Mission 7

Module 1 : Panorama de la SSI

La Sécurité des Systèmes d'Information (SSI) s'inscrit dans un monde numérique en constante évolution, où la connectivité et l'interconnexion ouvrent autant d'opportunités que de vulnérabilités. Voici un aperçu structuré :

---

1. Un monde numérique hyper-connecté

La transformation digitale a donné naissance à une société où les technologies connectées (IoT, réseaux sociaux, cloud computing) sont omniprésentes. Ces innovations favorisent la collaboration et l'efficacité, mais augmentent aussi la surface d'attaque pour les cybermenaces.

---

2. Un monde à hauts risques

Dans ce contexte hyper-connecté, les risques se multiplient :

- **Cyberattaques** : Vol de données, ransomware, attaques DDoS.
- **Erreurs humaines** : Mauvaise gestion des mots de passe ou phishing.
- **Espionnage industriel** : Exploitation de failles pour accéder à des informations stratégiques.
- **Risques systémiques** : Une attaque sur un acteur clé peut perturber toute une chaîne.

---

3. Les acteurs de la cybersécurité

Plusieurs parties prenantes agissent pour sécuriser le cyberespace :

- **États** : Réglementation, agences nationales (ex. : ANSSI en France).
- **Entreprises** : Investissements dans la protection des données et infrastructures.
- **Utilisateurs** : Premiers responsables de la sécurité par leurs comportements.
- **Hackers éthiques** : Identifient les failles pour prévenir les cyberattaques.

---

4. Protéger le cyberespace

La protection repose sur une approche globale :

- **Prévention** : Formation, politiques de sécurité, mise à jour régulière des systèmes.
- **Détection** : Surveillance continue, outils d'analyse pour repérer les anomalies.
- **Réaction** : Plans de reprise d'activité et gestion de crise après une attaque.
- **Innovation** : Intégration de technologies comme l'IA et la blockchain pour renforcer la sécurité.

---

5. Les règles d’or de la sécurité

Pour renforcer la SSI, quelques bonnes pratiques essentielles :

1. **Sensibiliser** les utilisateurs aux risques et aux comportements sécurisés.
2. **Utiliser des mots de passe forts** et les gérer via des outils sécurisés.
3. **Mettre à jour régulièrement** les systèmes et logiciels.
4. **Protéger les accès** (authentification multi-facteurs, VPN).
5. **Faire des sauvegardes fréquentes** pour limiter les pertes de données.
6. **Détecter les signaux faibles** grâce à des outils de monitoring.

Conclusion

La SSI est un enjeu majeur dans un monde numérique hyper-connecté. Elle repose sur une collaboration entre tous les acteurs et sur l’application rigoureuse de principes de protection et de résilience pour sécuriser les systèmes d’information face à des menaces toujours plus sophistiquées.

Module 2 Sécurité de l’authentification

L’authentification est un pilier de la sécurité des systèmes d’information. Elle garantit que seul un utilisateur autorisé peut accéder à une ressource ou un service. Voici une vue d'ensemble des concepts clés liés à la sécurité de l’authentification.

---

1. Principes de l’authentification

L'authentification repose sur trois éléments principaux, souvent combinés pour renforcer la sécurité :

- **Ce que l’on sait** : Identifiants et mots de passe.
- **Ce que l’on possède** : Un dispositif (clé USB, smartphone, carte).
- **Ce que l’on est** : Biométrie (empreintes digitales, reconnaissance faciale).

L’authentification forte combine au moins deux de ces facteurs (ex. : mot de passe + code envoyé par SMS).

---

2. Attaques sur les mots de passe

Les mots de passe sont des cibles privilégiées pour les attaquants :

- **Attaques par force brute** : Essais systématiques de combinaisons possibles.
- **Phishing** : Tromper l’utilisateur pour obtenir ses identifiants.
- **Attaques par dictionnaire** : Utilisation de listes de mots de passe courants.
- **Recyclage d’identifiants** : Exploitation de mots de passe réutilisés sur plusieurs comptes.
- **Keylogging** : Capture des frappes au clavier par un logiciel malveillant.

