique de l'utilisation d'un système d'information pour disposer d'une preuve des actions menées sur des données.

Exemple : en cas d'action malveillante sur un service informatique de l'organisation, le fichier de journalisation (*log*) doit permettre de prouver qui est intervenu et sur quel service, afin d'apporter la preuve de l'acte.

CHAPITRE 1

Fiche savoirs technologiques 3

Sécurité et sûreté

I Définitions

La sûreté vise à prévenir les risques et conséquences d'un événement accidentel ou involontaire.

La sécurité consiste à prévenir les actes de malveillance en combinant des moyens humains, techniques et organisationnels. Cette notion est souvent englobée dans le terme de sûreté informatique. Elle doit permettre de faire face aux risques de vol de données, d'intrusion dans le système informatique, ou d'effectuer la recherche de dégradation de service du SI.

II Les périmètres respectifs

1. Le périmètre de la sûreté informatique

a. Les menaces non intentionnelles

Le périmètre de la sûreté informatique englobe les menaces non intentionnelles qui sont, par définition, peu prévisibles et non-volontaires.

b. Les types de menaces

Menace d'accident naturel	Menace humaine	Menace liée au matériel
Un risque naturel (orage, inondation, etc.) est un élément imprévu ou difficilement prévisible qui peut être dangereux lorsqu'il impacte une vulnérabilité du SI.	L'erreur humaine, la maladresse ou la négligence peuvent mettre à jour une faiblesse du SI et mettre en échec sa stabilité.	Le choix du matériel informatique peut rendre plus ou moins vulnérable le SI. La réduction de certains coûts d'acquisition peut être source de menaces pour le SI.

2. Le périmètre de la sécurité informatique

a. Les menaces délibérées

Le périmètre de la sécurité informatique regroupe les menaces délibérées qui proviennent de personnes malveillantes, et qui peuvent nuire au SI. Ces personnes sont internes ou externes à l'organisation, et disposent de capacités plus ou moins importantes dans les possibilités de détérioration du SI, selon leur niveau de compétence technique et leurs droits d'accès au SI.

b. Les catégories d'attaquants

D'après l'ANSSI, les profils des attaquants peuvent être regroupés selon trois grandes catégories :

- les organisations structurées guidées par une logique d'efficacité et de gain disposant de moyens sophistiqués et conséquents, voire quasi illimités (États, crime organisé) ;
- les organisations ou groupes guidés par une motivation idéologique disposant de moyens significatifs mis en œuvre de façon relativement coordonnée (terroristes, activistes) ;
- les attaquants disposant de moyens limités mais spécialisés (individus isolés, groupes d'individus).

3. Les principaux types de menaces

Quatre principaux types de menaces sont mis en avant par l'ANSSI : la déstabilisation, l'espionnage, le sabotage et la cybercriminalité.

Menaces	Types d'attaques
Déstabilisation	• Déni de service : action qui rend un service inaccessible, par l'envoi d'une multitude de requêtes vers un serveur pour provoquer sa panne ou sa dégradation. • **Défiguration** : ajout ou remplacement des pages d'un site Web afin de revendiquer un message idéologique. • **Divulgation de données** : récupération de données confidentielles d'une organisation en exploitant une vulnérabilité du réseau informatique.
Espionnage	• **Attaque par « point d'eau » (*wateringhole*)** : infection du site Internet d'une organisation pour contaminer les ordinateurs des visiteurs, afin d'accéder au réseau de l'organisation. • **Attaque par hameçonnage ciblé (*spearfishing*)** : usurpation de l'identité d'une personne connue du destinataire pour envoyer un message ciblé à un membre d'une organisation, afin de lui faire ouvrir une pièce jointe malveillante qui permettra d'accéder au réseau de l'organisation.
Sabotage	Les modes d'attaques sont nombreux, mais ils visent tous à créer une panne dans un périmètre ou sur l'ensemble du système d'information d'une organisation.
Cybercriminalité	• **Rançongiciel (*ransomware*)** : données confidentielles rendues inaccessibles jusqu'au paiement d'une rançon. Le chantage peut parfois toucher des données gênantes, que l'on menace de rendre publiques sur Internet. • **Hameçonnage (*phishing*)** : action visant à tromper un utilisateur pour l'inciter à communiquer des données personnelles, souvent des données bancaires. Les formes peuvent être diverses, telles que l'utilisation des réseaux sociaux, un courriel ou encore un SMS.

