**Sécurité des systèmes et des réseaux**

**1 - Définition et objectifs**

Définition :

l’ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires

mis en place pour conserver, rétablir et garantir la sécurité des systèmes informatique

Objectifs :

minimiser la vulnérabilité d’un système informatique

se protéger contre des menaces intentionnelles ou des menaces accidentelles

**2 - Vocabulaires**

**vulnérabilité** : 脆弱性

faille introduite de manière intentionnelle ou accidentelle

**attaque** : 攻击

action malveillant visant à exploiter une vulnérabilité d’un système

**intrusion** : 侵入

faute externe résultant de l’exploitation réussie d’une vulnérabilité

**menace** : 威胁

violation potentielle d’une propriété de sécurité

**risque** : 危机

menace + vulnérabilité

**virus** : 病毒

exécuter s’autoréplique et se greffe sur un autre programme pour en modifier le comportement, ex : cheval de Troie

**vers** : 蠕虫

un programme malveillant qui se diffuse à travers le réseau, il fonctionne de manière autonome et ne se réplique pas sur la machine

**spyware** : 间谍软件

collecter et transmettre des données sur le réseau à l’issue de l’utilisateur du système compromis

**bombe** **logique** : 逻辑炸弹，隐藏在电脑程序中旨在破坏他人电脑程序的

rester en sommeil jusqu’à ce que des conditions particulières surviennent pour causer des dommages

**porte** **dérobée** : 隐藏门

contourner un mécanisme de sécu à l’issue de l’utilisateur, une vulnérabilité du système qui peut être intentionnelle ou accidentelle, dans le but de teste et de maintenance

**cheval** **de** **Troie** ：木马病毒

des actions néfastes sous l’apparence d’un programme autorisé.

**spam** : 垃圾邮件

message non sollicité obtenue par une utilisation abusive d’une boîite mail

**sniffing** : 数据盗窃

accès illégal à des données sur un canal de communication ou sur un support vulnérable pour obtenir des informations sensibles

**sppofing** : 电子欺骗

usurpation d’identité pour obtenir des informations ou des accès

**déni de service (DDS et dDDS)** : 拒绝服务攻击没事目标电脑的网络或系统资源耗尽，使服务暂时终端或停止，使其对目标客户不可用

attaque d’un serveur ayant pour but de l’empêcher de rendre son service

dDDS s’appuie sur plusieurs certaines de terminaux zombis pour générer les requêtes

**3 - CID**

**confidentialité : 秘密性**

garder secret le contenu d’une information

mettre en place des mécanismes pour rendre cette information inintelligible par des tiers non autorisés : lors de la conservation/sauvegarde/transfert

la nécessité de laisser à un usager le contrôle sur des informations personnelles

**intégrité ：完整性**

assuré par tous les moyens contre les modifications accidentelles/volontaires

objectif : assurer que des informations sauvegardées ou transmis sont bien conforme aux données d’origine

nécessite la mise en place de contrôle d’accès pour la modification des données

**disponibilité ：无拘束性**

les données doivent être accessibles de manière fiable par toutes les entités autorisées

consiste à mettre en oeuvre les moyens matériels nécessaires pour assurer la bonne conservation des données/bonne fonctionnement du système

mettre en oeuvre un système de redondance des services pour palier à l’indisponibilité d’un servivce particulier

**authenticité/authentification ：真实公正性**

objectif : assurer qu’une entité est bien ce qu’elle prétend être (garantir la qualité de l’information qu’elle fourni, s’assurer qu’elle a le droit d’effectuer certains actions)

transmissions l’authenticité : s’assurer que l’information reçue est bien celle qui avait été envoyé

authenticité d’une personne/identification : limiter les accès aux seules ressources nécessaires

permettre de vérifier l’origine d’une information/l’identité d’une personne

**traçabilité ：可追溯性**

pouvoir être tracée de manière à permettre de détecter une faille à posteriori

indispensable pour disposer de prouves lors d’une intrusion ou pour prouver la modification de données

assurer la non répudiation de certaines actions qui ont pu être effectuées sur le système