---

3. Sécuriser ses mots de passe

Pour limiter les risques :

- **Choisir des mots de passe forts** : Longs, aléatoires, combinant lettres, chiffres et symboles.
- **Ne jamais réutiliser un mot de passe** sur plusieurs comptes.
- **Éviter les mots de passe basés sur des informations personnelles** (dates, noms).
- **Utiliser l’authentification multi-facteurs** (MFA) pour ajouter une couche de sécurité.

---

4. Gérer ses mots de passe

Pour gérer efficacement ses mots de passe :

- **Utiliser un gestionnaire de mots de passe** : Ces outils permettent de générer et stocker des mots de passe complexes de manière sécurisée.
- **Sauvegarder les mots de passe importants** dans un endroit sûr (support chiffré ou physique).
- **Mettre à jour régulièrement** les mots de passe sensibles ou exposés.

5. Notions de cryptographie

La cryptographie est essentielle pour sécuriser l’authentification et les données :

- **Hashage des mots de passe** : Technique qui transforme un mot de passe en une empreinte unique et non réversible. Les fonctions comme **SHA-256** sont courantes.
- **Chiffrement symétrique** : La même clé sert pour chiffrer et déchiffrer les données.
- **Chiffrement asymétrique** : Utilisation d’une clé publique pour chiffrer et d’une clé privée pour déchiffrer.
- **Certificats numériques** : Vérifient l’identité des parties dans une connexion sécurisée (ex. : HTTPS).

Conclusion

La sécurité de l’authentification repose sur des principes solides, mais elle est continuellement menacée par des attaques sophistiquées. Adopter des mots de passe forts, utiliser des outils adaptés comme les gestionnaires de mots de passe et intégrer des technologies cryptographiques sont essentiels pour garantir la protection des données et des accès

Module 3 : Sécurité d’Internet

Internet est un outil incontournable pour la communication, le partage d'informations et les services en ligne. Cependant, son utilisation expose les utilisateurs à divers risques liés à la navigation, aux fichiers téléchargés et aux connexions. Voici une vue d'ensemble des aspects essentiels pour comprendre et sécuriser son utilisation d'Internet.

---

1. Internet : de quoi s’agit-il ?

Internet est un réseau mondial interconnectant des millions de dispositifs, permettant la transmission d’informations via des protocoles standardisés comme HTTP, FTP ou SMTP. Il repose sur des infrastructures telles que les serveurs, les réseaux et les fournisseurs d'accès (FAI).

---

2. Les fichiers en provenance d’Internet

Les fichiers téléchargés sur Internet peuvent être porteurs de risques :

- **Logiciels malveillants** (virus, ransomwares, chevaux de Troie).
- **Documents piégés** contenant des macros ou scripts malveillants.
- **Failles de sécurité** exploitables via des fichiers.

Bonnes pratiques :

- Scanner les fichiers avant de les ouvrir avec un antivirus.
- Télécharger uniquement depuis des sources fiables.
- Mettre à jour régulièrement les applications de lecture (PDF, vidéos, etc.).

---

3. La navigation web

Naviguer sur le web peut exposer à :

- **Sites malveillants** : Tentatives de phishing, diffusion de malware.
- **Suivi des activités** : Traqueurs publicitaires, cookies, collectes de données personnelles.

Mesures de protection :

- Utiliser des navigateurs sécurisés et régulièrement mis à jour.
- Activer les bloqueurs de publicités et les extensions contre le suivi.
- Préférer les sites sécurisés en HTTPS.

---

4. La messagerie électronique

Les e-mails sont une porte d’entrée courante pour les cyberattaques :

- **Phishing** : Tentatives d’usurpation d’identité pour obtenir des informations sensibles.
- **Pièces jointes infectées** : Documents ou fichiers contenant des logiciels malveillants.
- **Liens frauduleux** : Redirections vers des sites malveillants.

