Version expérimentale
En cours de validation

RÉSUMÉ THÉORIQUE – FILIÈRE SYSTÈMES ET RÉSEAUX

M206 – SÉCURISER UNE INFRASTRUCTURE DIGITALE

45 heures

SOMMAIRE

SOMMAIRE

Sécuriser une infrastructure digitale

Dans ce module, vous allez :

- Découvrir les notions de base de la sécurité
- Identifier et classifier les menaces, les risques et les attaques de sécurité d'un système d'information
- Savoir sécuriser un système d'information selon les recommandations et les standards reconnus
- Savoir analyser et gérer les incidents efficacement
- Maitriser les techniques de filtrage et de contrôles d'accès
- Maitriser les techniques de sécurité d'un réseau
- Comprendre les principe des algorithmes cryptographiques
- Comprendre le principe de fonctionnement d'une infrastructure PKI de gestion de certificats numériques

75 heures

Sécuriser une infrastructure digitale

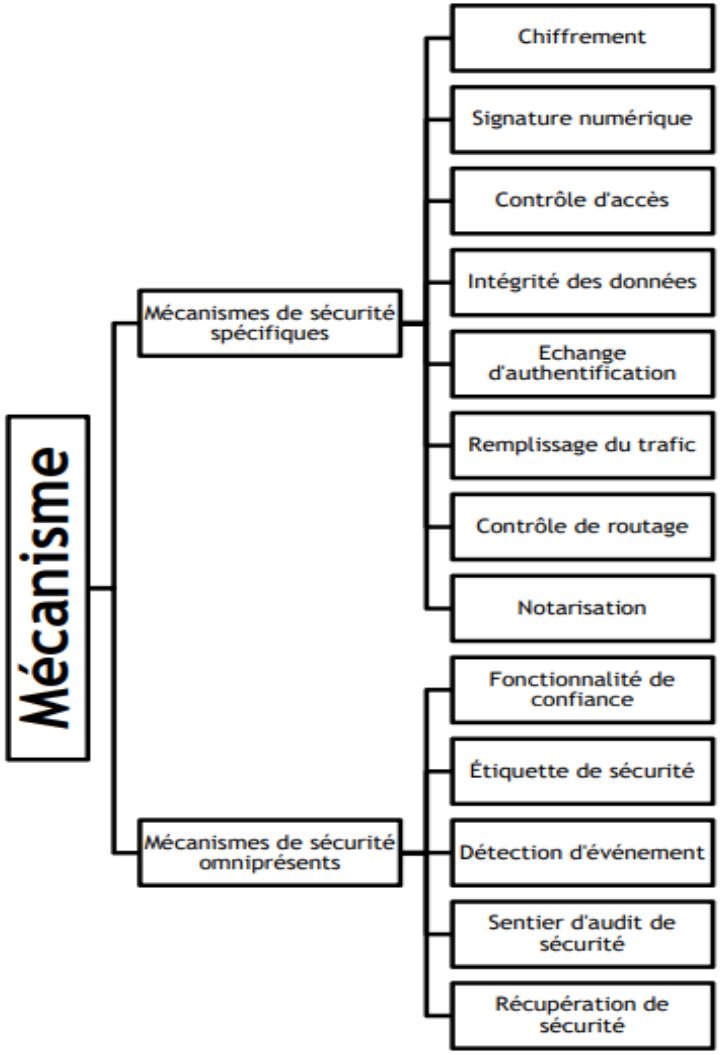
1. **Les bases de la sécurité informatique**
2. Les réglementations juridiques
3. La gestion des risques et d'incidents
4. Sécurité réseaux
5. Les listes de contrôle d'accès
6. La cryptographie
7. Infrastructure PKI

- Sigles scientifiques et mise en évidence des notions de sécurité informatique

- Le marché de la sécurité informatique a connu une croissance significative. L'entreprise Gartner1 s'attend à ce que le marché de la cybersécurité dépasse les 100 milliards de dollars en 2019 contre 76 milliards de dollars en 2015. Pour évaluer efficacement les besoins de sécurité d'une organisation et choisir divers produits et politiques de sécurité, le responsable de la sécurité a besoin d'un moyen systématique lui permettant de définir les exigences en matière de sécurité. L'architecture de sécurité OSI est utile aux gestionnaires pour organiser la tâche de sécurité. Elle a été développée en tant que norme internationale. Les fournisseurs d'ordinateurs et de communications ont développé des fonctionnalités de sécurité pour leurs produits et services qui se rapportent à cette définition structurée de services et de mécanismes.

L'architecture de sécurité se concentre sur les attaques de sécurité, les mécanismes et les services. Ceux-ci peuvent être définis brièvement comme suit :

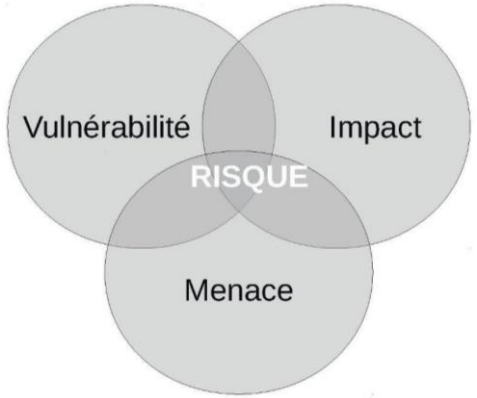
- **Attaque de sécurité :** toute action qui compromet la sécurité des informations appartenant à une organisation.
- **Mécanisme de sécurité :** un processus (ou un périphérique incorporant un tel processus) conçu pour détecter, prévenir ou récupérer une attaque de sécurité.
- **Service de sécurité :** un service de traitement ou de communication qui améliore la sécurité des systèmes de traitement de données et les transferts d'informations d'une organisation. Les services sont destinés à contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité pour fournir le service.



PARTIE 1

Menaces, risques et vulnérabilités

- Les **menaces** contre le système d'information entrent dans l'une des catégories suivantes : atteinte à la disponibilité des systèmes et des données, destruction de données, corruption ou falsification de données, vol ou espionnage de données, usage illicite d'un système ou d'un réseau, usage d'un système compromis pour attaquer d'autres cibles.
- Les **menaces** engendrent des **risques** et des coûts humains et financiers : perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété. Les **risques** peuvent se réaliser si les systèmes **menacés** présentent des **vulnérabilités**. Il est possible de préciser la notion de risque en la décrivant comme le produit d'un préjudice par une probabilité d'occurrence : risque = préjudice × probabilité d'occurrence
- Cette formule exprime qu'un événement dont la probabilité à survenir est assez élevée, par exemple la défaillance d'un disque dur, mais dont il est possible de prévenir le préjudice qu'il peut causer par des sauvegardes régulières, représente un risque acceptable ; il en va de même pour un événement à la gravité imparable, comme l'impact d'un météorite de grande taille, mais à la probabilité d'occurrence faible. Il va de soi que, dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces : cela irait sans dire, si l'oubli de cette condition n'était très fréquent.
- Si la question de la sécurité des systèmes d'information a été radicalement bouleversée par l'évolution rapide de l'Internet, elle ne saurait s'y réduire ; il s'agit d'un vaste problème dont les aspects techniques ne sont qu'une partie. Les aspects juridiques, sociaux, ergonomiques, psychologiques et organisationnels sont aussi importants.



PARTIE 1

Objectifs et services de la sécurité

Véritable enjeu pour les entreprises, la **sécurité informatique** a pour mission d'assurer que les **ressources matérielles ou logicielles** d'une structure sont seulement utilisées dans leur cadre prévu. Avec l'essor des technologies et la digitalisation des outils professionnels, mais aussi les différentes réglementations sur la protection des données comme le RGPD, la cybersecurité devient plus que vitale pour les entreprises. Nous allons donc voir ensemble les **5 objectifs de la sécurité informatique** visant principalement à protéger les systèmes d'information et les données.

- **L'intégrité des données:** le premier **objectif de la sécurité informatique** vise à assurer l'**intégrité des données informatiques** : la data doit rester fiable et crédible durant tout son cycle de vie. La cybersecurité permet alors de garantir et de préserver **la validité et l'exactitude des données**. On distingue généralement deux types d'intégrité, dont les processus et méthodes peuvent varier : **l'intégrité physique** : protection de données uniques et exactes lorsqu'elles sont stockées et récupérées. **l'intégrité logique** : conservation inchangée des données au cours de leurs manipulations multiples au niveau d'une base de données relationnelle.
- **L'authenticité des identifiants: l'authentification** permet d'assurer l'identité d'un utilisateur grâce à l'usage d'un **code d'accès** : ici, l'**objectif de la sécurité informatique** est de garantir que chaque utilisateur est bien celui qu'il dit être. Le **contrôle d'accès**, par un mot de passe par exemple, permet de limiter la consultation ou l'utilisation de certaines ressources seulement aux personnes autorisées et de maintenir la confiance dans les relations d'échange. Petit point à noter : il ne faut pas confondre **identification** et **authentification**. La première représente l'**identifiant public**, tandis que la seconde correspond à un **élément secret** seulement connu de l'utilisateur. Ainsi, le mécanisme de sécurité fait correspondre l'identifiant public avec l'élément d'authentification afin de **garantir l'authenticité de l'identifiant**.
- **La confidentialité des données: t**roisième **objectif de la sécurité informatique**, et pas le moindre : la **confidentialité des données**. La mission est ici de maintenir une **non-divulgation des données** et/ou leur **non-accessibilité** aux personnes ou systèmes informatiques non autorisés. En effet, toutes les entreprises possèdent des informations importantes qu'elles souhaitent garder **confidentielles**, peu importe leur secteur d'activité. Elles concernent souvent l'entreprise elle-même, ses clients ou ses employés. À titre d'exemple, il peut s'agir de données du type :identifiants bancaires ;renseignements sur des produits ;informations contractuelles ;détail des processus de fabrication ;description des stratégies marketing et commerciales ;etc…

