# Module 1 : Panorama de la Sécurité des Systèmes d'Information (SSI)

1. Présentation de la SSI :
La sécurité des systèmes d'information (SSI) est le pilier central de la protection des données numériques et repose sur le triptyque CIA: Confidentialité, Intégrité, et Disponibilité.
- Confidentialité: Ce principe garantit que seules les personnes autorisées ont accès aux informations sensibles. Par exemple, des mesures telles que le chiffrement des données et la gestion stricte des autorisations d'accès sont essentielles pour maintenir cette confidentialité.
- Intégrité: L'intégrité assure que les données ne sont ni modifiées ni altérées de manière non autorisée. Des mécanismes tels que les contrôles de somme de contrôle (hashing) et les systèmes de vérification des signatures numériques contribuent à protéger cette intégrité.
- Disponibilité: Cela signifie que les informations et les systèmes doivent être accessibles aux utilisateurs autorisés lorsque cela est nécessaire. Des exemples incluent la mise en place de serveurs redondants et de systèmes de sauvegarde pour éviter les interruptions de service.

2. Enjeux de la cybersécurité :

La cybersécurité est devenue primordiale en raison de la prolifération des cybermenaces, dont la gravité et la fréquence augmentent chaque année. Le module souligne les attaques notoires qui ont exposé des millions de données personnelles, démontrant l'impact significatif des failles de sécurité sur les entreprises et les individus. Par exemple, les cyberattaques célèbres telles que celles ayant visé des infrastructures critiques montrent la nécessité d'une préparation et d'une vigilance accrues.

3. Acteurs de la sécurité :
La sécurité des systèmes d'information implique divers acteurs :
- Utilisateurs: Ils jouent un rôle clé, car leurs comportements peuvent renforcer ou compromettre la sécurité. Une simple négligence, telle que cliquer sur un lien de phishing, peut exposer l'ensemble du système.
- Administrateurs système: Responsables de la configuration et de la maintenance des systèmes, ils doivent s'assurer que les mesures de sécurité telles que les pare-feu et les logiciels de détection d'intrusion (IDS) sont en place et à jour.
- Autorités de régulation: Des organismes tels que l'ANSSI en France élaborent des normes de sécurité et fournissent des recommandations pour protéger les infrastructures critiques.

4. Menaces et vulnérabilités :

Le module explore un large éventail de menaces, notamment :
- Logiciels malveillants (malwares): Ces programmes nuisibles, tels que les virus, les vers, et les ransomwares, infiltrent les systèmes pour voler ou détruire des données. Par exemple, le ransomware WannaCry a paralysé des centaines d'organisations en 2017.
- Phishing: Une technique d'ingénierie sociale visant à tromper les utilisateurs pour qu'ils révèlent des informations sensibles.
- Attaques DDoS: Elles visent à rendre un service indisponible en saturant les serveurs de requêtes.

La distinction entre vulnérabilité (faiblesse d'un système) et menace (potentiel d'exploitation de cette faiblesse) est cruciale. L'évaluation régulière des systèmes permet de prévenir l'exploitation des vulnérabilités grâce à des tests de pénétration et des audits de sécurité.

5. Bonnes pratiques de sécurité :
Le module recommande des stratégies de protection telles que :
- Mots de passe complexes et uniques: Ils doivent être combinés avec l'utilisation de gestionnaires de mots de passe pour en faciliter la gestion.
- Mises à jour régulières: Assurer que tous les logiciels et systèmes sont à jour pour protéger contre les vulnérabilités connues.
- Pare-feu et antivirus: Utilisés pour surveiller et filtrer le trafic entrant et sortant des réseaux.
- Sensibilisation des utilisateurs: La formation continue sur les bonnes pratiques, comme le non-partage des informations d'identification, est essentielle pour prévenir les erreurs humaines.

## Module 2 : Sécurité de l'authentification

Le module Sécurité de l'authentification se concentre sur la protection de l'accès aux systèmes d'information et explore les méthodes pour garantir que seuls les utilisateurs autorisés puissent accéder aux données sensibles.

1. Définition et principes de l'authentification :
L'authentification est le processus qui confirme l'identité d'un utilisateur. Cette étape va au-delà de l'identification (qui consiste à déclarer qui l'on est) et inclut des mécanismes de vérification tels que l'utilisation de mots de passe ou de technologies biométriques.

2. Méthodes d'authentification :
Plusieurs méthodes sont expliquées en détail :
- Authentification par mot de passe : Bien que courante, elle reste vulnérable aux attaques par force brute et autres.
- Authentification biométrique : Utilisant des caractéristiques uniques de l'utilisateur, elle améliore la sécurité mais peut poser des questions de confidentialité.
- Clés de sécurité : Des dispositifs matériels comme les clés USB sécurisées

garantissent un niveau de sécurité supplémentaire.

3. Authentification multifacteur (MFA) :
La MFA est mise en avant pour sa capacité à combiner plusieurs types de preuves (mot de passe, empreinte digitale, code envoyé par SMS) afin de sécuriser davantage l'accès. Cette méthode réduit considérablement le risque de compromission en exigeant plusieurs étapes pour valider l'identité de l'utilisateur.