Bonnes pratiques :

- Ne pas ouvrir d’e-mails ou de pièces jointes provenant d’expéditeurs inconnus.
- Vérifier les liens avant de cliquer (survoler pour voir l’URL).
- Activer les filtres anti-spam et signaler les messages suspects.

---

5. L’envers du décor d’une connexion Web

Chaque connexion web repose sur des échanges invisibles pour l’utilisateur :

- **Adresses IP** : Identifient les appareils connectés, souvent exploitées pour localiser ou suivre l’utilisateur.
- **Serveurs DNS** : Convertissent les noms de domaine en adresses IP.
- **Cookies et trackers** : Collectent des informations sur les habitudes de navigation.
- **Risques associés** : Collecte de données personnelles, redirections malveillantes.

Conseils pour sécuriser sa connexion :

- Utiliser un VPN pour masquer son adresse IP et sécuriser les échanges.
- Paramétrer les cookies pour limiter leur collecte.
- Éviter les réseaux Wi-Fi publics ou utiliser une connexion sécurisée (VPN).

Conclusion

Internet est un outil puissant mais potentiellement risqué. Une utilisation sécurisée repose sur des pratiques comme le choix de sources fiables, la vigilance face aux contenus suspects, la navigation sur des sites sécurisés et la protection de sa vie privée via des outils comme le VPN et les bloqueurs de traqueurs. La sensibilisation aux menaces est la première défense pour protéger ses données et ses activités en ligne.

Module 4 : Sécurité du poste de travail et nomadisme

Le poste de travail est une cible privilégiée des cyberattaques, surtout dans un contexte de nomadisme (télétravail, déplacements). Garantir sa sécurité repose sur des configurations adaptées, des mises à jour régulières et des pratiques rigoureuses.

---

1. Applications et mises à jour

Les applications et systèmes d'exploitation nécessitent des mises à jour régulières pour corriger les failles de sécurité :

- **Mises à jour automatiques** : Activer pour bénéficier rapidement des correctifs.
- **Installation d'applications fiables** : Télécharger uniquement depuis des sources officielles.
- **Désinstallation des logiciels inutiles** : Réduire la surface d'attaque en supprimant les programmes obsolètes ou non utilisés.

---

2. Options de configuration de base

Les réglages par défaut doivent être ajustés pour renforcer la sécurité :

- **Activer le pare-feu** pour bloquer les connexions non autorisées.
- **Configurer des mots de passe robustes** pour les comptes utilisateurs.
- **Limiter les privilèges** des utilisateurs standards pour éviter des modifications accidentelles ou malveillantes.

---

3. Configurations complémentaires

Certaines mesures avancées augmentent la protection :

- **Chiffrement des données** (ex. : BitLocker sous Windows) pour protéger les fichiers en cas de vol ou de perte.
- **Authentification multi-facteurs (MFA)** pour renforcer l'accès aux services critiques.
- **Antivirus et anti-malware** : Installer des solutions de protection et les maintenir à jour.

---

4. Sécurité des périphériques amovibles

Les clés USB, disques durs externes et autres périphériques représentent un risque potentiel :

- **Scanner les périphériques avant utilisation** pour détecter d'éventuels virus.
- **Restreindre les autorisations** d'exécution automatique pour empêcher l'installation de programmes malveillants.
- **Utiliser des périphériques chiffrés** pour protéger les données sensibles.

---

5. Séparation des usages

Séparer les usages personnels et professionnels est essentiel pour limiter les risques :

- **Utiliser des comptes distincts** sur l’ordinateur pour chaque usage.
- **Éviter d’installer des applications personnelles** sur les dispositifs professionnels.
- **Ne pas mélanger les réseaux** : Privilégier un VPN pour les connexions professionnelles à distance.

Conclusion

La sécurité du poste de travail, particulièrement dans un contexte nomade, repose sur des pratiques préventives et des configurations adaptées. Une attention particulière aux mises à jour, à la gestion des périphériques et à la séparation des usages contribue à protéger les données et l’intégrité des systèmes, même en dehors du cadre professionnel habituel.