Module : S'initier à la sécurité des systèmes d'information

A. Introduction à la sécurité informatique

- **Définition et enjeux :**
  La sécurité informatique désigne l'ensemble des mesures et des pratiques mises en œuvre pour protéger les systèmes d'information, les réseaux, les données et les infrastructures informatiques contre divers types de menaces. Elle vise à garantir que les informations restent accessibles uniquement aux personnes autorisées, intactes et disponibles en tout temps. Pour ce faire, elle repose sur trois objectifs fondamentaux, souvent résumés par la triade Confidentialité, Intégrité et Disponibilité
- **Cadre général :**
  Évolution des menaces numériques et des cyberattaques Avec l'essor rapide du numérique, les menaces informatiques se diversifient et se sophistiquent, entraînant des risques majeurs pour les organisations et les particuliers :

Multiplication et diversification des attaques :
Les cybercriminels exploitent des techniques de plus en plus avancées pour contourner les mesures de sécurité traditionnelles. On observe l'émergence de ransomwares ciblés, d'attaques par déni de service (DDoS) amplifiées et de campagnes de phishing extrêmement personnalisées.
Automatisation des attaques :
L'utilisation de scripts automatisés et d'intelligence artificielle permet de lancer des attaques à grande échelle, rendant plus difficile la détection et la réaction en temps réel.
Exploitation des vulnérabilités :
La découverte rapide de nouvelles failles dans les logiciels et systèmes d'exploitation, souvent exploitées avant même la mise en place des correctifs, augmente le risque d'intrusions.
Attaques sur la chaîne d'approvisionnement :
Les cybercriminels ciblent de plus en plus les fournisseurs et sous-traitants pour compromettre des systèmes interconnectés, amplifiant ainsi l'impact potentiel d'une attaque.
Risque accru lié à la transformation numérique :
La migration vers le cloud, l'essor de l'Internet des objets (IoT) et l'augmentation du télétravail créent de nouveaux vecteurs d'attaque, nécessitant une adaptation constante des dispositifs de sécurité.
En résumé, l'évolution des menaces numériques et des cyberattaques impose une veille constante et une réévaluation régulière des stratégies de sécurité pour anticiper et contrer efficacement ces risques.

1. Les virus et autres maliciels

- **Types de virus et maliciels :**
  - Virus classiques, vers, chevaux de Troie, ransomwares, spyware, adware…
  - Fonctionnement de ces programmes malveillants et modes d'infection (via e-mails, téléchargements, supports amovibles, etc.).

Étude de cas :
Exemple concret : Le virus "ILOVEYOU" (année 2000)
Description :
Le virus "ILOVEYOU" était un ver informatique qui s'est propagé massivement par e-mail. Le message avait pour objet : "ILOVEYOU" et un fichier joint intitulé "LOVE-LETTER-FOR-YOU.txt.vbs".
Propagation :
La victime ouvrait la pièce jointe, croyant lire une lettre d'amour.
Le script Visual Basic (VBScript) s'exécutait et infectait le système.

Le virus envoyait automatiquement une copie de lui-même à tous les contacts de la victime via Outlook.
Il modifiait des fichiers (images, musiques…) et pouvait les rendre inutilisables.
Conséquences :
Des millions de systèmes infectés dans le monde en quelques heures.
Pertes estimées à plusieurs milliards de dollars.
Impact sur des institutions gouvernementales, banques, entreprises, etc.

- Moyens de détection

Antivirus et Antimalwares :
Ils analysent les fichiers à l'ouverture ou au téléchargement.
Détection basée sur des signatures connues ou via analyse comportementale.
Systèmes de détection d'intrusion (IDS) :
Surveillent le trafic réseau pour détecter des comportements suspects ou non autorisés.
Sandboxes (bac à sable) :
Exécutent les fichiers dans un environnement isolé pour observer leur comportement avant de les lancer réellement.
Surveillance de l'activité système :
Détection de modifications inhabituelles dans les fichiers système, les processus, ou les connexions réseau.

