ACCUEIL CONTRÔLE D'ACCÈS 2017

DGSI - Analyse du CCTP - RDV du 10.02.2017

- Présents pour l'EMSE : David Michalon et Dominique BERTHET
- Présents pour la DGSI : Laurent BASTY, XXX, XXX

Contenu du CCTP

- CCTP trop ambitieux pour les délais souhaités : trop de domaines sont pris en compte (MdE Gardanne, Anti-Intrusion, SSI, ...). L'aggrégation des alertes dans une interface unique peut se faire via des API entre les différents systèmes (bien demander des API ouvertes)
- Il faut plutôt décrire les normes de sécurité souhaitées sur les équipements plutôt que citer des modèles existants comme base de référence.
- Vu les délais contraints, il est déconseillé de tout intégrer de suite. L'anti-intrusion ne doit pas forcement être incluse dans ce CCTP. Idem pour le SSI. Les remontées d'alertes de chaque système pouvant maintenant facilement être agrégées via des API.
- Il faut éliminer toutes interruption du fonctionnement du contrôle d'accès liée à un dysfonctionnement annexe (réseau, électricité, ...).
- Il faut éventuellement se recentrer sur les priorités en terme de sécurité (L1 et L2)... (cette solution ne permet pas de supprimer la distribution de clés aux utilisateurs)
- L'intégration de la MdE de Gardanne (vu les délais) n'apporte que des contraintes techniques. Le système de badge préconisé (avec photo) offrira moins de souplesse aux élèves (prêt de clé, ...).
- L'intégration de plusieurs système est toujours une source de faille de sécurité.
- Bien prévoir une MCO sur 5 ans (Maintenance en Condition Opérationnelle)

Serrures Portes

- Il est conseillé de garder la possibilité d'ouvrir avec une clé en cas de panne du système. Un organigramme de gestion des clés devra être proposé. Les utilisateurs rendront leurs clés à la remise des nouveaux badges. On ne changera donc pas les barillets mais les serrures.
- Pour les barillets, demander la reprise de l'existant
- Prévoir des serrures à coupure en déclenchement
- Faire chiffrer L3 filaire et L3 radio
- La technologie radio offre très peu de sécurité (compromission possible par USB, écoute, ...) et peut être brouillée par le WIFI qui utilise les mêmes fréquences.
- Si le coût au déploiement d'un système filaire est beaucoup plus élevé, le coût de maintenance est moindre que pour un système radio.
- Garder un système double (clé/badge) va nous permettre un déploiement beaucoup plus souple.

Infrastructure

- L'intelligence doit être au niveau des RIO (Remote Input Output).

- En cas de panne de l'UTL, les lecteurs doivent pouvoir fonctionner.
- Pour la gestions des traces il faut demander des fonctionnalités de filtrage précises et pertinentes (par ID, ...) et surtout pas par lecteur.
- Pour le déploiement il faut impérativement installer les nouveaux concentrateurs en premier, avant de démonter l'existant.
- Il est conseillé d'installer la solution logicielle sur une infrastructure de virtualisation dédiée redondante (cf coûts induits).

Résilience

Le système dit être le plus résilient possible, il faudrait donc :

- évoquer le cas des coupures réseaux dans le CCTP (fonctionnement en mode dégradé, niveau d'autonomie souhaité, ...)
- prévoir une réplication et une synchronisation en temps réel des données entre Saint-Étienne et Gardanne afin de garantir un fonctionnement autonome pour chaque campus en cas de coupure réseau ou de panne du serveur principal. (VM réplicat à installer à Gardanne).

Niveau de sécurité

- Il faut impérativement décrire les niveaux de sécurité et définir les priorités.

Niveau 1

- La biométrie est la seule façon de réellement prouver que le porteur est le propriétaire du badge. Un code peut être transmis à un tiers.
- Un système ANTI PASS BACK est obligatoire pour assurer le comptage. Il devra être relier au SSI.
- Compter environ 10k€ par porte L1

Biométrie

- Les personnes devant avoir des accès de niveau 1 (ou 2 double authentification) devront fournir leur empreinte. L'enrôlement se fera à la remise du badge **sur des lecteurs dédiés** (à prévoir).
- Cette empreinte sera chiffrée (4096) et stockée directement sur le badge. Ainsi aucune base biométrique ne sera gérée par le système. Il y aura juste un échange (hashage) entre le badges et le lecteur.
- La demande d'autorisation à la CNIL devra être faite rapidement. Avec ce système de stockage sur le badge, elle sera simplifiée.
- Il faudra déterminer précisément les populations pouvant pénétrer en niveau 1 (Direction/DRH).

Badges

- Mise en place d'une carte comprenant uniquement une photo et un numéro afin de pouvoir identifier le porteur, Les badges anonymes auxquels nous pensions incitent moins les utilisateurs à régir en cas de perte.
- Le port visible du badge dans les locaux pour tous les permanents et visiteurs devra être la règle. Des signalisations devront être mise en place à l'entrée des bâtiments pour le rappeler.
- les étudiants devront toujours avoir un badge sur eux.
- la carte d'étudiant ne devra contenir aucun service ou tous les services si les accès sont plus strictement controlés.
- les badges devront être à minima du type Desfire EVx 4k afin de pouvoir héberger l'empreinte biométrique et l'ID0 du porteur chiffrée en 4096 bits (à voir pour la restauration).