4. Risques et défis de l'authentification :
Des défis comme la gestion des mots de passe, la réutilisation sur plusieurs comptes, et les attaques d'ingénierie sociale sont discutés. Le module suggère des solutions telles que l'utilisation de mots de passe générés aléatoirement et l'adoption de gestionnaires de mots de passe pour simplifier cette gestion. Des audits de sécurité réguliers sont également recommandés pour identifier les faiblesses potentielles.

5. Bonnes pratiques :
- Changer régulièrement les mots de passe : Cela réduit le risque d'utilisation d'informations compromises.
- Utilisation de la MFA : Recommandée pour la majorité des accès sensibles.
- Sensibilisation des utilisateurs : Informer sur les techniques de phishing et les pratiques de sécurité aide à prévenir les attaques.

Conclusion du module 2 :
L'authentification est présentée comme un élément fondamental de la sécurité des systèmes d'information. En combinant des méthodes modernes et une sensibilisation constante des utilisateurs, il est possible de limiter les risques liés à l'accès non autorisé.

Ces modules offrent une compréhension essentielle et approfondie de la sécurité des systèmes d'information et de l'authentification. Le premier module présente les bases de la protection des données et des systèmes, tandis que le second détaille comment renforcer la sécurité par des méthodes d'authentification avancées et des pratiques exemplaires.

**Compte rendu module 3**

Le **module 3** de la formation **SecNumAcadémie** de l'ANSSI, intitulé **"Sécurité sur Internet"**, se concentre sur les bonnes pratiques et les risques associés à l'utilisation d'Internet au quotidien. Ce module est conçu pour aider les utilisateurs à comprendre les menaces qui pèsent sur leur sécurité numérique lorsqu'ils naviguent en ligne et à adopter des comportements plus sûrs. Voici un résumé détaillé des principaux thèmes abordés dans ce module.

1. **Introduction à Internet et ses risques**

Le module commence par une vue d'ensemble du fonctionnement d'Internet et des services qu'il offre, comme le web, les mails, et les applications en ligne. Il est essentiel de comprendre qu'Internet, bien que source de nombreuses ressources, représente également un terrain propice pour les cybercriminels. Ils peuvent exploiter les failles de sécurité pour commettre des fraudes, installer des malwares ou espionner les utilisateurs.

2. **Les fichiers téléchargés depuis Internet**

Un point crucial abordé dans ce module concerne les **fichiers téléchargés**. Beaucoup de cyberattaques débutent par l'ouverture de fichiers malveillants. Ces fichiers peuvent être dissimulés dans des pièces jointes d'emails, des téléchargements depuis des sites non sécurisés, ou même dans des publicités. Le module conseille de toujours vérifier la source des fichiers avant de les télécharger, d'éviter les fichiers exécutables provenant de sources non fiables, et de mettre en place des protections comme les antivirus pour les analyser.

3. **La navigation web sécurisée**

Naviguer sur Internet de manière sécurisée est essentiel pour éviter les attaques. Le module met en lumière l'importance de **l'utilisation du protocole HTTPS** lors de la connexion à des sites web. HTTPS garantit que la connexion entre l'utilisateur et le site est cryptée et sécurisée. En revanche, les sites HTTP (non sécurisés) présentent un risque accru d'interception des données personnelles. Les utilisateurs doivent également se méfier des sites web qui semblent suspects, éviter de télécharger des contenus à partir de sites inconnus, et bien gérer les **cookies** qui peuvent être utilisés pour collecter des informations personnelles sans leur consentement.

4. **La messagerie électronique et les attaques par phishing**

La messagerie électronique est l'un des vecteurs d'attaque les plus utilisés par les cybercriminels, principalement par le biais de **phishing**. Le phishing est une technique consistant à tromper l'utilisateur en lui envoyant un message qui semble provenir d'une source fiable (comme une banque ou un service en ligne), mais qui a pour but de récupérer des informations sensibles comme des identifiants ou des numéros de carte bancaire. Le module enseigne comment identifier les emails suspects, vérifier les liens avant de cliquer, et éviter de répondre à des sollicitations non sollicitées.

5. **L'envers du décor d'une connexion Internet**

Une autre partie du module se concentre sur la **compréhension des connexions Internet** et des termes techniques qui y sont associés, tels que **les DNS (Domain Name System)**, **les adresses IP**, et **les routes de données**. Ces éléments sont essentiels pour comprendre comment les cybercriminels peuvent exploiter les failles de sécurité dans les protocoles de communication Internet. Par exemple, une mauvaise configuration des DNS ou une connexion non sécurisée peut rendre une machine vulnérable à des attaques par **interception de données** ou **détournement de session**.