**4 - démarches à voir**

identification et évaluation des risques

établissement d’une politique de sécurité

mise en place de la solution de sécurité des contres mesures

auditer/évaluer la solution mise place

**5 - Quelques procédures**

domaine à protéger : il ne faut protéger que le nécessaire

architecture de sécurité : équipements, paramètres de sécurité et mécanismes de prévention et de détection

prévoir les failles : plan de continuité d’activité, plan de reprise d’activité

élaboration de charte à destination des utilisateurs : sensibilisation aux risques, faire adhérer à la politique globale

gérer l’évolution des RH et du système : déf d’un organigramme précis avec les responsabilité de chacun

méthodes de développement sûres, de mise à jour des failles

**6 - facteur humain**

élément le plus important d’une politique de sécurité

vulnérabilités vienent des utilisateurs : non respect des procédures, incompréhension de l’intérêt d’une procédure, surcharge induite par des procédures sur l’activité

système n’est fiable que si tout le monde : ne donne pas son mot de passe à un collègue, ne le laisse pas sur un post-it

**7 - architecture de sécurité OSI**

objectif : fournir une approche systématique pour évaluer et choisir des moyens de sécurité adapté à des communications distribuées

3 aspects

attaques : passives,actives

mécanismes de sécurité : détection, prévention, récupération

services de sécurité : amélioration de la sécurité, mise en échec des attaques

**8 - attaques passives**

objectif : obtenir des informations sur une transmission d’informations, n’altère pas d’information

2 grands types d’attaques : écoute clandestine, capture et analyse de trafic

très difficile à détecter

**9 - attaques actives**

impliquer une altération de la communication :

usurpation d’identité : une personne se fait passer pour une autre n créant des données contenant de fausses informations (peut être assimilé à la contrefaçon)

rejeu : dans le but frauduleux pour btenir un accès normalement interdit, des réponses pour déterminer un mot de passe, incrémenter des revenues

altération de messages : modification des paquets d’une communication pour ajouter/supprimer/modifier l’information qu’il transporte

déni des service : envoie un très grand nombre d’informations (requêtes ou données) pour rendre le service inopérant, relativement simple à mettre en oeuvre

**10 - but des attaques**

4 objectifs :

interruption : qui vise la disponibilité des informations

interception : qui vise la confidentialité des informations

modification : qui vise l’intégrité des informations

fabrication : qui vise l’authenticité des informations

**11 - prévention des attaques**

attaques passives : difficile à détecter mais simple à prévenir

mettre en place des mécanismes pour les prévenir, ex : cryptage de l’info etc

attaques actives : simple à détecter mais difficiles à arrêter

mettre l’accent sur la détection et sur la récupération, ex : firewall etc

**12 - mécanismes de sécurité**

moyens de défense : détecter, prévenir, récupérer

quelques mécanismes :

authentification : mécanisme central, authentifier un acteur peut se faire à l’aide de trois aspects, identifier l’émetteur d’un message

chiffrement des données : algo à base de clés permettant de transformer mes données

signature des données : données ajouté aux infos transmise pour assurer l’authenticité du message

contrôle d’accès : au système§moyen de communication

contrôle de routage : sécurisation des chemins empruntés et des mécanismes d’interconnexion

bourrage de trafic : des données sont ajoutées pour assurer la confidentialité en particulier au niveau du volume de trafic

notarisation : utilisation de tiers de confiance pour assurer certains services de sécurité

protection physique : attention aux support papiers

**13 - retour sur la chaîne de confiance**

un ami sur :

les organismes de certifications permettent de répondre à ce problème

établissement de graphes de confiance

il faut néanmoins tjs avoir la possibilité de révoquer la confiance accordée

**14 - services de sécurité**

authentification, contrôle d’accès, confidentialité des données, intégrité des données, non répudiation des données

**15 - principe du moindre privilège**

tout ce qui n’est pas explicitement autorisé sont interdit

il ne faut autoriser que ce qui est utilise et justifié par les tâches de l’utilisateur

attention néanmoins à ne pas tomber dans l’excès

ergonomie doit être présevé

**16 - défense en profondeur**

consiste à utiliser plusieurs techniques de sécurités parfois redondante pour arrêter/ralentir l’attaquant, ex : antivirus, pare-feu