- Moyens de prévention

Sensibilisation des utilisateurs :
Ne jamais ouvrir de pièces jointes ou cliquer sur des liens suspects.
Vérifier l'expéditeur avant d'agir sur un email inattendu.
Mise à jour régulière :
Systèmes d'exploitation, logiciels, antivirus, etc.
Les failles sont rapidement corrigées par des mises à jour.
Utilisation d'antivirus à jour :
Avec base de données virale constamment actualisée.
Pare-feu personnel et professionnel :
Limite les communications non autorisées.
Sauvegardes régulières :
Permet de restaurer les fichiers en cas d'infection ou d'attaque de type ransomware.
Filtrage des e-mails :
Utilisation de solutions antispam et d'analyse automatique des pièces jointes.

2. Les droits d'auteur et le Copyright

Cadre légal :
e rôle du droit d'auteur dans la protection des créations numériques
Qu'est-ce que le droit d'auteur ?
Le droit d'auteur est une branche de la propriété intellectuelle qui protège les œuvres de l'esprit. Cela inclut :
Les œuvres littéraires (livres, articles),
Les œuvres artistiques (photos, vidéos, musiques),
Et les créations numériques, notamment les logiciels.
Il protège automatiquement l'auteur dès la création de l'œuvre, sans qu'il soit nécessaire de la déposer.
.**Implications pratiques :**
Discuter des enjeux de la piraterie informatique, du respect des licences et de la propriété intellectuelle :

La piraterie informatique : une menace sérieuse
Définition :
La piraterie informatique désigne l'ensemble des actes illégaux consistant à copier, distribuer, modifier ou utiliser un logiciel ou un contenu numérique sans respecter les droits de son auteur.
Enjeux :

- ✓ Perte économique pour les éditeurs et développeurs.
- ✓ Violation du droit d'auteur et poursuites judiciaires possibles.
- ✓ Risque de sécurité : les logiciels piratés sont souvent infectés (malwares, backdoors...).
- ✓ Manque de mises à jour et de support technique.

Respect des licences logicielles
Une licence est un contrat légal qui précise comment un logiciel peut être utilisé.
Propriété intellectuelle dans le numérique
La propriété intellectuelle protège les œuvres numériques comme :

- ✓ Les logiciels, applications, algorithmes,
- ✓ Les créations artistiques (images, vidéos, musiques),
- ✓ Les bases de données,
- ✓ Les contenus web.

Conséquences juridiques et professionnelles

- ✓ Utilisation illégale de logiciels = délit (amendes, poursuites, blocage des services).
- ✓ Dans une entreprise ou une organisation, cela peut :
- ✓ Nuire à la réputation,
- ✓ Provoquer des sanctions internes,
- ✓ Compromettre la sécurité des données.

3. Les types d'attaques des systèmes informatiques

- **Catégorisation des attaques :**
  - Attaques par déni de service (DoS/DDoS)
  - Intrusions, phishing, man-in-the-middle
  - Exploitation de vulnérabilités (ex : injections SQL, XSS)
- **Méthodes d'attaque :**
  les techniques utilisées par les attaquants et comment ils exploitent les faiblesses des systèmes.

4. Techniques de protection

- **Politiques de sécurité :**
  Mise en place de règles et procédures internes pour sécuriser les accès et les données.
- **Mises à jour et correctifs :**
  Importance de maintenir les systèmes et logiciels à jour.
- **Gestion des identités et des accès :**
  Rôles des mots de passe robustes, authentification multi-facteurs et contrôle des privilèges.
- **Surveillance et audits :**
  Utilisation de journaux d'événements, audits réguliers et outils de monitoring pour détecter et réagir aux incidents.

5. Exploitation des Antivirus

- **Fonctionnement des antivirus :**
  - Détection par signature, heuristique et comportementale
  - Importance des mises à jour de la base de signatures.

- **Démonstration pratique :**
  Mettre en situation l'installation et la configuration d'un antivirus, et l'analyse d'un système pour détecter une infection.

