CAHIER DE RECETTE

Sécurité dans une Mairie

Version 0.1

Objet du document :

Ce document regroupe l'ensemble des documents de recette du projet PPE de la Mairie.

Statut du document :

- ☒ **En cours d'élaboration**
- ☐ **En cours de validation**
- ☐ **Validé**

Sommaire :

Table des matières

I. Présentation de l'entreprise

1. L'Entreprise STESIO

La mairie de Saint Chély d'Apcher veut améliorée la sécurité de leur parc informatique a l aide d'un double facteur d'authentification dans ces locaux.

2. Cahier des Charges

a. Objectif

Nous voulons offrir un meilleur service de sécurité à la mairie à l'aide d'une authentification à double facteur dans leurs locaux.

b. Périmètre

Dans ce projet, nous nous concentrons sur la sécurité des systèmes informatiques du réseau de la mairie de Saint Chély d'Apcher. La Mairie dispose de différents systèmes d'environnement mais la plus part sont des systèmes Windows et Linux.

c. Description fonctionnelle

Fonction principale de la solution : Pouvoir sécuriser les systèmes informatiques de la mairie.

Sous-fonctions :
-> Sécurisation à distance
-> Avoir un double facteur d'authentification
-> Double authentification sur certaines applications

Existant :
-> Un Serveur Windows Server 2016

Contraintes :
-> Accès à distance sur différentes plateforme (multiplateforme)
-> Avoir différents niveaux d'accès aux applications
-> Permette le déploiement à Distance de l'Agent
-> Evolution à la Veille technologique

d. Enveloppe budgétaire

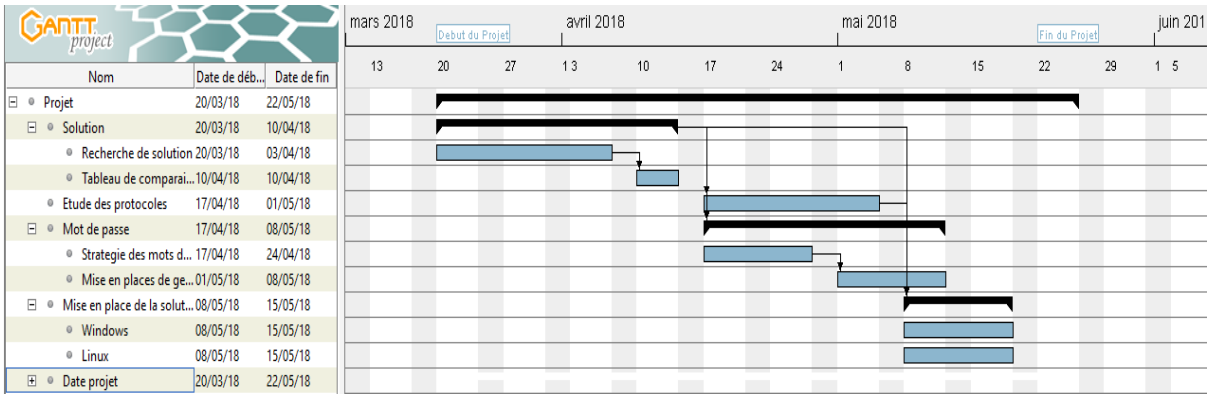
Dans notre problématique pour satisfaire les exigences de la mairie, notre solution logicielle devra être égale à environ 80 euros par membre de la mairie. Nous ne parlerons pas du matériel utilisé étant donné qu'elle sera hébergée sur le serveur de la mairie actuellement.

e. Délais

En analysant le cahier des charges nous avons recherché plusieurs solution ensuite nous avons réalisé un tableau comparatif des différentes solutions. Puis nous avons réaliser des document expliquant les bonnes pratique de mot de passe et nous avons réaliser les test puis la mise en places de la solution choisie sur Windows 10 et Debian 9.

.

Notre étude va être en plusieurs étapes au fil du temps, ci-dessous, un schéma prévisionnel (schéma GANTT[1]) :



3. Les Solutions Envisagées

a. Introduction

Notre problématique principale est : " Comment sécuriser les systèmes informatiques d'une Mairie à double facteur ? " entre les Ordinateurs de la Mairie

L'authentification sur un ordinateur se fait par différentes manières, classées ici selon 4 facteurs :

➔ Authentification par quelque chose que vous savez

IL s'agit d'une méthode d'authentification par mot de passe ou par code pin. Cette méthode a pour avantage la simplicité de sa mise en œuvre et dans le fait que la plupart des gens sont familiers avec cette méthode. C'est la plus méthode la plus utilisé. Elle a cependant de nombreux inconvénients :

_ Un mot de passe peut facilement être copié ou être voler à l'aide d'une attaque de type phishing, …

_ Beaucoup de personnes utilisent le même mot de passe pour plusieurs applications. Dans le cas d'un vol du mot de passe le voleur peut s'infiltré dans toute les applications avec se mot de passe.

[1] Représentation visuelle de l'état d'avancement des différentes activités (tâches) qui constituent un projet.

_ De nombreuse personne n'utilise des mots de passe facilement devinable par autrui. L'utilisation de mot de passe fort et donc conseil pour mieux sécuriser son mot de passe.