**Conclusion**

Le module 3 de SecNumAcadémie fournit une base solide pour comprendre les risques auxquels les utilisateurs sont exposés sur Internet et propose des solutions concrètes pour renforcer la sécurité. En appliquant les bonnes pratiques recommandées dans ce module, les utilisateurs peuvent réduire considérablement leur exposition aux cyberattaques et protéger leurs informations personnelles. Ces connaissances sont essentielles non seulement dans un cadre professionnel, mais aussi dans la vie privée, afin d'agir de manière plus sécurisée au quotidien sur Internet.

**Compte rendu module 4**

Le **module 4 de SecNumAcadémie**, intitulé *"Sécurité du poste de travail et nomadisme"*, est axé sur la protection des équipements informatiques, en particulier ceux utilisés dans des contextes de travail mobile ou à distance. Il aborde diverses techniques et bonnes pratiques pour sécuriser les appareils, éviter les failles et prévenir les attaques. Voici un développement détaillé des principaux thèmes abordés.

1. **Applications et mises à jour**

L'un des points essentiels de ce module est de maintenir toutes les **applications** de votre poste de travail à jour. En effet, les cybercriminels exploitent souvent des **vulnérabilités non corrigées** dans les logiciels pour pénétrer les systèmes. Cela peut inclure les systèmes d'exploitation, les logiciels de productivité, les navigateurs web, mais aussi les applications mobiles utilisées dans le cadre du travail.
Les mises à jour automatiques et les patchs de sécurité permettent de fermer ces portes laissées ouvertes par des failles de sécurité, et de réduire ainsi les risques d'infection par des malwares, des rançongiciels ou des attaques par exploitation de vulnérabilité.

2. **Options de configuration de base**

Le module insiste sur l'importance de la configuration sécurisée dès le début de l'utilisation d'un appareil. Cela inclut :

- **La gestion des mots de passe** : Utilisation de mots de passe complexes et uniques, et activation de l'authentification à deux facteurs (2FA) lorsque possible.
- **Le pare-feu** : Assurer que le pare-feu de l'ordinateur est activé et configuré correctement afin de filtrer le trafic réseau et prévenir les intrusions.
- **L'antivirus** : Installer un logiciel antivirus fiable pour détecter et bloquer les menaces avant qu'elles n'affectent le système. Un antivirus à jour est indispensable pour la détection en temps réel des virus et des malwares.

3. **Configurations complémentaires**

Une fois les configurations de base mises en place, il existe des configurations **complémentaires** qui augmentent encore la sécurité. Ces configurations incluent :

- **Le chiffrement des données** : Cette technique permet de protéger les informations stockées sur le poste de travail. Si l'appareil est volé ou perdu, les données restent illisibles sans la clé de déchiffrement.
- **La séparation des profils utilisateurs** : Créer des espaces de travail distincts pour séparer les activités professionnelles et personnelles. Cela permet d'éviter qu'une infection provenant d'un usage personnel n'atteigne les données professionnelles sensibles.

4. **Sécurité des périphériques amovibles**

Les périphériques amovibles, tels que les **clés USB**, les disques durs externes, ou encore les cartes SD, sont souvent utilisés pour transporter des données, mais ils peuvent aussi être des vecteurs d'attaque. Un périphérique infecté peut transmettre des malwares à votre ordinateur en étant simplement branché. Le module recommande de :

- Désactiver l'auto-exécution de ces périphériques.
- Utiliser des logiciels de chiffrement pour protéger les données stockées sur ces supports.
- Ne jamais connecter des périphériques provenant de sources inconnues ou non fiables.

5. **Séparation des usages et gestion des appareils dans un contexte de nomadisme**

Le module aborde également la question de la **séparation des usages**. Lorsque des appareils sont utilisés à la fois pour des activités professionnelles et personnelles, il est crucial de les protéger contre la contamination croisée. Par exemple :

- **Utiliser des outils comme des machines virtuelles** ou des comptes séparés pour créer des espaces distincts pour chaque type d'usage.
- **Utiliser des appareils dédiés** pour des activités sensibles, comme les transactions financières ou les communications professionnelles.

Le **nomadisme**, ou le travail à distance, pose des défis supplémentaires en matière de sécurité. Il est important de protéger les connexions sans fil utilisées dans ces contextes (Wi-Fi public, par exemple) et d'assurer que les dispositifs mobiles utilisés sont protégés par des mécanismes de sécurité, comme le chiffrement des données, des mots de passe complexes et l'activation des systèmes de localisation pour pouvoir retrouver un appareil perdu ou volé.

**Conclusion**

Le module 4 de SecNumAcadémie offre une série de recommandations pratiques pour sécuriser les appareils de travail, en particulier dans des contextes où la mobilité et le travail à distance sont de plus en plus courants. Ces recommandations sont cruciales pour éviter les intrusions, protéger les données sensibles et garantir une bonne hygiène de sécurité numérique. En combinant des configurations de base robustes, des mises à jour régulières, la gestion des périphériques amovibles, et l’adoption de bonnes pratiques de sécurité dans des environnements mobiles, les utilisateurs peuvent se protéger efficacement contre les menaces croissantes.