6. Utilisation des firewalls

- **Rôle des firewalls :**
  Filtrer le trafic réseau entrant et sortant en fonction de règles prédéfinies pour protéger le réseau interne.
- **Types de firewalls :**
  - Firewalls matériels et logiciels
  - Firewalls de nouvelle génération intégrant des fonctionnalités avancées (inspection en profondeur, prévention d'intrusion, etc.).
- **Mise en place et configuration :**
  Expliquer comment définir et appliquer des règles de sécurité pour limiter les risques d'intrusions.

Conclusion

- **Synthèse et mise en perspective :**
  Revenir sur les points clés abordés et montrer l'interdépendance entre ces différents aspects pour construire une défense efficace des systèmes d'information.
- **Approche pédagogique :**
  Proposer des exercices pratiques, des études de cas et des mises en situation pour que les stagiaires puissent expérimenter et mieux comprendre les enjeux de la sécurité informatique.

B. Comprendre les données privées

1. Comprendre les données privées

- **Définition et types de données privées :**
  Identifier ce que l'on entend par données privées (données sensibles, informations personnelles, historiques d'activité, etc.).
- **Importance de la confidentialité :**
  La protection de ces données est cruciale pour préserver la vie privée et la confiance des utilisateurs.

2. Cadre légal et réglementaire

- **Lois sur la protection des données personnelles :**
  - Présenter les principaux textes législatifs (ex. RGPD en Europe, la loi Informatique et Libertés en France, ou d'autres lois nationales selon le contexte).
  - Discuter des implications juridiques en cas de non-conformité.
- **Exemples de sanctions :**
  Exemples d'amendes et de sanctions appliquées par les autorités compétentes :
  Entreprise sanctionnée pour usage de logiciels piratés

Cas : Maroc – 2022
Une entreprise opérant dans le secteur de l'ingénierie a été contrôlée par l'Office Marocain de la Propriété Industrielle et Commerciale (OMPIC) en partenariat avec BSA (Business Software Alliance).
Elle utilisait des copies non autorisées de logiciels comme AutoCAD et Microsoft Office.
Sanction :
Amende de 120 000 dirhams
Obligation d'acheter des licences officielles
Poursuites judiciaires envisagées en cas de récidive

3. Règles de protection des données utilisateurs

- **Mesures organisationnelles et techniques :**
  - Mettre en place des politiques de confidentialité, des audits de sécurité, et des formations régulières.
  - Décrire l'importance de la gestion des accès et de la limitation des privilèges.
- **Bonnes pratiques de stockage et de traitement :**
  - Utilisation de solutions sécurisées pour la collecte et le traitement des données.
  - Importance des sauvegardes régulières et des mises à jour de sécurité.

4. Droits d'accès des utilisateurs

- **Principes de transparence et de contrôle :**
  Les droits des utilisateurs (accès, rectification, suppression, opposition, portabilité) :
  Droits des utilisateurs sur leurs données personnelles
  Les utilisateurs ont le droit de contrôler leurs données personnelles. Ces droits s'appliquent à toute organisation (publique ou privée) qui collecte, traite ou conserve des données relatives à une personne.
- **Mécanismes de gestion des droits :**
  - Décrire les procédures permettant aux utilisateurs de consulter et gérer leurs propres données dans une application.
  - Importance d'une interface utilisateur intuitive et sécurisée pour l'exercice de ces droits.

5. Méthodes de cryptage des données

- **Concepts de base du cryptage :**
- Différence entre cryptage symétrique et asymétrique :

Cryptage Symétrique Principe :

Le cryptage symétrique utilise la même clé pour chiffrer et déchiffrer les données.
Comment ça fonctionne ?
L'expéditeur utilise une clé pour chiffrer un message.
Le destinataire utilise exactement la même clé pour déchiffrer le message.
Présentation des algorithmes courants (AES, RSA, etc.).
Cryptage Asymétrique Principe :
Le cryptage asymétrique utilise deux clés distinctes : une clé publique pour chiffrer et une clé privée pour déchiffrer.
Comment ça fonctionne ?
L'expéditeur utilise la clé publique du destinataire pour chiffrer un message.
Le destinataire utilise sa clé privée pour déchiffrer le message.