➔ Authentification par quelque chose que vous possédez

Cette manière de s'authentifier utilise en générale grâce une carte ou une clef. Le niveau de sécurité de cette méthode dépend des caractéristiques de l'outil concerne. Comme par exemple la certitude de non-reproductivité de l'outil, des essai qui mènent au blocage de la l'outil,…

➔ Authentification par quelque chose que vous êtes

Il s'agit de l'authentification pour des éléments de votre corps humain comme la rétine ou l'empreinte digital. Cela a pour avantage d'être unique et d'être plus rapide que le mot de passe mais a des inconvénients comme la nécessiter d'un matériel pas rependu et ca créer un problème d'authentification en cas d'accident comme une brulure qui « détruit » l'empreinte digital.

➔ Authentification par quelque chose que vous savez faire

Cette méthode permet de différentier des êtres humains des machines en leur montrant une image pour leur demander soit de recopier le teste afficher ou des sectionner des case ou il y a des éléments demandé,…Cette méthode permet seulement de se protéger des machines et non de personne mal intentionné.

Il faut donc mettre ne place plusieurs méthodes d'authentification pour augmenter la sécurité d'accès aux informations. Malheureusement le cout de la mise en œuvre, l'accessibilité à la technologie et l'évolution constante des solutions liées à la sécurité, la penser des utilisateur lambda qui voit sa plus comme une gène de nombreuse personnes n'utilise qu'un mot de passe peu robuste et perde leur information.

b. Tableau Comparatif des Solutions

(Tableau Comparatif des Solutions)

Nous avons choisie la nitrokey qui a comme avantages d être open source comparer a la yubico key qui la été précédemment mais qui se ferme petit a petit. Elle a aussi l avantage d'être facile d'utilisation, d'avoir une bonne bibliothèque en ligne et d'avoir un prix d'environ 40€ se qui respecte le cahier des charge.

II. Technique préalable

1. Un mot de passe fort

Au-delà des mots courants facilement détectables par des hackers, il faut créer des codes robustes :

- 12 caractères minimum, un mélange de lettres majuscules et minuscules, des caractères spéciaux en priorité avec des caractères de notre région géographique comme les é, ç pour la France ou plus largement de ce types la &"#_^ et de chiffres.

Plus les mots de passe sont longs et complexes, plus les machines auront du mal à les casser : on compte plusieurs années pour des codes incluant des majuscules, des minuscules, des chiffres et des caractères différents, contre quelques heures pour un mot de passe comme "iloveyou".

Par exemple, "J3su1st0nP3r3!!!" fera tourner les machines infructueusement pendant des lustres, contrairement à sa version simple.
Autre possibilité : utiliser un générateur de mot de passe, qui produira un code complexe à partir d'une phrase de votre choix.

Qu'est-ce qu'un mot de passe fort ?

– 1 – N'intégrez pas de mots liés à vous-même (enfant, date, anniversaire …) et préférez un minimum de 12 caractères avec minuscules, majuscules, chiffres et caractères spéciaux

– 2 – Multipliez les mots de passe (et non un seul) pour accéder à vos différents comptes et renforcer la sécurité

– 3 – Aménagez le degré de sensibilité et de confidentialité des données en fonction de l'accès du compte

– 4 – Changez les mots de passe par défaut des systèmes et applications

– 5 – Mettre à jour son mot de passe impérativement tous les 90 jours pour limiter les intrusions

– 6 – Ne les notez pas et ne les envoyez pas par mail

– 7 – Configurez votre navigateur afin de ne pas enregistrer automatiquement les mots de passe

2. Tutoriel d'installation

a. Installation de la Nitrokey pro sous Windows 10 sans Active Directory

1/ Connecter la Nitrokey a votre ordinateur comme une clef USB et confirmer tous les fenêtres .Les drivers doivent s'installer automatiquement.

2/ Télécharger et démarrer la « Nitrokey App ». Sa ne devrait pas ouvrir une fenêtre mais un icone devrait apparaitre dans la barre des taches, double cliquer sur le nouvelle icone

3/ Suivez les instructions pour change les code Pin qui sont par default pour le User PIN 123456 et celui de Admin PIN 1345678.
La nitrokey devrait être utilisable maintenant.

b. Installation de la Nitrokey pro sous GNU/Linux sans Active Directory

1/ Dans un terminal, taper cette commande pour installer le paquet libccid :

 # sudo apt-get update && sudo apt-get install libccid

2/ Puis comme pour Windows installer *et démarrer la « Nitrokey App ».*

3/ Suivez les instructions pour change les code Pin qui sont par default pour le User PIN 123456 et celui de Admin PIN 1345678

La nitrokey devrait être utilisable maintenant.

c. Difficulté rencontré

Lors de ce PPE notre groupe n a pas été souvent au complet car a cause de problème de sante d'un membre et la grève de la SNCF se qui nous a grandement ralentie notre travail.

Egalement nous n'avons pas reçu les matériels utile a notre projet la Nitrokey se qui nous a pas permis de tester le produit, les tutoriels trouver, etc.