Objectifs et services de la sécurité

- **La non-répudiation des informations:** la **non-répudiation des informations** a pour but d'assurer que l'émetteur d'une information (quelle qu'elle soit) ne soit pas en mesure de nier qu'il est bien à l'origine de celle-ci. Pour répondre à cet **objectif de la sécurité informatique** et qu'il se concrétise, on utilise la signature des emails, des documents ou des certificats. Ainsi, seul l'utilisateur possédant une clé privée peut apposer sa signature sur un email. Cette personne ne peut donc pas nier en être l'émetteur.
- **La disponibilité des données: d**ernier **objectif de la sécurité informatique**, c'est la **disponibilité des données**. En plus de rester fiable et confidentielle, la data doit être accessible et disponible en permanence pour toutes les personnes avec un droit d'accès. Cela permet de ne pas être pénalisé en passant à côté d'informations cruciales pour une prise de décision ou bien ne pas pouvoir accomplir une tâche ou une fonction. Cet aspect de la **cybersecurité** est assez complexe, puisque cela exige une **étude minutieuse des droits d'accès** : certains utilisateurs ont des droits de consultation, d'autres de lecture et d'autres de modifications. Il faut donc bien arbitrer les différents accès afin de conserver une bonne confidentialité des données tout en facilitant leur consultation pour que l'entreprise reste compétitive.

Un service de sécurité est un service fourni par une couche de protocoles de systèmes ouverts communicants, qui assure une sécurité adéquate des systèmes ou des transferts de données. ces services se divisent en cinq catégories et quatorze services spécifiques.

- **L'authentification:** le service d'authentification est chargé d'assurer qu'une communication est authentique. Dans le cas d'un seul message, tel qu'un signal d'avertissement ou d'alarme, la fonction du service d'authentification est d'assurer au destinataire que le message provient de la source qu'il prétend être. Dans le cas d'une interaction continue, comme la connexion d'un terminal à un hôte, deux aspects sont impliqués. Tout d'abord, au moment de l'initiation de la connexion, le service garantit que les deux entités sont authentiques, c'est-à-dire que chacune est l'entité qu'elle prétend être. Deuxièmement, le service doit s'assurer que la connexion n'est pas entravée de telle sorte qu'un tiers peut se faire passer comme l'une des deux parties légitimes aux fins d'une transmission ou d'une réception non autorisée. Deux services d'authentification spécifiques sont définis: - Authentification par entité intermédiaire, - Authentification d'origine de données.
- **Contrôle d'accès:** dans le contexte de la sécurité du réseau, le contrôle d'accès permet de limiter et de contrôler l'accès aux systèmes hôtes et aux applications via les liaisons de communication. Pour ce faire, chaque entité qui tente d'accéder doit d'abord être identifiée ou authentifiée, de sorte que les droits d'accès peuvent être adaptés à l'individu.

Objectifs et services de la sécurité

- **Confidentialité des données:** la confidentialité est la protection des données transmises contre les attaques passives. En ce qui concerne le contenu d'une transmission de données, plusieurs niveaux de protection peuvent être identifiés. Le service le plus large protège toutes les données transmises entre deux utilisateurs sur une période de temps. Par exemple, lorsqu'une connexion TCP est configurée entre deux systèmes, cette protection large empêche la sortie de toute donnée utilisateur transmise sur la connexion TCP. Des formes plus étroites de ce service peuvent également être définies, y compris la protection d'un seul message ou même des champs spécifiques dans un message. Ces améliorations sont moins utiles que l'approche générale et peuvent même être plus complexes et coûteuses à mettre en œuvre. Il y'a un autre aspect de la confidentialité, qui est la protection des flux de trafic liés à l'analyse. Cela nécessite qu'un attaquant ne puisse pas observer la source, la destination, la fréquence, la longueur ou d'autres caractéristiques du trafic dans une installation de communication.
- **Intégrité des données:** comme pour la confidentialité, l'intégrité peut s'appliquer à un flux de messages, un seul message ou des champs sélectionnés dans un message. Encore une fois, l'approche la plus utile et la plus simple est la protection totale des flux. Un service d'intégrité axé sur la connexion, qui traite d'un flux de messages, assure que les messages sont reçus comme envoyés, sans : duplication, insertion, modification, réorganisation ou répétition.
- **Non répudiation:** la non répudiation empêche l'émetteur ou le récepteur de refuser un message transmis. Ainsi, lorsqu'un message est envoyé, le destinataire peut prouver que l'expéditeur présumé a en effet envoyé le message. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le prétendu séquestre a effectivement reçu le message.
- **Service de disponibilité** Les deux standards X.800 et RFC 2828 définissent la disponibilité pour être la propriété d'un système ou une ressource système accessible et utilisable à la demande par une entité système autorisé, selon les spécifications de performance du système. Une variété d'attaques peut entraîner la perte ou la réduction de la disponibilité. Certaines de ces attaques sont soumises à des contre- mesures automatises, telles que l'authentification et le cryptage, tandis que d'autres nécessitent une sorte d'action physique pour éviter ou se remettre de la perte de disponibilité des éléments d'un système distribué. X.800 traite en outre la disponibilité en tant que propriété d'être associée à divers services de sécurité. Un service de disponibilité est celui qui protège un système pour assurer sa disponibilité. Ce service répond aux problèmes de sécurité soulevés par les attaques de déni de service.

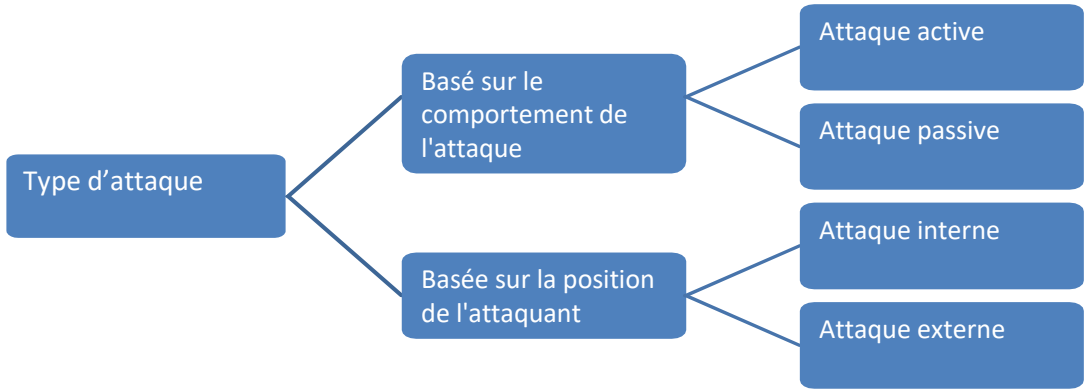
Objectifs et services de la sécurité

Service de Sécurité	Description	Service spécifique desécurité	Description
Authentification	L'assurance que l'entité communicante est celle qu'elle prétend être.	Authentification parentité intermédiaire	Utilisé en association avec une connexion logique pour donner confiance à l'identité des entités connectées.
		Authentification d'origine de données	Dans un transfert sans connexion, il fournit l'assurance que la source des données reçuesest tel que revendiqué.
Contrôle d'accès	La prévention de l'utilisation non autorisée d'une ressource (c.-à-d., Ce service contrôle qui peut avoir accès à une ressource, dans quelles conditions l'accès peut se produire et ce que les personnes qui ont accès à la ressource peuvent faire).	N/A	N/A
La confidentialitédes données	La protection des données contre la divulgation non autorisée.	Confidentialité de laconnexion	La protection de toutes les données del'utilisateur sur une connexion.
		Confidentialité sansconnexion	La protection de toutes les données del'utilisateur dans un seul bloc de données.
		Confidentialité dechamp sélectif	La confidentialité des champs sélectionnés dans les données de l'utilisateur sur une connexionou dans un seul bloc de données.
		Confidentialité du fluxde trafic	La protection de l'information pourrait êtredérivée depuis l'observation des flux de trafic.
L'intégrité desdonnées	L'assurance que les données reçues sont exactement comme envoyées par une entité autorisée (c'est-à-dire ne contiennent aucune modification, insertion, suppression oureproduction).	Intégrité de connexionavec récupération	Fournit l'intégrité de toutes les donnéesutilisateur sur une connexion et détecte toute modification, insertion, suppression ouréponse.
		Intégrité de la connexion sansrécupération	Comme ci-dessus, mais ne fournit qu'unedétection sans récupération.
		Intégrité de connexiondu champ sélectif	Fournit l'intégrité des champs sélectionnés dans les données utilisateur d'un bloc de données transféré sur une connexion et prend la forme de déterminer si les champs sélectionnés ont été modifiés, insérés, supprimés ou reproduits.
		Intégrité sansconnexion du champ sélectif	Fournit l'intégrité des champs sélectionnés dans un seul bloc de données sans connexion ; Prendla forme de déterminer si les champs sélectionnés ont été modifiés.
Non répudiation	Fournit une protection contre le déni par l'une des entités impliquées dans une communication d'avoir participé à tout ou partie dela communication.	Non répudiation - Origine	Preuve que le message a été envoyé par la partie spécifiée.
		Non répudiation - Destination	Preuve que le message a été reçu par la partiespécifiée.