Conclusion

- **Synthèse et mise en perspective :**
  Récapituler l'importance de combiner un cadre légal solide, des pratiques de protection robustes et des techniques de cryptage avancées pour garantir la confidentialité des données.

C. Gestion de la politique d'utilisation des mots de passe

1. Gestion de la politique d'utilisation des mots de passe

- **Élaboration d'une politique de mot de passe robuste :**
  - Imposer une longueur minimale, l'utilisation de majuscules, minuscules, chiffres et caractères spéciaux.
  - Définir une durée de validité et prévoir la mise à jour régulière des mots de passe.
- **Stockage sécurisé :**
  - Utiliser des techniques de hachage (avec salage) pour le stockage des mots de passe.
- **Bonnes pratiques utilisateur :**
  - Sensibiliser les utilisateurs aux risques liés au partage ou à la réutilisation des mots de passe.

2. Gestion appropriée des rôles d'utilisateurs

- **Définition et mise en place de rôles clairs :**
  - Identifier les différents niveaux d'accès nécessaires (administrateur, éditeur, utilisateur standard, etc.).
- **Principe du moindre privilège :**
  - Accorder uniquement les droits indispensables à l'exécution des tâches.
- **Contrôles d'accès et audit :**
  - Mettre en place des systèmes de gestion des identités (IAM) pour contrôler et suivre les accès.
- **Gestion dynamique des rôles :**
  - Adapter et réviser régulièrement les rôles en fonction des évolutions des responsabilités.

3. Connaissances en types de chiffrements

- **Chiffrement symétrique :**
  - Utiliser des algorithmes tels que AES(AES est un algorithme de cryptage symétrique qui a été adopté comme **norme de cryptage** par le gouvernement américain en 2001 pour remplacer l'ancien algorithme **DES (Data Encryption Standard)**. Il est utilisé pour sécuriser des informations sensibles dans divers systèmes, y compris les communications Internet (HTTPS), le stockage de

données, et les applications de messagerie.) pour chiffrer les données en transit et au repos.

- **Chiffrement asymétrique :**
  - Employer RSA ou ECC (Le choix entre **RSA** (Rivest-Shamir-Adleman) et **ECC** (Elliptic Curve Cryptography) dépend principalement des **besoins de sécurité** et des **contraintes de performance** de votre application) pour l'échange sécurisé de clés et la protection des communications.
- **Utilisation combinée :**
  - Implémenter des protocoles hybrides (ex. TLS : (Transport Layer Security) est un protocole de sécurité conçu pour assurer des communications cryptées sur un réseau informatique, en particulier sur Internet. Il est couramment utilisé pour sécuriser les échanges de données entre les serveurs et les clients, notamment dans des applications comme la navigation web (HTTPS), les emails (SMTP, IMAP, POP3), et d'autres communications sécurisées.) qui tirent parti des avantages de chacun.
- **Sécurité des clés :**
  - Gérer et protéger correctement les clés de chiffrement (stockage, rotation et accès restreint).

4. Fonctionnement d'un firewall dans la protection d'application HTTP

- **Rôle des firewalls applicatifs (WAF) :**
  - Filtrer et surveiller le trafic HTTP/HTTPS pour détecter et bloquer les attaques courantes (ex. injections SQL, XSS, etc.).
- **Inspection en profondeur :**
  - Analyser les requêtes pour identifier des comportements anormaux et appliquer des règles de sécurité spécifiques.
- **Mise en place et configuration :**
  - Définir des règles adaptées à l'application, telles que le blocage d'adresses IP suspectes et la limitation des tentatives d'accès.
- **Surveillance et mise à jour continue :**
  - Mettre en place des outils de monitoring pour détecter les attaques en temps réel et ajuster la configuration du firewall selon l'évolution des menaces.

Conclusion

La protection des applications Web repose sur une approche globale combinant :

- Une gestion stricte des mots de passe et des rôles pour limiter l'accès non autorisé.
- Des techniques de chiffrement avancées pour garantir la confidentialité et l'intégrité des données.
- L'utilisation de firewalls applicatifs pour détecter et bloquer les attaques visant les applications HTTP.