Data Security

Ce repository contient les cours, les exercices et les sources du module Data Security du Bachelor CSI.

Le support de cours est disponible dans le dossier `./doc/build/pdf` au format PDF.

Raison d'être

Parmi les assets d'un SI on trouve :

- Le code source
- Les données
- Les configurations
- Les secrets
- L'infrastructure

En cas de souci de cyber sécurité les risque le plus grand pour l'entreprise est la fuite de données. Les trois grandes sources de revenue des pirates sont :

- Les ransomware qui chiffrent tout le système si possible. Il y a donc eu un accès à la machine (serveur ou poste). Il impacte alors le maintient en condition opérationnelle. La confidentialité des données, leur intégrité. Potentiellement les sources du logiciel. En 2021 5 millions de dollars pour le redémarrage du Colonial Pipeline Que les victimes paient la rançon ou non mais surtout s'ils ne paient pas, les données finissent sur des forums de pirates type RaidForum ou darkweb, etc. Quels sont les moyens de rentrer sur le serveur ?
  - Privilege escalation, reverse shell, RCE mais comment ?
    * L'interface entre le serveur et le web est souvent le point d'entrée. Comme par example avec Nginx et ce buffer overflow qui peut mener à une RCE.
    * Sur les drivers Linux de chipset WiFi
    * Définir me fuzztesting
    * Philips Hue RCE
    * L'avantage du close source est que les failles sont moins connues, "security through obscurity".
    * Désavantage du close source, les failles sont moins connues, donc moins de gens pour les corriger. Exemple de Log4j dans Tableau Software, on est tributaire de la communication de l'éditeur.

    Les moyens de remédiation contre ces attacks de type zero day :
  - Les données publiques qui ne devraient pas l'être à cause de serveurs mal configurés ou mauvaises pratiques. Ces données peuvent contenir

des mots de passe, des informations personnelles, des données sensibles, etc :

    * Un fichier de log qui contient des mots de passe (sshpass, etc) qui est public.
    * Un fichier déposé par erreur dans un path accessible.
    * Un Path Traversal qui permet de trouver des fichiers sensibles.
    * Le WP install laissé sur le serveur.
    * Des wp config avec example, on sert sur le domaine, mais on oublie que les fichiers `*.php` sont accessibles.

  La remédiation consiste à configurer correctement les serveurs, imaginer toutes les mauvaises configurations/pratiques et se "pentester".

  – Les mises à jour régulières de toutes vos libraries, frameworks, outil, etc.

- Le vol de données, sans accès shell ou droits suffisant pour chiffrer le système. Elles peuvent être récupérées par les mêmes moyens que les données publiées en publique par erreur (cf. chapitre précédent). Les données sont volées et revendues. Les données peuvent être utilisées pour du phishing, du social engineering, etc.

  – Impact sur la réputation :
    * Flow bank victime de vol de données, le régulateur ferme la banque moins d'un an plus tard.
    * Crédit Suisse, qui blanchit l'argent du traffic de drogue. 1 an après le Credit Suisse disparaît.
  – Impact financier direct lié au RGPB qui sanctionne les fuites de données personnelles.