PARTIE 1

Attaques informatiques

En informatique, une attaque est une tentative d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé**. Internet Engineering Task Force** définit l'attaque dans RFC 2828 comme, « Un assaut sur la sécurité du système qui découle d'une menace intelligente, c'est-à-dire d'un acte intelligent qui est une tentative délibérée (en particulier dans le sens d'une méthode ou d'une technique) pour échapper aux services de sécurité et violer la politique de sécurité d'un système. »

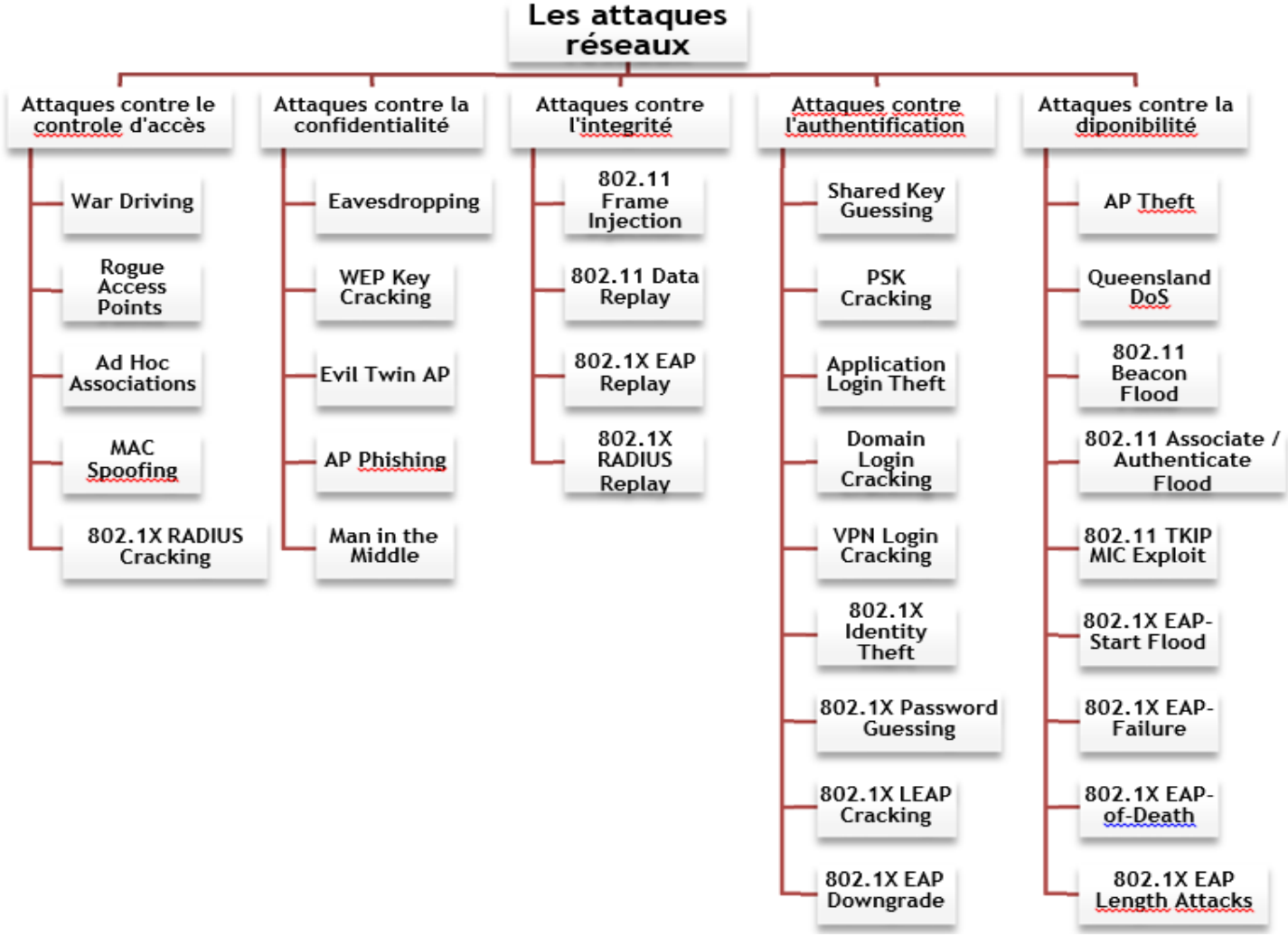


une attaque peut être classée par son comportement ou par la position de l'attaquant.
Une attaque peut être active ou passive.
Une «attaque active» tente de modifier les ressources du système ou d'affecter leur fonctionnement.
Une «attaque passive» tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système. (P. Ex., Écoutes téléphoniques).
Une attaque peut être perpétrée de l'intérieur ou de l'extérieur de l'organisation.

PARTIE 1

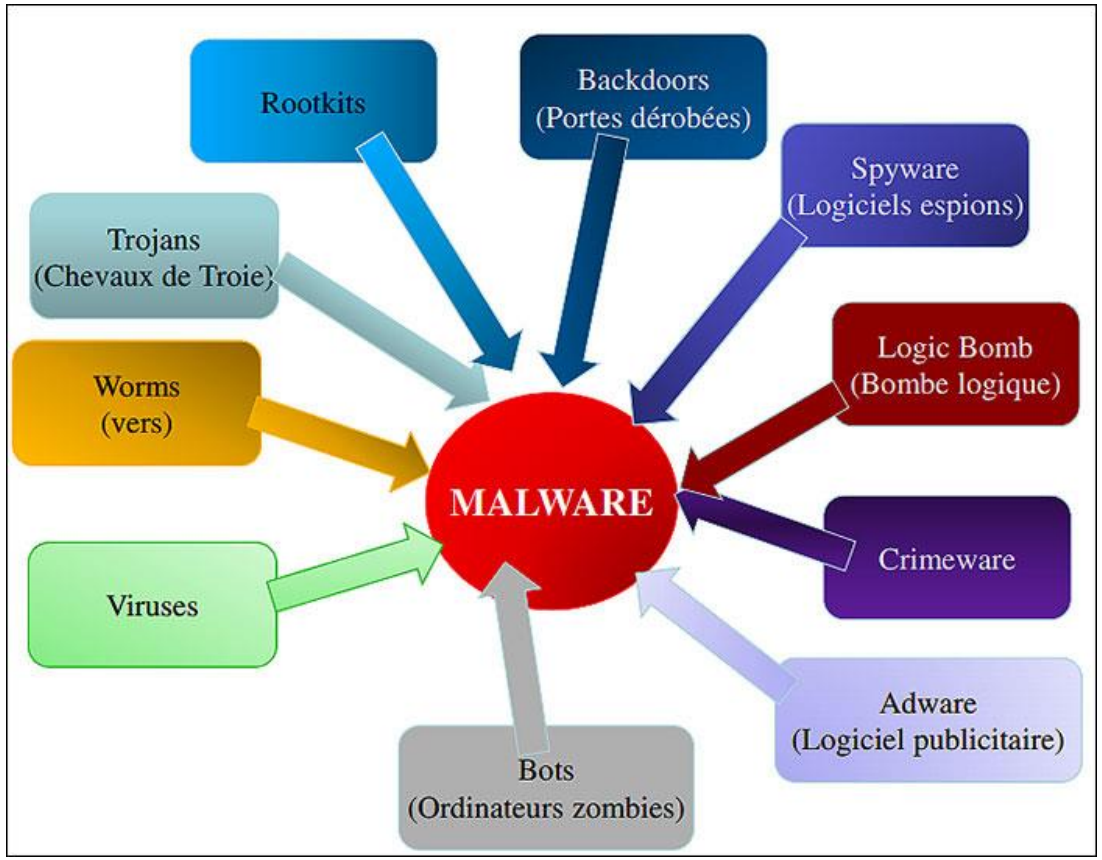
Attaques informatiques

Les attaques réseaux contre 802.11 et 802.1X, peuvent être classées selon le type de menace, et mises en correspondance avec des méthodes et des outils de piratage associés, à savoir, les attaques contre le contrôle d'accès, les attaques contre la confidentialité, les attaques contre l'intégrité, les attaques contre l'authentification, et les attaques contre la disponibilité