D'après www.ssi.gouv.fr

Fiche savoirs technologiques 4

La sécurité des terminaux utilisateurs et de leurs données

I Définition

Sécuriser un terminal utilisateur et ses données implique de :
- réaliser des configurations système qui permettent de se protéger des attaques ;
- installer des applications et des matériels qui empêchent toute intrusion ;
- définir avec les utilisateurs les bonnes pratiques à adopter.

II La configuration du système : quelques règles à respecter

Système d'exploitation	– Configurer les mises à jour automatiques – Installer les correctifs et les [redacted]
Applications	– Autoriser les applications vérifiées ([redacted]) – Isoler les applications obsolètes – Interdire les téléchargements de sources inconnues – Limiter les modules optionnelles
Exécution automatique	Désactiver les ports et lecteurs
***Boot* sur périphériques externes**	Désactiver le *boot* et insérer un mot de passe

III Les applications et matériels spécifiques

Antivirus	Logiciel chargé de détecter et de stopper les *malwares* connus : virus, vers, *keylogger*, chevaux de Troie, etc. Il fonctionne avec une [redacted] qui contient les signatures des *malware* connus. **Exemples :** Bitdefender, Avast, Norton, Kapersky.
Antispam	Le *spam* (ou courriel indésirable, ou pourriel) est une communication électronique non sollicitée. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. **Exemples :** Altospam, Postbox, McAfee.
Pare-feu (*firewall*)	Il inspecte les paquets réseaux entrants et sortants et implémente un mécanisme de filtrage basé sur des règles. Il ne transmet pas les paquets qui ne les respectent pas. On distingue les pare-feux matériels (pour un réseau) et les pare-feux logiciels (pour un poste de travail). **Exemples :** Sophos, Stormshield, ZoneAlarm.
Coffre-fort numérique (ou portefeuille de mots de passe)	Il permet de centraliser ses mots de passe en les protégeant par un seul mot de passe fort. **Exemples :** KeyPass ou 1Password.
Système d'authentification unique (en anglais *Single Sign-On*, SSO)	Un seul formulaire d'authentification permet d'accéder à l'ensemble des services de sa session utilisateur.
Mobile Device Management (« gestion des terminaux mobiles »)	Application qui permet la gestion d'une flotte d'appareils nomades. Son objectif est d'harmoniser les outils numériques avec des programmes et applications à jour et une sécurité correcte (présence d'un antivirus ou autre dispositif de sécurisation contre les *malwares*).

> Voir lexique BTS SIO, p. 221

IV La promotion des bonnes pratiques

1. L'authentification

L'**authentification** permet de protéger le SI contre les attaques par dictionnaire, force brute, **table arc-en-ciel**.

Recommandations ANSSI pour obtenir une authentification forte	
R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.)
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.
+	**Choix du mot de passe :**
Au moins 12 caractères de types différents, idéalement une **passphrase** (passe de phrase ou phrase secrète). Pour cela deux méthodes : • La méthode phonétique : « J'ai acheté huit CD pour cent euros cet après-midi » deviendra : ght8CD%E7am. • La méthode des premières lettres : la citation « un tient vaut mieux que deux tu l'auras » donnera : 1tvmQ2tl'A.	
+	**Authentification à double facteurs :**

Quelque chose que je sais	Quelque chose que je possède	Quelque chose que je suis
• Mot de passe • Tracé de verrouillage	• *One time password* : mot de passe temporaire Exemple : Token SafeNet	Empreinte biométrique

www.ssi.gouv.fr.

