05/12/2016

Rapport TP 1

Audit

Aurélien Monnet-Paquet
M2 CYCERSECURITY

Table des matières

Audit de sécurité de la salle F103 de l'IM2AG 2
1. Organisation 2
2. Sécurité physique du site 2
3. Bios 2
4. Réseaux 3
5. Mon PC portable 3
6. Mon smartphone 4

Audit de sécurité de la salle F103 de l'IM2AG

1. Organisation

L'équipe du service info du bâtiment im2ag se situe au deuxième étage en F205.
Pour les contacter : im2ag-cmi@ujf-grenoble.fr ou au 0476635484.

La politique de sécurité des SI n'est pas disponible et la charte d'utilisation n'est pas à jour.

Recommandations :

Mettre à jours la politique de sécurité et la charte d'utilisation puis les mettre à disposition des étudiants et du personnel.

2. Sécurité physique du site

Salle protégée par accès par badge. (Badge falsifié par deux étudiants de l'ensimag au passage, à vérifier avec les nouveaux badges en cours de déploiement à ce jour).

Détecteur de mouvement dans la salle. On peut imaginer un système de détection d'intrusion.

Les boitiers des ordinateurs sont protégés par des câbles antivol mais pas les périphériques.

Il me semble déjà avoir assisté à une coupure de courant dans une autre salle du bâtiment et les ordinateurs mis à dispositions n'étaient plus alimentés donc il n'y a pas d'onduleur pour les ordis.

Pas de sortie d'urgence par l'extérieur.

Détection incendie automatique inexistante (ainsi que le chauffage).

Recommandations :

Vérifier s'il n'est pas possible de falsifié les badges d'accès.

Vérifier la présence d'incendie automatiquement via détecteur de fumée / contrôle de la température de la pièce.

Mettre du matériel antivol sur les périphériques.

3. Bios

Un mot de passe est requis pour accéder au BIOS.
Le mot de passe résiste aux tentatives naïves et mot de passe par défaut.

4. Réseaux

Un accès root est disponible sur chaque machines configurées de la même manière par défaut.

Il existe deux réseaux distincts dans la salle F103.

Premier réseau sur le port rouge :

- Adresse privées en 192.168.142.0/24
- 192.168.142.1 est un routeur
- 192.168.142.2 est un serveur NFS
    - Il est possible de monter le serveur NFS en local
        - mount -o 192.168.142.2:/srv /local
    - Nous avons ainsi la topologie du serveur
        - Notamment un (ensemble de) disque totalisant 6 To de données disponibles.
- Internet via le proxy

Deuxième réseau sur le port bleu :

- Pas de serveur DHCP
- Internet sans le proxy

Recommandation :

Mettre un serveur DHCP en état de marche pour le réseau bleu.

5. Mon PC portable

Chiffrement des partitions contre l'exploitation de mes données personnelles en cas de vol.

Ajout d'un mot de passe BIOS.

Installation d'une application antivol (« Prey »).

Utilisation d'un VPN contre la localisation et pour augmenter la privacy.

Sauvegarde de l'adresse MAC.

Sauvegarde des données importante.

Configuration du pare-feu.

Mises à jour effectuées dès que possible.

6. Mon smartphone

Dernière mise à jour installée.

Chiffrement des données (mémoire + disque).

Utilisation d'applications de chiffrement de communication (Signal, Telegram, Wickr Me).

Utilisation d'un VPN.

Sauvegarde de l'IMEI + MAC + IMSI.

Installation d'une application antivol (« Prey »).