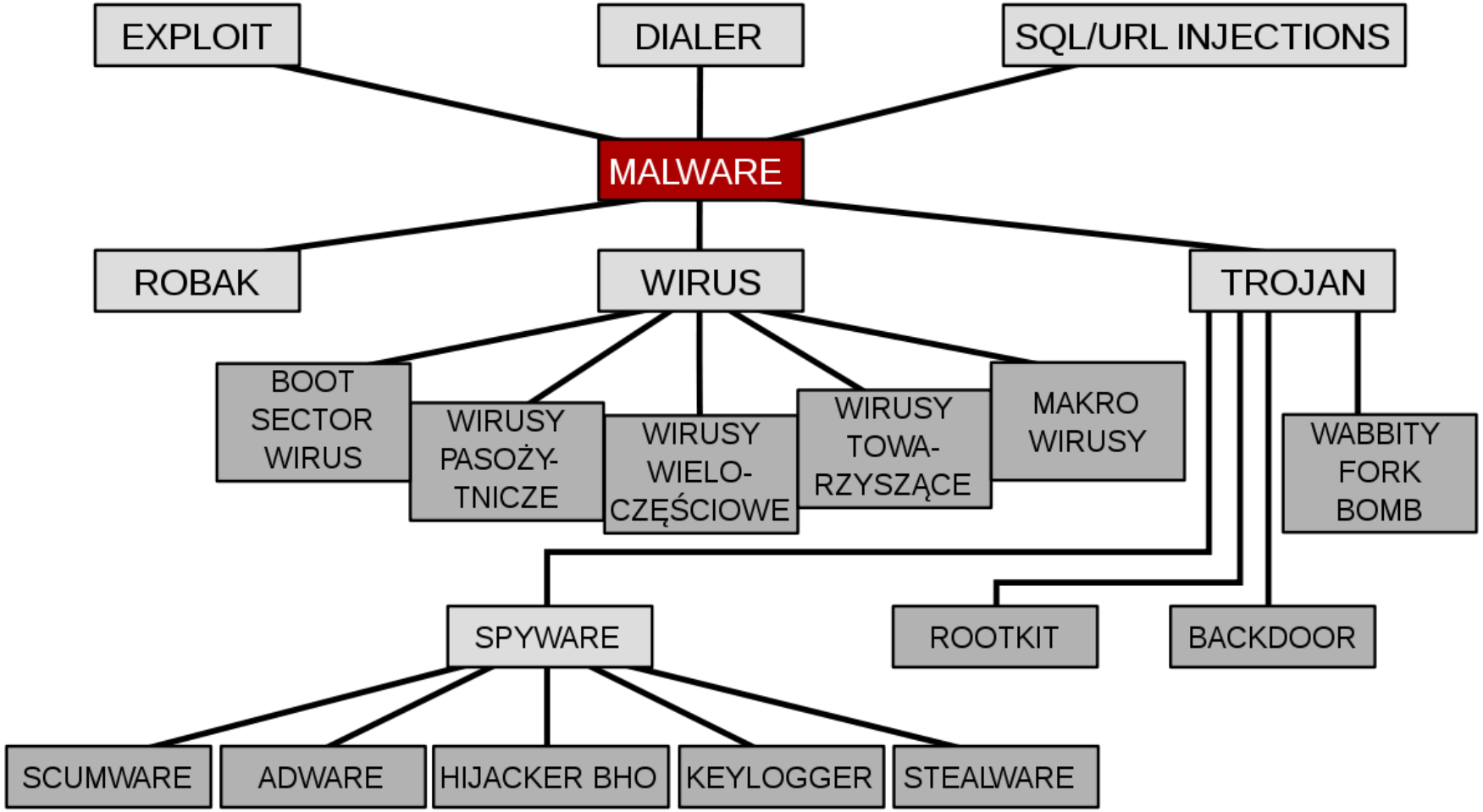


PARTIE 1

Les logiciels malveillants



Les logiciels malveillants



Composantes de sécurité d'une infrastructure digitale

- **Un antivirus** est un programme qui a pour but principal de détecter, neutraliser ou éradiquer les logiciels malveillants des ordinateurs et autres appareils informatiques qui sont infectés. Il joue également un rôle préventif en empêchant les virus d'infecter les systèmes informatiques et de leur nuire. À titre d'illustration, un système dépourvu d'antivirus est comme une maison avec une porte ouverte et non protégée. Cela attirera sans l'ombre d'un doute les cambrioleurs et les intrus indésirables. C'est aussi le cas d'un ordinateur non protégé : il peut être infecté par tout type de programme informatique malveillant. Un antivirus agira comme une porte fermée, avec un garde de sécurité, protégeant ainsi votre système de toutes sortes d'attaques. Il vous protège contre plusieurs types de logiciels malveillants comme les virus, les vers informatiques et les malwares.
- **Un pare-feu** (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

  une interface pour le réseau à protéger (réseau interne) ;
  une interface pour le réseau externe.
  Un système pare-feu contient un ensemble de règles prédéfinies permettant :
  D'autoriser la connexion (allow) ;
  De bloquer la connexion (deny) ;
  De rejeter la demande de connexion sans avertir l'émetteur (drop).
  L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité.
  On distingue habituellement deux types de politiques de sécurité permettant :
  soit d'autoriser uniquement les communications ayant été explicitement autorisées (c'est le principe du moindre privilège) ;
  soit d'empêcher les échanges qui ont été explicitement interdits.
  La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.
  Dans le cas où la zone protégée se limite à l'ordinateur sur lequel le firewall est installé on parle de firewall personnel (pare-feu personnel).
- **Un proxy server** est une sorte de pont qui vous relie au reste d'Internet. Normalement, lorsque vous naviguez sur Internet, vous vous connectez directement au site Web qui vous intéresse. Un proxy établit à votre place la communication avec le site Web.

Composantes de la sécurité d'une infrastructure digitale

- **Un système IDS/IPS:** Les IDS et les IPS font tous deux partie de l'infrastructure réseau. Les IDS/IPS comparent les paquets de réseau à une base de données de cyber menaces contenant des signatures connues de cyberattaques et repèrent tous les paquets qui concordent avec ces signatures.

La principale différence entre les deux tient au fait que l'IDS est un système de surveillance, alors que l'IPS est un système de contrôle.
L'IDS ne modifie en aucune façon les paquets réseau, alors que l'IPS empêche la transmission du paquet en fonction de son contenu, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.

- **Un UTM**: En sécurité informatique, Unified threat management, ou UTM (en français : gestion unifiée des menaces) fait référence à des pare-feu réseau possédant de nombreuses fonctionnalités supplémentaires qui ne sont pas disponibles dans les pare-feu traditionnels. Parmi les fonctionnalités présentes dans un UTM, outre le pare-feu traditionnel, on cite généralement le filtrage anti-spam, un logiciel antivirus, un système de détection ou de prévention d'intrusion (IDS ou IPS), et un filtrage de contenu applicatif (filtrage URL). Toutes ces fonctionnalités sont regroupées dans un même boîtier, généralement appelé appliance.
- **Un SIEM**: abréviation de 'Security Information & Event Management', et est une solution qui combine des outils existants ; à savoir le SIM (Security Information Management) et le SEM (Security Event Management). Les solutions Modern SIEM incluent également des technologies telles que le SOAR pour automatiser la réponse aux menaces et l'UEBA pour détecter les menaces en se basant sur les comportements anormaux. Ensemble, ils fournissent une détection et une réponse accélérées aux événements ou incidents de sécurité au sein d'un environnement IT. Ils fournissent une vue complète et centralisée de la posture de sécurité d'une infrastructure IT et fournissent aux professionnels de la cybersecurité un aperçu des activités au sein de leur environnement IT.
- **Un DLP**: C'est un système de protection contre la perte de données vous permet de créer et d'appliquer des règles afin de contrôler le contenu que les utilisateurs peuvent partager dans des fichiers en dehors de l'organisation. Vous pouvez ainsi contrôler le contenu que les utilisateurs sont autorisés à partager, et éviter toute exposition involontaire d'informations sensibles telles que les numéros de carte de crédit ou de carte d'identité. Les règles de protection contre la perte de données déclenchent des analyses de fichiers pour le contenu sensible et empêchent les utilisateurs de le partager. Elles déterminent la nature des incidents liés à la protection contre la perte de données, lesquels déclenchent des actions telles que le blocage du contenu spécifié. Vous pouvez autoriser le partage contrôlé pour les membres d'un domaine, d'une unité organisationnelle ou d'un groupe.
- **Un SEG**: Les passerelles de messagerie sécurisées (SEG) sont une solution de sécurité de messagerie qui se trouve en ligne sur le chemin des e-mails de l'Internet public au serveur de messagerie de l'entreprise. Cette position lui permet d'inspecter les e-mails à la recherche de contenu malveillant avant qu'ils n'atteignent les systèmes de l'entreprise.