2. Les bons usages sur Internet

Navigateurs	• Utiliser des protocoles SSL/TLS. • Effacer l'historique de navigations, les fichiers temporaires, les **cookies**.
Accès Internet	Un proxy (serveur mandataire) est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour éviter les sites malveillants. Il permet : • l'authentification des utilisateurs et la journalisation des requêtes ; • la mise en cache des pages consultées sur Internet afin d'accélérer les navigations, la mise en place de pare-feux ; • la sécurité par filtrage des paquets (entrant/sortant).
Courriels	• Désactiver l'exécution des liens hypertextes et l'affichage des images. • Être très vigilant avec les courriels dont les émetteurs sont inconnus et avec certains types de contenus. • Marquer les indésirables comme tels afin d'affiner la politique de détection des *spams*. • Si besoin, créer une adresse poubelle.

> Voir lexique BTS SIO, p. 221

Fiche savoirs technologiques 5

Les authentifications, privilèges et habilitations des utilisateurs

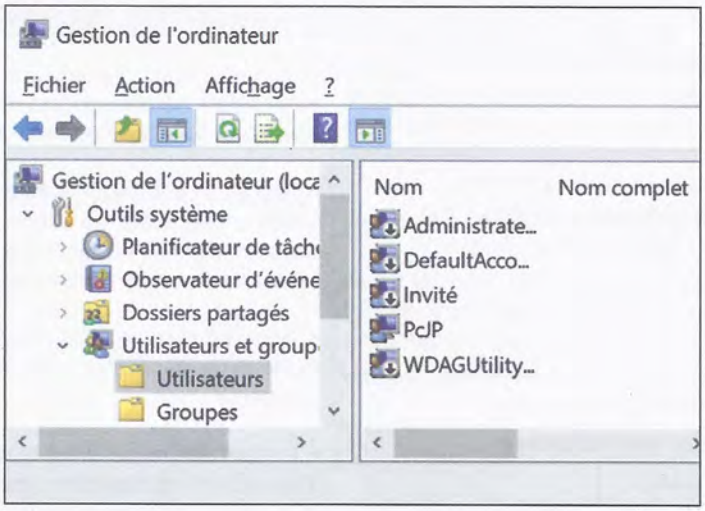
I Les principes de l'authentification et de l'habilitation

Authentification	Habilitation
Processus qui permet de vérifier si l'utilisateur est bien celui qu'il prétend être. • Elle permet de vérifier et de prouver l'identité d'un utilisateur qui veut ouvrir une session dans un SI, et de lui accorder les droits d'accès inhérents à son compte. • Elle s'appuie sur l'utilisation d'un identifiant (*login*) et d'un mot de passe (*password*). • Elle repose sur un compte utilisateur local ou un compte utilisateur sur un gestionnaire de domaine, comme *Active Directory*.	**Processus qui permet de savoir si un utilisateur a accès à une ressource ou non.** • Elle inclut l'autorisation, l'accréditation, les droits d'accès ou encore le contrôle d'accès. • Elle donne la permission à un utilisateur de réaliser des actions sur des ressources du SI : droit de consultation, droit de création, droit de modification, droit de suppression, etc. • Elle dépend des privilèges accordés. Le privilège est la délégation d'autorité sur un fichier ou un dossier dans un SI.

II Les techniques d'authentification

1. Le compte local

L'accès à un poste de travail s'effectue par des comptes utilisateurs. Ces comptes peuvent être nominatifs (chacun est associé à une seule personne) ou collectifs (des comptes sont associés à plusieurs personnes). Par défaut, le compte administrateur et le compte invité sont créés. L'ensemble des comptes locaux et des mots de passe sont stockés (sous forme d'empreintes numériques) dans la base SAM (Security Accounts Manager - %SystemRoot%\System32\Config\SAM).

