Notes de cours de sécurité des applications

Yann Miguel

16 mars 2021

Table des matières

1 Introduction

Un système d'information est composé d'actifs, c'est à dire d'objets à protéger. Quand on parle de sécuriser, on parle de réduire les risques, et non pas de les annuler.

Les tentatives d'intrusion sur des système d'information ou des pc personnels ne sont pas nouveau, elles existent depuis les années 1980.
Le but en général est l'acquisition de données pour les revendre, ou l'acquision de ressources pour les mettre à dispositions pour d'autres attaques.

L'année 2020 a établit un nouveau record en terme de quantité de notifications d'attaques informatiques.

Il y a trois critères pour déterminer le niveau de sécurité requis:

1. Disponibilité = accessibilité au moment voulu
2. Intégrité = exactitude et complétude
3. Confidentialité = accèssible que à ceux qui en ont besoin

Il y a souvent un critère complémentaire associé à ces trois là, la Preuve, qui est équivalent à une confiance suffisante. Il n'est pas obligatoire d'avoir un niveau de protection très fort sur chaque critère, il faut donc les prioriser.

Il n'y a pas de distinction nette entre surêté et sécurité. Le but d'un expert de sécurité est donc de s'assurer que les vulnérabilités sont maitrisées.

2 Cours 1

Afin de mieux le protéger contre des menaces, il est important de fairte un inventaire des composants du système d'information. Il est aussi crucial de connaître les connections réseaux utilisées par les composants afin de pouvoir sécuriser au maximum ces interactions, et les points de connection vers ces réseaux.

Afin de sécuriser un réseau interne, il est intéressant de le séparer en plusieurs sous-réseaux afin d'isoler les éléments les plus sensibles, et d'en empêcher l'accès depuis des sources non controllées.

Il faut faire attention au matériel personnel, qui n'est pas forcément aussi bien maintenu ou sécurisé que le matériel professionnel de l'établissement.

Sécurisation du wifi:

- utiliser WPA2 et CCMP(Counter Cipher Mode Protocol)
- modifier le SSID du wifi
- changer les identifiants par défault de la box
- chiffrer les communication par clé
- ne surtout pas utiliser le WPS sans l'option qui le désactive après 5 tentatives de clé loupées
- Si vous devez utiliser un wifi public, utilisez un VPN.

Il faut toujours attribuer le minimum possible de droits et de privilège à chaque utilisateur.

3 Cours 2

Deux types d'écoutes de traffic:
- passive, il écoute juste la conversation
- active, il écoute et peux modifier le contenu de la conversation

On peux utiliser un pare-feu pour filtrer les paquets qui vont entre un réseau et l'extérieur.
On peux contrer des DDOS avec un distributeur de charge, qui va répartir le traffic sur plusieurs serveurs, et va donc diminuer les chances de surcharge du serveur.

4 Cours 3

mesur de sécurité != selon organisation (type de donnée, taille orga)
normes iso 27k: normes internationales de sécu d'info
classi des infos sur diff levels pr donner le bon level de sécu used
sécu sys info != sécu projet, même si sécu sys info peut être obj projet

5 Informations importantes