Corrélation des services de sécurité et les mécanismes de sécurité

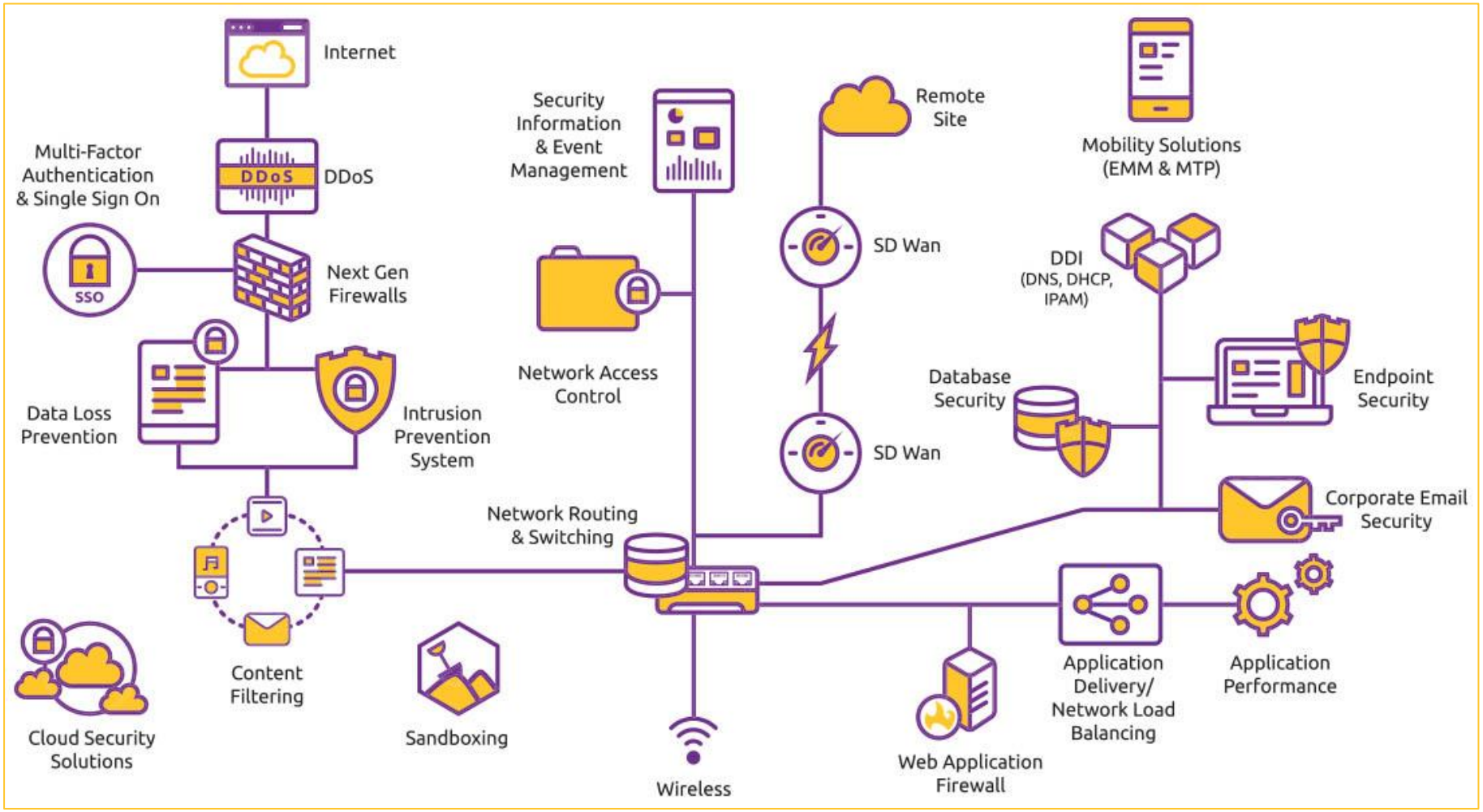
	Mécanisme							
Service	***Chiffrement***	***Signature numérique***	***Contrôle d'accès***	***Intégritédes données***	***Echange d'authentification***	***Remplissagedu trafic***	***Routage***	***Contrôle de la notarisation***
Authentification	X	X			X			
Authentification d'origine des données	X	X						
Contrôle d'accès			X					
Confidentialité	X						X	
Confidentialité des flux de trafic	X					X	X	
Intégrité des données	X	X		X				
Non répudiation		X		X				X
Disponibilité				X	X			

01 - Les bases de la sécurité informatique

- Identification des composantes de sécurité d'un SI et bonnes pratiques opérationnelles

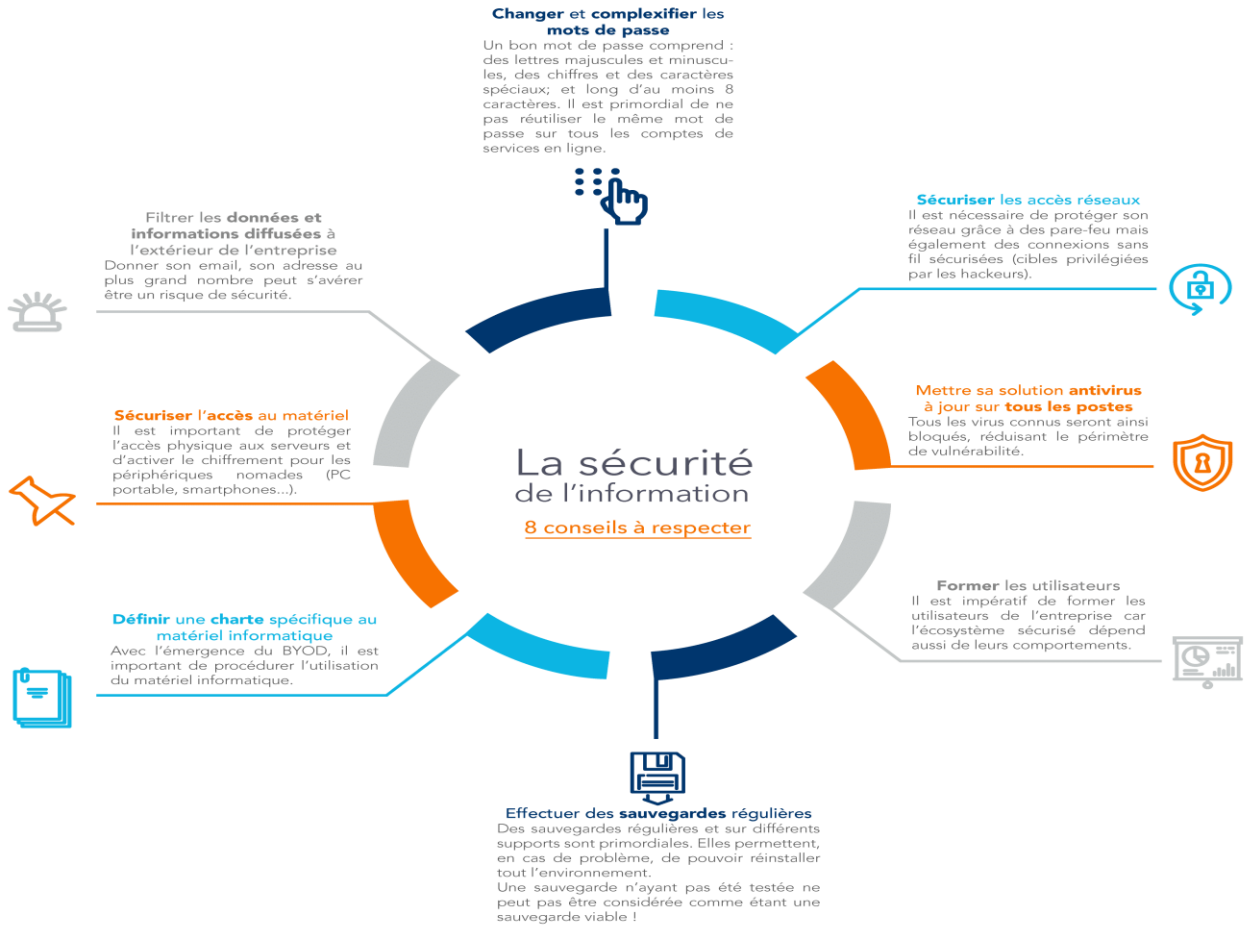
PARTIE 1

Schéma des composantes essentielles de sécurité d'une infrastructure digitale



PARTIE 1

Schéma de recommandations pour sécuriser une infrastructure digitale



Sécuriser un poste de travail Windows

- **Utilisez un pare-feu système**, Windows dispose déjà d'un pare-feu intégré et automatiquement activé.
- **Maintenez tous les logiciels à jour**: Activer les mises à joursmicrosoft pour garder à jour Windows, Microsoft Office et les autres applications Microsoft. Activez les mises à jour automatiques pour les logiciels autres que Microsoft, en particulier les navigateurs, le lecteur Adobe Acrobat et les autres applications que vous utilisez régulièrement.
- **Utilisez un logiciel antivirus et maintenez-le à jour** Si vous exécutez Windows, vous avez Sécurité Windows ou Windows Defender Security Center déjà installé sur votre appareil.
- **Assurez-vous que vos mots de passe sont choisis avec soin** et protégés Pour savoir comment procéder, voir Protéger vos mots de passe.
- **N'ouvrez pas les pièces jointes suspectes** et ne cliquez pas sur les liens inhabituels dans les messages. Ils peuvent apparaître dans le courrier électronique, les tweets, les billets, les publicités en ligne, les messages ou les pièces jointes. Ils se déguisent parfois sous forme de sources fiables et connues.
- **Naviguer sur le web de façon sécurisée**: Évitez de visiter des sites qui offrent du contenu potentiellement illicite. La plupart de ces sites installent des logiciels malveillants à la volée ou proposent des téléchargements qui contiennent des logiciels malveillants. Utilisez un navigateur moderne comme Microsoft Edge, qui permet de bloquer les sites web malveillants et empêche le code malveillant de s'exécuter sur votre ordinateur.
- **Ne touchez pas au matériel piraté** Évitez de diffuser en continu ou de télécharger des films, de la musique, des livres ou des applications qui ne proviennent pas de sources fiables. Ils peuvent contenir des programmes malveillants.
- **N'utilisez pas de bases de données utilisateur ou d'autres appareils externes**, sauf si vous les possédez Pour éviter une infection par des programmes malveillants et des virus, assurez-vous que tous les appareils externes vous appartiennent ou proviennent d'une source fiable.
- **Utiliser Sécurité Windows Sécurité Windows** (ou Windows Defender Security Center dans Windows 8 ou les versions antérieures de Windows 10) est intégrée à Windows et fournit une détection, une prévention et une suppression des programmes malveillants en temps réel avec une protection fournie par le cloud. Il est destiné aux clients domestiques, aux petites et aux grandes entreprises.
- **Windows Defender** hors ligne s'exécute en dehors de Windows pour supprimer les rootkits et autres menaces qui se cachent du système d'exploitation Windows. Cet outil utilise un petit environnement d'exploitation distinct, où les menaces dissimulées ne peuvent pas échapper aux analyses anti-programme malveillant. Avec Windows 10 et 11, Microsoft Defender hors ligne est intégré au système d'exploitation et peut s'exécuter à partir de Sécurité Windows. Il est fourni en tant que téléchargement distinct pour les versions précédentes de Windows.