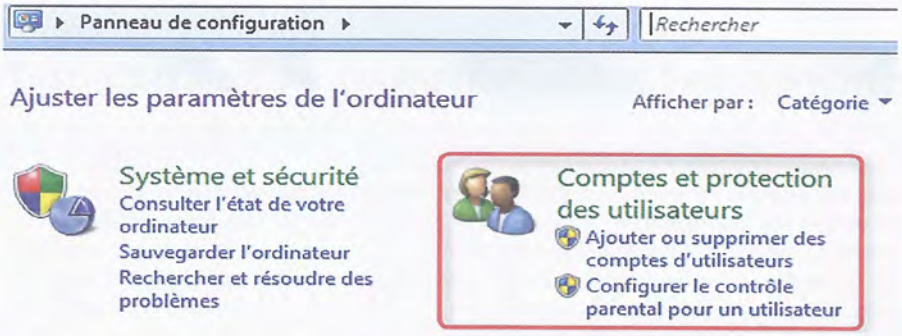


2. Les comptes itinérants

Les authentifications centralisées sur un contrôleur de domaine s'effectuent grâce à l'annuaire LDAP (*Lightweight Directory Access Protocol*) et au protocole Kerberos (protocole réseau d'authentification reposant sur un chiffrement symétrique et un système de tickets).

› Voir lexique BTS SIO, p. 221

III Les techniques d'habilitations associées aux comptes utilisateurs



Les **comptes administrateurs** (ou superutilisateurs) possèdent les privilèges les plus élevés. Ils ont un contrôle total sur l'ensemble des ressources du SI. Ces comptes sont par ailleurs habilités à créer, modifier et supprimer d'autres comptes.
Les **comptes utilisateurs** n'ont pas la possibilité de réaliser des opérations privilégiées, ni de créer des comptes. Ils peuvent cependant configurer le système et installer certains logiciels.
Les **comptes invités** sont des comptes génériques aux droits très restreints. Ils ne peuvent pas installer des logiciels et n'ont pas accès aux répertoires contenant des informations sensibles. Chaque compte utilisateur appartient à un groupe d'utilisateurs qui définit, par défaut, ses droits d'accès ou privilèges.

IV Les bonnes pratiques en matière d'authentification et d'habilitation

Authentification	Habilitation (valable pour l'ensemble des comptes)
Compte administrateur	• Respecter le principe « du besoin d'en connaître » : habilitations nécessaires à la réalisation des tâches inhérentes à l'activité de l'utilisateur. • Respecter le principe « du moindre privilège » : mettre en place des habilitations strictement nécessaires aux activités liées à chaque compte. Ce principe ne doit pas être supérieur au « besoin d'en connaître ». • Gérer efficacement les mobilités : éviter l'accumulation des habilitations (fonctions successivement occupées). • Réaliser une revue annuelle des habilitations afin d'identifier et de supprimer les comptes non utilisés ou qui n'ont plus lieu d'exister. • Mettre en place des procédures d'attributions des habilitations à appliquer systématiquement à l'arrivée ainsi qu'au départ ou au changement d'affectation d'un utilisateur du SI. • Définir des mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès.
• Utiliser des comptes d'administration dédiés et non partagés entre différents utilisateurs : l'administrateur doit disposer de plusieurs comptes d'administration distincts selon les tâches qu'il doit réaliser. • Protéger (confidentialité et intégrité) l'accès aux annuaires des comptes administrateurs. • Ne pas autoriser l'ouverture de sessions de travail (activités qui ne sont pas de l'ordre de l'administration) sur des postes réservés aux actions d'administration. • Attribuer des droits d'administration à des groupes plutôt qu'à des utilisateurs individuels.	
Compte utilisateur	
• Doit être nominatif. • Ne pas utiliser de comptes partagés entre plusieurs utilisateurs. • Donner accès seulement aux données nécessaires aux activités et restreindre l'accès aux répertoires contenant des données sensibles. • Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour. • Ne pas donner accès aux disques et aux applications sensibles aux utilisateurs visiteurs.	

