TD Méthodologie d'analyse des systèmes d'information

Projet Mesure de présence

Contexte projet

L'objectif est de mesurer le taux d'occupation des salles de réunions de l'entreprise afin de le comparer au taux de réservation de ces salles. Ce projet va permettre d'analyser le taux de fréquentation des salles de réunions sur les campus WIND et FIRE afin de pouvoir prendre des mesures sur la réservation des salles et potentiellement gagner de l'espace de travail si certaines salles de réunion sont sous-utilisées.

Le projet de mesure de présence concerne l'installation de capteurs dans les salles de réunion pour relever l'occupation de la salle à intervalles réguliers. Ces données seront consolidées et présentées sous forme de tableau de bord pour une lecture facilité. Un capteur IOT (Internet of Things) de chaleur relève toutes les 5 minutes l'information sur l'occupation de la salle, sauvegarde cette information sous forme de booléen dans sa mémoire interne puis envoie les données de présence toutes les heures via le réseau SIGFOX à un serveur Microsoft Azure administré par l'éditeur COGEE.

Fonctionnement

- Mesure de la présence dans une salle de réunion avec un capteur infra-rouge (chaleur)
- Remontée des informations d'occupation toutes les heures à un serveur central via le réseau SIGFOX
- Sauvegarde des données par l'éditeur COGEE et présentation d'un tableau de bord pour affichage de statistiques
- Possibilité de trier des statistiques précises et filtrées sur les capteurs

Choix techniques

Capteur IOT

Type	Boitier IP20 Capteur PIR (Pyroelectir InfrRed) infra-rouge basse consommation Module STM32 Flash 128kB Interrupteur Par aimant Plage de température -10°C / +55°C Type d'antenne Intégrée de type 1/4 d'onde
Réseau	SIGFOX, réseau M2M (machine-to-machine) Fréquence 868.2 MHz Puissance d'émission +14 dBm Sensibilité -142 dBm
Sécurité	Saut de fréquence Génération d'un HMAC à partir de la clé secrète AES-128 du capteur, lors de la transmission d'une trame

Portail Web COGEE

Hébergement	PaaS (Platform As A Service) fourni par Microsoft AZURE Datacenters européens (Dublin et Amsterdam)
Authentification	Utilisateurs : HTTPS, SSL v3 Admins : accès au back-office via VPN, accès au front-office admin via filtrage IP
Base de données	Les bases de données clients sont isolées logiquement dans des instances différentes. Politique de sauvegarde AZURE

Interconnexion avec le backend SIGFOX avec le service Azure IoT Hub pour la récolte des données des capteurs.

Les clés de chiffrement sont stockées dans le module Azure Key Vault.

Le portail internet est sécurisé par le module AZURE Security & Compliance.

Objectif du projet

Récolter des données sur l'occupation des salles de réunions de l'entreprise sans interconnexion avec le système d'information en place et avec peu de modification d'infrastructures.

Projet Audit sécurité automatisé

Contexte projet

Fortify Static Code Analyser (SCA) développé par HP est un logiciel permettant de tester la sécurité des applications par l'analyse statique de leur code (SAST). Les failles de sécurité logicielles sont identifiées, puis hiérarchisées par niveau de risque. De bonnes pratiques sont données pour corriger les lignes de code et remédier ainsi aux vulnérabilités.

Fortify est capable d'analyser les applications développées en interne, avec de nombreux langages dont COBOL et JAVA, ainsi que les applications mobiles pour smartphone.

Fonctionnement

Les grandes fonctionnalités de HP Fortify SCA sont les suivantes :

- Compréhension de 22 langages différents ;
- Détection plus de 669 vulnérabilités ;
- Support de nombreux IDE (Eclipse, Intellij, IBM RAD, Visual Studio, …) ;
- Possibilité de lancer jusqu'à 10 revues de code en parallèle ;
- Client web accessible depuis le réseau interne ;
- Client lourd, permettant la modification de code, installé sur le poste du responsable de la sécurité.

Fortify génère des artéfacts lors de la réalisation d'une revue de code qui contient toutes les données de l'analyse. Depuis cet artefact, un rapport d'audit est généré pour être compréhensible par les responsables applicatifs et les développeurs.

Choix techniques

Elle est composée de :

- Une base de données (MySQL);
- Deux serveurs virtualisés (Fortify 360 et Fortify SCA) ;
- Un poste, sur lequel est installé le client lourd.

L'application dispose donc d'un compte unique disposant de droit administrateur qui permet de réaliser la revue de code et transmet le rapport d'audit généré aux demandeurs. Le compte administrateur est utilisé par deux personnes.

L'application n'est pas connectée à Internet et est uniquement utilisée sur le réseau interne.

Objectif du projet

Il est prévu dans la stratégie de sécurité de l'entreprise qu'une revue de la sécurité des codes développés en interne soit réalisée pour chaque projet applicatif. La solution HP Fortify a été identifiée pour répondre à ce besoin pour les applications de l'entreprise.