Sécuriser un poste de travail Linux

- **N'installez que les paquets nécessaires**: Vous ne devez installer que les paquets dont votre entreprise a besoin pour protéger la fonctionnalité de votre serveur. Les distributions de serveurs Linux sont fournies avec une variété de paquets courants déjà installés, tels que adduser et base-passwd. Pendant l'installation, les utilisateurs peuvent choisir d'installer des paquets supplémentaires, notamment un serveur Open SSH, un serveur DNS, une pile LAMP et un serveur d'impression.
- **Désactivez le login root:** Les distributions Linux comprennent un superutilisateur appelé « root » qui dispose de droits d'administration élevés. Le maintien de la connexion root peut présenter un risque pour la sécurité et diminuer la sécurité des ressources cloud des petites entreprises hébergées sur le serveur, car les pirates peuvent exploiter cet identifiant pour accéder au serveur. Pour renforcer la sécurité de votre serveur, vous devez désactiver cette connexion.
- **Configurez une MFA:** L'authentification à deux facteurs (MFA) améliore considérablement la sécurité de l'accès des utilisateurs en exigeant un mot de passe et un second jeton avant que les utilisateurs puissent se connecter au serveur.
- **Gérez les mots de passe**: Une bonne hygiène des mots de passe ne concerne pas seulement les utilisateurs qui se connectent à leurs ordinateurs personnels ou aux applications SaaS. Pour les serveurs, les administrateurs doivent également s'assurer que les utilisateurs utilisent des mots de passe suffisamment rigoureux. Cette pratique les rend beaucoup plus résistants aux attaques.
- **Logiciel antivirus côté serveur :**Bien que les ordinateurs Linux soient considérés comme relativement résistants aux virus, aux logiciels malveillants et à d'autres formes de cyberattaques, tous les terminaux Linux, y compris les ordinateurs de bureau, devraient être protégés par un antivirus. Les produits antivirus renforceront les capacités défensives de tout serveur qu'il exécute.
- **Mettez à jour régulièrement ou automatiquement** Vous ne devez pas conserver d'anciens paquets non corrigés, car ils introduisent dans le système des vulnérabilités critiques qui pourraient être exploitées par des cybercriminels. Pour éviter ce problème, assurez-vous que votre serveur, ou votre pool de serveurs, est mis à jour régulièrement.
- **Activez un pare-feu :**Chaque serveur Linux devrait être équipé d'un pare-feu comme première ligne de défense contre les demandes de connexion non autorisées ou malveillantes. UFW (uncomplicated firewall) est un pare-feu Linux de base courant. Vous devez inspecter la politique de pare-feu pour vous assurer qu'elle est adaptée à l'environnement d'exploitation de votre entreprise.
- **Sauvegardez votre serveur:** Il y a toujours des choses qui peuvent mal tourner lorsqu'il s'agit de systèmes informatiques, et les paquets peuvent créer des problèmes de dépendance et d'autres problèmes. Il est donc vital que vous conserviez la possibilité de revenir en arrière dans les modifications apportées à votre serveur.
- **Gardez la sécurité à l'esprit:** Linux peut être le meilleur serveur pour votre petite entreprise ou votre entreprise, car les distributions ont généralement une posture de sécurité décente configurée automatiquement. Cependant, pour augmenter considérablement vos défenses et minimiser les chances d'accès des utilisateurs malveillants, vous devez renforcer votre serveur Linux en appliquant les conseils des meilleures pratiques.

Sécuriser une infrastructure digitale

1. Les bases de la sécurité informatique
2. **Les réglementations juridiques**
3. La gestion des risques et d'incidents
4. Sécurité réseaux
5. Les listes de contrôle d'accès
6. La cryptographie
7. Infrastructure PKI

La cybercriminalité

- **La cybercriminalité** n'étant pas définie avec rigueur, elle conduit vers des dérives terminologiques. Ainsi, MM. Alterman et Bloch retiennent comme définition du délit informatique, la définition de la cybercriminalité proposée par des experts de l'Organisation pour la Coopération et le Développement Economique (OCDE), à savoir « ***tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmissions de données*** ». Ces juristes, intégrant dans leur définition la notion morale, semblent considérer que le droit pénal ne peut à lui seul contenir toute l'approche « sanction » de l'utilisation frauduleuse de l'informatique. Cependant, cette démarche ne saurait être retenue dans la mesure où les chartes de règlement des litiges, telle la charte de l'Internet par exemple, ont révélé leurs limites comme monde alternatif de règlement des conflits. L'application de la norme pénale se pose ainsi comme solution face à l'échec de ces initiatives.
- La confusion opérée par ces auteurs, entre la cybercriminalité et le délit informatique, s'avère symptomatique d'une difficulté d'appréhender cette forme de délinquance. Ce considère que « la seule démarche acceptable consiste à réserver l'acception de fraude informatique aux hypothèses dans lesquelles la technique informatique est au cœur de l'agissement incriminable » tout en sachant fort bien qu'il est parfois difficile d'isoler le « noyau dur » de la « périphérie ». La nécessaire clarification des actes qui relèvent de la cybercriminalité a conduit la doctrine à multiplier les notions désignant les actes illégaux en rapport avec l'informatique. Cette démarche a engendré une pléthore de définitions doctrinales de la cybercriminalité en Europe et aux Etats-Unis.
- Les tentatives de définition de la cybercriminalité, ont montré comment ce phénomène est vaste , complexe et touche beaucoup de domaines. Certains auteurs désignant les délinquants, ou qualifiant les actes qu'ils réalisent, commettent parfois des confusions de sens, en désignant sous la terminologie de « pirate » tous les délinquants en informatique. Ainsi, il convient d'aborder dans cette partie la distinction de la cybercriminalité et les criminalités apparentées. Il s'agit d'une distinction relative aux termes juridiques, et d'une distinction relative aux auteurs de l'infraction.
- Bien que les notions de « criminalité informatique » et de « cybercriminalité » sont étroitement liées, il existe néanmoins une distinction entre les deux conceptions. Ainsi, la criminalité informatique représente l'infraction générique, dont la cybercriminalité est une variante. Cette dernière est une forme particulière de la criminalité informatique, forme qui ne s'exprime que sur et à travers le réseau de télécommunication, contrairement aux autres délits informatiques qui ne nécessitent pas d'intéraction avec le réseau de télécommunication.

Le Cyberespace

- **Le cyberespace** se présente comme un espace indéfini. Un espace virtuel d'ordinateurs tous reliés entre eux grâce à des réseaux qu'explorent les « cybernautes », dont les systèmes nerveux sont directement branchés sur les réseaux grâce à une prise fixée sur leur crâne. Le cyberespace comporte beaucoup de caractéristiques qui prennent de l'importance lorsqu'on envisage la problématique de sa régulation. Il peut être considéré comme une « illusion », c'est « une hallucination consensuelle ». Il peut être considéré aussi comme une réalité, mais une réalité dans « un monde virtuel ». Un monde d'ordinateurs en réseaux de télécommunications, de logiciels et de données informatiques, avec une présence sentie dans un monde physique, c'est donc une « réalité virtuelle ».
- Le cyberespace est un espace complexe à comprendre. Il est à la fois naturel et artificiel. Naturel car sa source est naturelle : le monde réel. En même temps il est un espace artificiel. Tout d'abord, le langage utilisé est artificiel - celui des mathématiques en commençant par le codage fondamental (0,1) et en finissant par des équations mathématiques de plus en plus élaborées. Ces équations sont comme le germe d'une infinité d'images dont la plupart n'ont pas de correspondance dans le monde naturel. Le cyberespace est aussi artificiel parce qu'il résulte d'une technologie sophistiquée, mise en œuvre par l'être humain.
- Compte tenu de l'éventail des nouvelles technologies mises à la disposition des personnes malveillantes et qui font une large place à l'ingéniosité d'une part et de la spécificité des délits informatiques d'autre part, l'usage des N.T.I.C pour commettre des nouvelles infractions est devenu un phénomène international. Internet a fait fleurir une multitude d'infractions liées à la circulation de l'information telle que les violations du droit d'auteur , les violations de vie privée et du secret des correspondances, les délits de presse et de diffamation, etc.

La cybercriminalité et la criminalité de haute technologie

La criminalité de haute technologie est la criminalité qui recouvre l'ensemble des actes illégaux intéressant l'informatique et les télécommunications tant sur le plan des matériels que des logiciels. Elle concerne la criminalité informatique proprement dite et la contrefaçon / le clonage de composants électroniques capables de créer des dysfonctionnements dans les systèmes d'information, de télécommunications ou autorisant un usage frauduleux. Dans cette optique, la criminalité de haute technologie peut couvrir deux catégories :

- Les infractions liées aux systèmes informatiques non connectés aux réseaux de télécommunication.
- Les infractions liées aux systèmes informatiques connectés aux réseaux de télécommunication.

Par rapport à notre définition de la cybercriminalité141, le premier type d'infractions ne tombe pas sous cette catégorie. En revanche, la seconde catégorie d'infractions peut être classée sous la catégorie de la cybercriminalité, dans la mesure où les infractions impliquant, par un moyen ou par un autre un réseau de télécommunication. Dans cette optique, nous pouvons affirmer que quelques infractions de haute technologie peuvent être considérées comme des cybercriminalités et que d'autre, en revanche ne peuvent pas l'être.