> Voir lexique BTS SIO, p. 221

Fiche savoirs technologiques 6

La gestion des droits d'accès aux données

Le contrôle d'accès précise qui (utilisateur) est autorisé à faire quoi (lectures, écritures, suppressions, modifications, etc.) sur quelles données.

I Les principes de la gestion des droits d'accès aux données

Elle a pour but de limiter les actions qui peuvent être réalisées sur les données (fichiers et dossiers), l'utilisation des applications et la gestion du système.
Le principe est de restreindre les privilèges des différents utilisateurs.

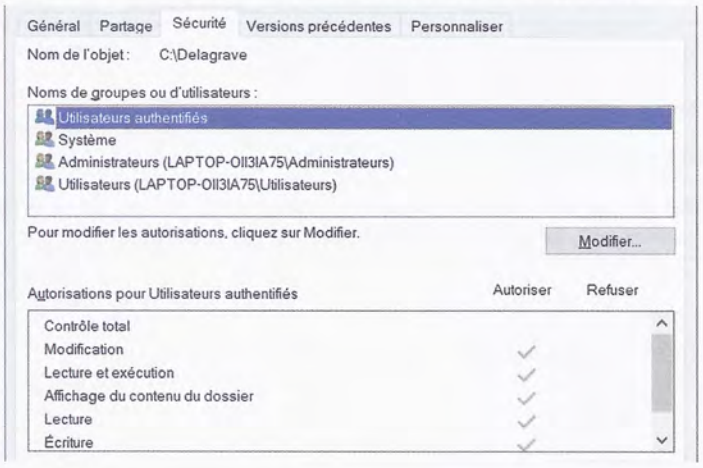
Exemple sous UNIX : la commande **ls -al** affiche les droits sur les fichiers et les répertoires, représentés par les lettres ci-dessous :

r - read	Lire un fichier/lister un répertoire
w – write	Ajouter, supprimer, modifier un fichier dans un répertoire
X – execute	Exécuter un fichier / traverser un répertoire

Droits	Utilisateurs	Ressources concernées
-rwxr-x---	1 root	apple.exe
drw-r-----	1 brows	Reports
-rw-rw-r--	1 darkness	gold.txt

La commande **chmod** munie des opérateurs **+**, **-**, **u**, permet de modifier et de changer les droits d'accès.

Exemple sous Windows : les droits d'accès s'appuient sur le système de fichiers NTFS pour pouvoir mettre en œuvre un modèle de moindre privilège grâce à des listes de contrôle d'accès (ACL). La gestion des autorisations se fait à partir de l'onglet « Sécurité » de chaque dossier ou fichier :



Les différents privilèges sont :
- l'accès au contenu du répertoire (Afficher le contenu du dossier) ;
- la lecture des fichiers, de leurs propriétés et de leurs répertoires (Lecture) ;
- l'exécution des programmes et des scripts (Lecture et exécution) ;
- l'écriture dans les fichiers et l'ajout des fichiers dans les répertoires (Écriture) ;
- l'affichage, la modification, la suppression des fichiers et répertoires (Modifier) ;
- tous les droits (Contrôle total) habituellement réservés à l'administrateur : modification, ajout, déplacement ou suppression des fichiers et répertoires ;
- la modification des paramètres des autorisations pour tous les autres utilisateurs.

> Voir lexique BTS SIO, p. 221

II Les outils de la gestion des droits d'accès aux données

Différents modèles de gestion des droits d'accès sont possibles au sein d'un système d'information, mais leur finalité est la même : ne permettre l'accès et la modification des données qu'aux personnes autorisées. Les deux principaux modèles sont :

