Introduction à la Sécurité des systèmes d'informations	Semestre 4	Responsable : Sylvain LECOMTE

Objectifs de l'ECUE en termes de compétences et d'acquis d'apprentissage visés

A l'issue de cet ECUE, l'apprenant aura progressé sur les compétences suivantes du référentiel de la formation :

- BC1.3. Identifier les éléments de contexte d'un projet et les formaliser : besoins exprimés par un client, politique de l'entreprise, aspects réglementaires…
- BC1.8. Effectuer une recherche documentaire
- BC2.1. Comprendre un problème et son contexte
- BC2.2. Analyser le problème, formuler des hypothèses, le simplifier
- BC2.3. Choisir la démarche/ la méthodologie, Concevoir des modèles
- BC2.4. Développer, tester, comparer et valider des solutions

Plus précisément, il sera capable de :

- Connaître les principales réglementations en vigueur en matière de protection des données (RGPD, etc.)
- Analyser un document émis par des organisations contribuant à la sécurité des systèmes d'information (ANSSI, CERT-FR, etc.)
- Identifier les potentielles conséquences d'une faille ou d'une attaque de sécurité sur un système d'information
- Identifier les différentes sources possibles d'une attaque de sécurité connue
- Analyser des données pour identifier des anomalies au sein d'un système d'information
- Proposer des solutions de remédiation à des incidents de sécurité (règles de sécurité, élaboration de mots de passe, etc.)

Description de l'ECUE

Dans cet ECUE, l'élève apprendra à différencier les concepts de confidentialité, d'intégrité et de disponibilité des données, avant d'être sensibilisé aux différents types d'attaques (virus, malwares, phishing, etc.) et aux failles qui peuvent être exploitées. Les mécanismes fondamentaux de protection seront introduits (authentification, chiffrement, etc.) et les principales lois et réglementations en vigueur en matière de protection des données (RGPD, etc.) seront introduites.

De plus en plus de maison sont « intelligentes » et connectées au travers de solutions domotiques.

Ces solutions (type Jeedom ou Home Assistant), si elles sont mal sécurisées, peuvent exposer des données personnelles et sensibles.

Ce module se divisera en plusieurs blocs :

- Présentation de différentes solutions domitiques open source et des différents protocoles utilisés (RFC433, Wifi, Bluetooth, ZigBee). L'accent sera mis sur la sécurisation de ces solutions et protocoles
- Etude des contraintes posées par la RGPD : Quelles données stockées, délais de conservation (notamment dans le cas de domotisation d'entreprises)
- Installation de la solution domotique choisie sur Rasp PI 5 et mise ne place de plusieurs cartes, notamment : Météo, présence de périphériques (type téléphone), détection de mouvements. L'installation finale présentera à minima un design affichant la météo du lieu où l'on se trouve, et la liste des terminaux présents dans la salle.
- Mise en place des solutions de sécurisation et sureté pour le bon fonctionnement du service domotique :
    - Le Raspberry fonctionnant sous Linux, il est possible de mettre en place des scripts de sauvegarde et de surveillances (alertes de tentatives d'intrusion).
    - La sécurisation de la connexion réseau est également un point à identifier et travailler.
    - La tolérance aux fautes via des mécanismes de sauvegarde
    - Mise en place de solutions d'Audit pour détecter les intrusions
- Chaque groupe tentera d'exploiter une faille dans la domotisation du groupe voisin pour en extraire les données et ainsi obtenir un bonus lors de l'évaluation si cette intrusion n'a pas été détectée et traitée.

Prérequis

Références

Gildas Avoine, Pascal Junod, Philippe Oechslin et Sylvain Pasini, Sécurité informatique, Vuibert, 3ème édition, 2015.

https://www.economie.gouv.fr/entreprises/gerer-son-entreprise-au-quotidien/assurer-sa-cybersecurite-et-la-protection-de-ses/le