La distinction relative aux auteurs de l'infraction

La criminalité de haute technologie est la criminalité qui recouvre l'ensemble des actes illégaux

Parce qu'elle est difficile à conceptualiser, la cybercriminalité est une source de confusion terminologique. Certains auteurs désignant les délinquants ou qualifiant les actes qu'ils réalisent, commettent quelquefois des confusions de sens en désignant, sous la terminologie de « hacker » ou « pirate » tous les délinquants en informatique. Il convient donc de s'attarder sur les termes caractérisant ce délit, afin d'éviter les confusions terminologiques concernant le « hacker », le cracker, et le crasher.

- **Le Hacker:** Dans l'esprit de beaucoup, les hackers sont tous ceux qui utilisent les N.T.I.C. à des fins contraires à la loi. Ce n'est en réalité absolument pas la bonne définition. Le terme « hacker » ne se contente pas d'une définition unique. D'origine anglo-saxonne, il appartient désormais au langage courant. Le dictionnaire de la langue anglaise Collins Cobuild en propose dans son édition de 2000, deux définitions:

a. Un hacker informatique est quelqu'un qui tente de s'introduire dans les systèmes informatiques, en particulier pour obtenir des renseignements secrets ou confidentiels qui y sont entreposés.

b. Un hacker informatique est quelqu'un qui utilise beaucoup l'ordinateur, notamment au point de n'avoir plus de temps pour quoi que ce soit d'autre.

Le terme hacker provient du verbe hack ; to hack, qui signifie la pénétration à l'intérieur d'un système informatique ou un ordinateur145. Le hacker peut être considéré comme« une personne qui prend du plaisir à explorer en détail un système programmable et qui cherche sans cesse à étendre ses connaissances dans ce domaine»

le terme hacking signifie : (a) toute personne qui s'intéresse à explorer les systèmes informatiques ; (b) un expert dans une langue particulière (C+, C++) ou dans un domaine des système d'exploitation ; (c) une personne forte dans les détails de la programmation ; (d) une personne qui s'intéresse au défi intellectuel ; et (e) une personne qui essaie de découvrir les informations sensitives147 .Il revêt deux actes : passer le temps devant un système informatique ; et entrer à l'intérieur de ce système.

La distinction relative aux auteurs de l'infraction

- **Le Cracker, le Crasher, et le Phreaker :** Le terme crasher provient du verbe to crash qui signifie « s'écraser ». Il convient de proposer une définition de ce terme dans une logique comparative, en considérant le crasher comme la personne qui pénètre à l'intérieur d'un système informatique et détruit un de ses éléments par plaisir. Dans cette optique, la distinction entre le crasher et le cracker est trouvée dans la finalité de l'infraction. Tandis que le crasher pénètre à l'intérieur d'un système informatique et détruit les données, le cracker soit détruit soit introduit des données dans ce système.
- Le terme « phreaking » provient de la contraction des deux mots anglais phone (téléphone) et freak (monstre). On comprend par phreaking toutes les méthodes pour accéder illégalement à un système lié à la téléphonie, Cela comprend la corruption et le détournement de PABX, de VMB, de téléphone portable, de modem...etc, À cet égard, le phreaker désigne l'auteur d'une fraude informatique constituée par l'utilisation des lignes téléphoniques.

PARTIE 1

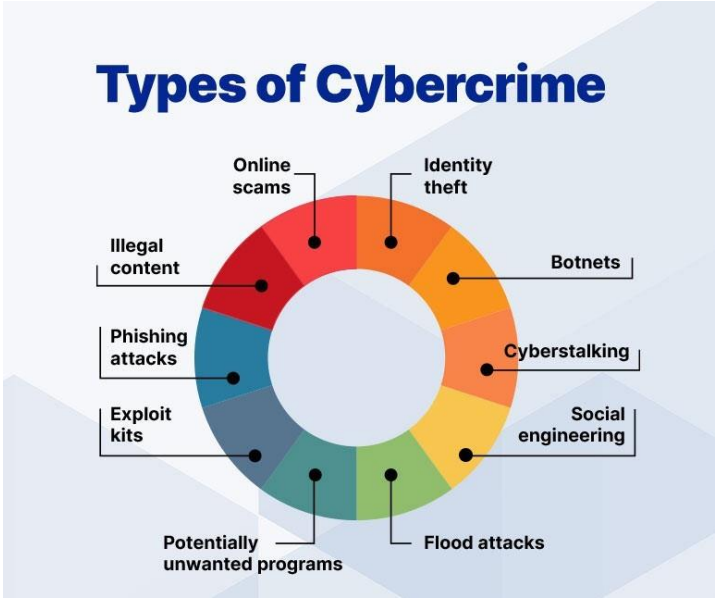
Types des actes de la cybercriminalité

Quels sont les différents types de la cybercriminalité ?

1. **Type des infractions liées aux formes de criminalité traditionnelles facilité par les NTIC**: Ce sont des infractions classiques, qui ont pu évoluer avec les nouvelles technologies de l'information et de la communication38, alors ils ont fait partie d'une transformation de commettre ces infractions au niveau réel à les commettre au niveau virtuel, sachant que ce dernier facilite les opérations. Alors on peut citer quelques exemples les plus connus de ces infractions concernant cette catégorie: La contrefaçon (numérique), L'escroquerie en ligne, Le phishing (hameçonnage), Le spamming, Le blanchiment d'argent en ligne, Le terrorisme numérique ou cyber terrorisme, Harcèlement en ligne ou Cyber harcèlement , Une nouvelle forme de cyber harcèlement : Sexting, La cyber intimidation.

2.Type des infractions liées aux systèmes d'information et aux systèmes de traitement automatisé des données (STAD): Ce type des infractions est apparu avec l'apparition et le développement des systèmes de réseaux d'informatique, et notamment l'internet. Ces infractions sont commis seulement au niveau virtuel et concernant la destruction des systèmes et les données. On peut citer deux exemples de ces infractions les plus connus en communié pour bien comprendre ce type de la cybercriminalité. : Le Dos et le DDOS, La défacement de site web ou le hacking,

3.Type des infractions atteinte à les données personnelles et à la vie privé: Ce type concerne les personnes lui-même au niveau virtuel, ainsi leurs donnée privé et leurs vie. Pour bien comprendre ce type de la cybercriminalité on va donner quelques exemples : L'usurpation d'identité numérique, Diffamation numérique, Atteinte à la base des données personnelles.



Les étapes d'une cyberattaque réussie

Une cyberattaque réussie exige une planification soignée et une exécution précise. Ce que les piratages efficaces ont en commun est le fait de pouvoir attendre à couvert le bon moment pour frapper. Et si les attaques ont recours à diverses méthodes, elles ont généralement plusieurs étapes similaires en commun. Afin de pouvoir parer les cyberattaques, il est important de comprendre quelles sont ces étapes. Décryptons ensemble leur schéma type.

1. **Reconnaissance:** Avant de perpétrer une attaque, les hackers commencent par identifier une cible vulnérable et ils explorent le meilleur moyen de l'exploiter. La cible initiale peut être n'importe qui au sein d'une entreprise, que ce soit un dirigeant ou un administrateur. Les agresseurs ont juste besoin d'un point d'entrée pour démarrer. Les e-mails de phishing ciblés sont courants à cette étape pour introduire efficacement un malware.
2. **Exploration:** Une fois la cible identifiée, l'étape suivante consiste à identifier un maillon faible permettant aux agresseurs de s'infiltrer. Ils procèdent généralement par l'exploration du réseau d'une entreprise, au moyen d'outils faciles à trouver sur Internet, jusqu'à repérer des points d'entrée. Cette étape du processus peut prendre du temps, parfois des mois, le temps que les criminels repèrent des vulnérabilités.
3. **Accès et élévation:** Une fois les faiblesses du réseau ciblé identifiées, l'étape suivante de la cyberattaque consiste à se frayer un accès et remonter. Dans quasiment tous les cas, un accès privilégié est nécessaire car il permet aux agresseurs d'évoluer librement au sein de l'environnement. Des tableaux Rainbow et d'autres outils comparables aident les infiltrés à voler des identifiants, à faire remonter les privilèges jusqu'au niveau admin, puis à s'introduire dans tout système du réseau accessible via le compte administrateur. Une fois que les agresseurs disposent de privilèges élevés, ils prennent le réseau d'assaut, lequel leur « appartient » désormais.
4. **Exfiltration:** Etant libres de circuler sur le réseau, les agresseurs peuvent avoir accès aux systèmes détenant les données les plus sensibles de l'organisation qu'ils peuvent ainsi extraire à loisir. Mais outre le fait de voler des données privées, ils peuvent aussi changer ou effacer des fichiers sur les systèmes compromis.
5. **Attente:** Maintenant que les criminels disposent d'un accès sans restriction au réseau ciblé, il ne leur reste plus qu'à rester silencieux, en sommeil. Pour ce faire, les hackers peuvent installer des programmes malveillants secrets, comme des root kits. Ainsi, ils peuvent revenir quand ça leur chante. Et grâce aux privilèges élevés obtenus plus tôt, ils ne sont plus dépendants d'un point d'accès unique. Les criminels peuvent aller et venir à leur guise.
6. **Assaut:** Heureusement, ce n'est pas le cas de toutes les cyberattaques, car l'assaut est l'étape d'une attaque où les choses se compliquent sérieusement. C'est à ce stade que des cybercriminels risquent de modifier la fonctionnalité des équipements matériels d'une victime ou les désactiver tout simplement. L'attaque Stuxnet des infrastructures critiques en Iran en est un exemple classique. Lors de la phase d'assaut, l'attaque n'a été que de très courte durée. Toutefois, les agresseurs avaient déjà pris le contrôle de l'environnement. Il est donc généralement trop tard pour que l'organisation victime puisse se défendre d'elle-même contre la compromission.