DAC ***(Discretionary Access Control)*** **Contrôle d'accès discrétionnaire**	**RBAC** ***(Role-Based Access Control)*** **Contrôle d'accès basé sur des rôles**
Le créateur d'une ressource est le propriétaire de celle-ci. Il fixe alors la politique de contrôle d'accès de cette ressource : il décide quel utilisateur peut réaliser quelle action. **Exemple :** En tant que propriétaire du fichier paie.xls, j'autorise uniquement Alice à lire le fichier.	Il convient de définir tout d'abord des rôles qui représentent un ensemble de privilèges. Les utilisateurs sont affectés à un rôle et héritent donc des droits inhérents à celui-ci. **Exemple :** Le rôle RH donne les droits d'accès en lecture et en écriture au fichier paie.xls. On attribue le rôle à Bob, qui pourra donc modifier le fichier.
Ce modèle de gestion est décentralisé. Il correspond à l'attribution de droits par un compte local sur un poste de travail.	Ce modèle de gestion est centralisé, comme dans un *Active Directory* où les utilisateurs appartiennent et héritent des groupes.

III La gestion dans le cadre d'un *Active Directory*

Dans un *Active Directory* (gestion centralisée des utilisateurs), des groupes de sécurité sont prédéfinis pour attribuer des droits particuliers aux différents comptes (utilisateurs) créés. Ci-dessous, un exemple de groupes présents dans l'*Active Directory* :

Administrateurs	Accès complet et illimité à l'ordinateur promu du domaine
Administrateur du domaine	Droits sur tous les objets du domaine et administration du domaine
Opérateurs de comptes	Création, modification et suppression des objets locaux
Utilisateurs du domaine	Groupe par défaut de tout nouvel utilisateur
Invité du domaine	Inclut le compte invité du domaine. Lorsque les membres de ce groupe se connectent, un profil de domaine est créé sur l'ordinateur

Fiche savoirs technologiques 7

La sécurité des communications numériques

La sécurisation des communications (acheminements des données) dans un réseau local implique l'utilisation de protocoles spécifiques et la mise en œuvre d'infrastructures réseaux particulières pour segmenter (diviser) de façon logique et physique le réseau interne.

I Le protocole de sécurisation des communications

Un protocole est un ensemble de règles à suivre pour établir une communication dans un réseau informatique. La communication peut être sécurisée en utilisant des protocoles spécifiques :

- le **protocole 802.1x** : c'est une solution standard de sécurisation des réseaux mise au point par l'IEEE (*Institute of Electrical and Electronics Engineers*, Institut des ingénieurs électriciens et électroniciens). Il s'appuie sur le protocole AAA (*Authentification, Authorization, Accounting/Auditing*), un modèle de sécurité qui a trois fonctions : authentification, autorisation et traçabilité. Il permet à un utilisateur souhaitant accéder à un réseau de s'authentifier grâce à un serveur central d'authentification ;
- le **protocole EAP** (*Extensible Authentication Protocol*) : il permet la demande d'autorisation de connexion au serveur (support universel permettant le transport de différentes méthodes d'authentifications) ;
- le **protocole SSH** (*Secure Shell*) : il permet d'administrer les matériels d'interconnexion, les administrateurs réseaux. Il impose un échange de clés secrètes de chiffrement en début de connexion.

II La segmentation et les restrictions logiques des réseaux

Segmenter un réseau permet de diviser celui-ci en plusieurs sous-réseaux et, ainsi, d'imposer des règles supplémentaires pour autoriser les communications.

1. Les sous-réseaux IP

Dans un réseau local, les hôtes sont identifiés par des adresses IPv4 privées constituées de 4 octets de 8 bits. Une adresse est composée d'une partie réseau, qui définit le réseau d'appartenance de l'hôte, et d'une partie hôte, qui identifie l'hôte dans son réseau. Tous les hôtes d'un même réseau peuvent communiquer entre eux : on parle de domaine de diffusion. Cependant, les hôtes appartenant à des réseaux différents ne peuvent pas s'échanger des informations directement : ils doivent utiliser une passerelle.

2. Les VLANs

Un VLAN (*Virtual Local Area Network*) décrit un réseau local virtuel. Son objectif est de regrouper de façon logique et indépendante un ensemble d'hôtes. Il permet de créer des domaines de diffusion gérés par les commutateurs indépendamment de l'emplacement géographique où se situe le nœud. On distingue trois types de VLANs :

- le **VLAN de niveau 1** : on affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est alors déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN ;
- le **VLAN de niveau 2** : on affecte manuellement chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par son adresse MAC. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation ;
- le **VLAN de niveau 3** : on affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est alors déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise.

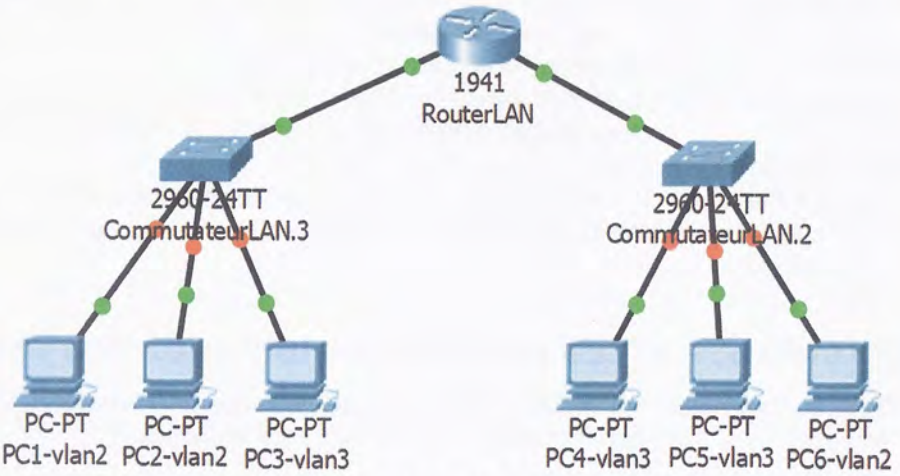
> Voir lexique BTS SIO, p. 221

III La segmentation et les restrictions physiques des réseaux

Un réseau informatique est constitué d'équipements d'interconnexion permettant de répartir de façon physique et logique (sous-réseau IP et VLANs) les différents hôtes du LAN.

1. Les commutateurs

Sans VLAN, un commutateur (*switch*, en anglais) considère que toutes ses interfaces sont dans le même LAN et le même domaine de diffusion. Avec la mise en place de VLANs, un commutateur place ses interfaces dans des sous-réseaux et domaines de diffusion différents. Un commutateur a alors plusieurs séparations logiques sur un même support physique.



Par défaut, sans configuration précise, les ports d'un commutateur sont dans le VLAN 1. L'administrateur réseau doit donc configurer chaque port du commutateur dans un VLAN particulier (par exemple, avec un commutateur Cisco : Switch port mode acces vlan 2). Pour permettre la communication entre des VLANs différents, il faut configurer un port en mode trunk (norme 802.1q) et relier ce port au routeur pour assurer le routage intervlan.

2. Les routeurs

Les routeurs (ou passerelles) sont des équipements réseaux permettant de relier différents réseaux qui n'appartiennent pas au même réseau logique afin qu'ils puissent échanger des données. Pour acheminer les données vers les bons réseaux, le routeur dispose d'une table de routage qui lui indique la route à suivre. Dans un réseau local, le routeur, par l'intermédiaire de règles de sécurité, achemine ou non les informations vers différents réseaux internes. Cela permet ainsi d'instaurer une sécurité supplémentaire, qui ne permet pas le relais des trames de diffusion. Par exemple, avec un routeur Cisco, l'administrateur peut configurer des ACL (*Access Control Lists*) qui constituent des règles de filtrage sur chaque interface. On distingue les ACL standards, qui servent à filtrer les paquets uniquement sur les IP sources, et les ACL étendues, qui permettent de filtrer sur quasiment tous les champs des en-têtes IP, TCP et UDP.

Exemple : deny 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

Le réseau 192.168.1.0 /24 ne pourra pas communiquer avec le réseau 192.168.3.0 /24. Les paquets seront alors détruits au niveau du routeur.