Les étapes d'une cyberattaque réussie

7. Obfuscation: Le plus souvent, les agresseurs souhaitent effacer leurs traces, mais ce n'est pas une vérité universelle, encore moins s'ils souhaitent laisser une « carte de visite » pour se vanter de leurs exploits. L'objectif de l'obfuscation est de perturber l'enquête légale, de rendre l'investigation confuse et de désorienter les enquêteurs. Plusieurs techniques et outils le permettent, y compris ceux de nettoyage de fichiers journaux, de spoofing, de désinformation, de comptes zombis, de commandes de chevaux de Troie, etc.

Les outils établissant un périmètre de sécurité traditionnel, comme les pare-feu de nouvelle génération, offrent peu de protection contre les attaques ciblées avancées.
Pour contrer une cyberattaque, contrôler les accès privilégiés devient indispensable. A partir de la troisième étape, chacune implique en effet des identifiants privilégiés.
Cela permet d'identifier les comptes privilégiés présents sur le réseau, d'en assurer le contrôle et d'analyser leur utilisation. Chaque identifiant privilégié doit être mis à jour en continu. Ainsi, même si un intrus compromet un identifiant, il ne pourra pas s'en servir pour se déplacer vers d'autres systèmes et en extraire des données.

Droit pénal relatif à la cybercrominalité

Ces règles dérogatoires au droit commun concernent les organes chargés des enquêtes et les pouvoirs dont ils sont dotés.

Les organes compétents

- La direction Générale de la Sécurité des Systèmes d'Information (DGSSI), chargée d'apporter le soutien nécessaire aux administrations, organismes publics et infrastructures d'importance vitale pour la mise à niveau de la sécurité de leurs systèmes d'information. Cette structure créée il y a 10 ans est rattachée à l'Administration de la défense nationale et chargée entre autres d'assurer la veille technologique pour anticiper les évolutions et proposer les innovations nécessaires en matière de sécurité des systèmes d'information (SI). La DGSSI travaille pour le développement de dispositifs de systèmes sécurisés au profit des administrations et organismes publics.
- La Commission nationale de contrôle de la protection des données à caractère personnel ou CNDP est une commission marocaine, créée par la loi n°09-08 du 18 février 2009, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Elle est chargée de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'homme. La Commission est formée de personnalités notoirement connues pour leur impartialité, leur probité morale et leur compétence dans les domaines juridiques, judiciaires et informatiques.
- Le maCERT (Moroccan Computer Emergency Response Team) est le centre de veille, détection et réponse aux attaques informatiques. La Direction de gestion de ce centre qui fait partie des quatre directions de la DGSSI est chargée de la mise en oeuvre, en relation avec les autres administrations, de systèmes de veille, de détection, d'alerte des événements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat et de la coordination de la réaction à ces événements.

Textes législatifs et réglementaires Marocaines

- **Lois:**

1. La loi n° 43-20: relative aux services de confiance pour les transactions électroniques a pour objet de fixer le régime applicable aux : Services de confiance pour les transactions électroniques ; Moyens et prestations de cryptologie ; Opérations effectuées par les prestataires de services de confiance et les règles à respecter par ces derniers et les titulaires des certificats électroniques. Elle fixe également les prérogatives de l'Autorité nationale des services de confiance pour les transactions électroniques.
2. La loi 05-20: relative à la cybersécurité vise notamment à mettre en place un cadre juridique préconisant un ensemble de règles et de mesures de sécurité afin d'assurer et renforcer la sécurité et la résilience des systèmes d'information des administrations de l'Etat, des collectivités territoriales, des établissements et entreprises publics et de toute autre personne morale de droit public de l'Etat ainsi que des infrastructures d'importance vitale disposant des systèmes d'information sensibles.
3. LOI N°31-08 ÉDICTANT DES MESURES DE PROTECTION DU CONSOMMATEUR, Y COMPRIS LA PROTECTION DU CONSOMMATEUR EN LIGNE: Cette loi se fixe pour principal objectif le renforcement et la protection des droits des consommateurs, et ce, en leur garantissant une meilleure information, en les protégeant contre les clauses abusives et certaines pratiques commerciales, et en prévoyant des dispositions complémentaires relatives à la garantie conventionnelle, au service après vente et au surendettement. De même et au regard du rôle important du mouvement consumériste dans l'information, la sensibilisation et la protection juridique des droits des consommateurs, cette loi accorde aux associations de consommateurs reconnues d'utilité publique le droit d'ester en justice en représentation des intérêts collectifs des consommateurs.

Textes législatifs et réglementaires Marocaines

- **Lois:**

4. LOI 53-05: relative à l'échange électronique de données juridiques, cette loi fixe le régime applicable aux données juridiques échangées par voie électronique (cryptographie) et à la signature électronique. Elle détermine également le cadre juridique applicable aux opérations effectuées par les prestataires de service de certification électronique, ainsi que les règles à respecter par ces derniers et les titulaires des certificats électroniques délivrés.
5. LOI N°24-96: consolidée relative à la poste et aux télécommunications, telle qu'elle a été modifiée et complétée, L'objet de cette loi est de définir le cadre juridique précisant le nouveau paysage du secteur de la poste et des télécommunications, notamment celui des réseaux des Télécommunications.
6. LOI 09-08: relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel
7. LOI 07-03: complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, cette loi permet de sanctionner toutes les intrusions non autorisées dans un système de traitement automatisé de données.

Textes législatifs et réglementaires Marocaines

- **décrets:**

1. DÉCRET N° 2-21-406: du 4 hija 1442 (15 juillet 2021) pris pour l'application de la loi n° 05-20 relative à la cyber sécurité.
2. Décret N° 2-13-881 du 28 rabii I 1436 (20 janvier 2015) modifiant et complétant le décret N° 2-08-518 du 25 joumada I 1430 (21 mai 2009) pris pour l'application des articles 13, 14, 15, 21 et 23 de la loi N° 53-05 relative à l'échange électronique des données juridiques.
3. Décret N° 2-08-518 du 25 Joumada I 1430 (21 mai 2009) pris pour l'application des articles 13, 14, 15, 21 et 23 de la loi n° 53-05 relative à l'échange électronique des données juridiques.
4. Décret n°2-11-509 du 22 chaoual 1432 (21 septembre 2011) complétant le décret n° 2-82-673 du 28 rabii I 1403 (13 janvier 1983) relatif à l'organisation de l'Administration de la Défense Nationale et portant création de la Direction Générale de la Sécuirté des Systèmes d'Information.
5. DÉCRET N° 2-09-165: DU 25 joumada i 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel, Cette loi vise à assurer une protection efficace des particuliers contre les abus d'utilisation des données de nature à porter atteinte à leur vie privée et d'harmoniser le système marocain de protection des données personnelles avec celles de ses partenaires notamment européens. En outre, la loi institue une Commission Nationale de protection des Données Personnelles (CNDP).

Textes législatifs et réglementaires Marocaines

- **arrêtés:**

1. Arrêté du Chef du gouvernement n° 3-88-13 du 28 rabii I 1436 (20 janvier 2015) fixant la forme et le contenu de la demande d'autorisation préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations de cryptographie et le dossier l'accompagnant.
2. Arrêté du Chef du gouvernement n° 3-87-13 du 28 rabii I 1436 (20 janvier 2015) fixant la forme de la déclaration préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations de cryptographie et le contenu du dossier l'accompagnant.
3. Arrêté du Chef du gouvernement n° 3-90-13 du 28 rabii I 1436 (20 janvier 2015) fixant le modèle du cahier des charges devant accompagner la demande d'agrément de prestataire de services de certification électronique.
4. Arrêté du Chef du gouvernement n° 3-89-13 du 28 rabii I 1436 (20 janvier 2015) fixant le modèle du cahier des charges devant accompagner la demande que doivent déposer les personnes ne disposant pas de l'agrément de prestataires de services de certification électronique et qui entendent fournir des prestations de cryptographie soumises à autorisation.
5. ARRÊTÉ N° 3-74-11: fixant l'organisation de la direction générale de la sécurité des systèmes d'information, cet arrêté concerne la création des divisions et des services des directions relevant de la Direction Générale de la Sécurité des Systèmes d'Information.

Textes législatifs et réglementaires Marocaines

- **Exemples des infractions et des sanctions:**

1. Article 65 de la loi 43.20: Sans préjudice des sanctions pénales plus graves prévues par la législation en vigueur, est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 100.000 à 500.000 dirhams, quiconque a fait sciemment de fausses déclarations ou a remis de faux documents au prestataire de services de confiance pour l'obtention d'un service de confiance.
2. Article 56 de la loi 08-09: est puni d'un emprisonnement de trois mois a un an et d'une amende de 2000 a 200000 DH ou de l'une de ses deux peines seulement quiconque procède à un traitement de données à caractère personnel en violation des dispositions de l'article 4,
3. Article 84 de la loi 24-96: Sera puni d'un emprisonnement d'un mois à deux ans et d'une amende de 10.000 à 200.000 dirhams quiconque aura, par la rupture des fils ou des câbles, par la destruction ou la dégradation des appareils ou par tout autre moyen, volontairement causé l'interruption des télécommunications.
4. Article 607-3 de la loi 07-3: Le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un mois à trois mois d'emprisonnement et de 2.000 à 10.000 dirhams d'amende ou de l'une de ces deux peines seulement.
5. Article 607-7 de la loi 07-03: Sans préjudice de dispositions pénales plus sévères, le faux ou la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de 10.000 à 1.000.000 de dirhams.