La mission pour le développement de la vidéoprotection vous informe

Fiche : La sécurité des transmissions en Vidéoprotection

1. Introduction : Les nouvelles menaces

Les progrès techniques en matière de compression d'images (notamment le MPEG 4/ H264) ont permis de banaliser le transport des images de vidéo protection, qui ne sont plus maintenant exclusivement transmises sur de la fibre optique dédiée, mais peuvent utiliser largement des réseaux IP, dédiés ou non à la vidéo. Parfois, pour des raisons de cout, le réseau Internet est même utilisé (cf déports de certains CSU vers les services de Police/ Gendarmerie pour les réseaux de voie publique, cf liaisons de télémaintenance ou de renvois d'alarmes pour les réseaux dans les Etablissements recevant du public).

Ce nouveau contexte induit un certain nombre de nouvelles menaces :

- **Risque sur les réseaux de Vidéoprotection eux mêmes (Risque propre)** :
  Les images de voie publique peuvent être interceptées par l'écoute des liaisons entre les caméras et les CSU (par exemple si des réseaux Wifi sont utilisés pour le rapatriement des images) ou par des attaques malveillantes (hacking sur le site CSU dans le cas de l'utilisation d'Internet pour les déports vers le CORG) ;
  Des attaques malveillantes peuvent également paralyser les réseaux de Vidéoprotection (déni de service)
- **Risque induit sur d'autres systèmes (Risque induit) :** La cohabitation sur le même réseau interne de la commune ou de l'entreprise des images Vidéo et des applications informatiques traditionnelles fait peser un risque nouveau sur ces applications informatiques.

2. Analyse

Pour avancer sur les deux risques mentionnés, on commencera par énoncer quelques précautions qui sont valables quelle que soit l'architecture du réseau urbain de vidéo protection, puis on approfondira les risques dans différentes configurations de réseaux.

2. 1. Considérations générales

Le schéma de réseau est en général le suivant :

Pour les réseaux de voie publique
Caméra → liaison Télécom 1 → CSU – Serveur ←→ Liaison Telecom 2 → CORG/ DDSP

Pour les réseaux privés relevant le la loi de 95
Caméra → liaison Télécom 1 → Centre d'enregistrement– Serveur ←→ Liaison Telecom 2 → centre de télémaintenance ou de veille sous traitée.

La seconde partie du schéma (déport Télécom 2) n'est pas systématique.

Lorsque les liaisons Telecom sont des liaisons permanentes dédiées à la Vidéo (liaisons fibre optique, xDSL louées à un opérateur ou Faisceaux hertziens mis en place par le SZSIC) , le risque sécuritaire est a priori négligeable.

On notera que la cohabitation sur un même support physique (notamment fibre optique) de flux différents n'est pas forcément une mauvaise chose. Il faut très clairement distinguer :

- l'utilisation d'une même fibre optique (et a fortiori de plusieurs fibres optiques différentes) pour transmettre des flux qui disposent chacun d'un « tuyau » propre et ne peuvent pas interagir entre eux : conduits multiplexés disposant chacun de x Mb/s, VLAN, VPN chiffrés. Dans ces cas, l'utilisation d'un support fibre optique pour transmettre à la fois les images du réseau de Vidéoprotection et les flux informatiques propres de l'entreprise ou de la mairie ne pose pas de problème de sécurité et peut même être conseillé dans une optique de rationalisation financière.
- Le mélange sur un support physique **et** dans un même circuit télécom de paquets IP Vidéo et de paquets IP d'autres réseaux informatiques, qui ne seraient séparés que par les routeurs, en fonction de l'adresse IP de destination. Dans ce cas, il y a un risque fort d'intrusion de ces autres réseaux informatiques (surtout s'ils sont ouverts sur Internet) sur le réseau Vidéo, entrainant de possibles écoutes ou des attaques paralysant le réseau. A l'inverse, les réseaux de vidéoprotection ayant des terminaisons dans la rue ouvertes à tous, peuvent être un point d'entrée pour les hackers souhaitant pénétrer le réseau informatique.

Recommandation 1 (source ANSSI : Agence nationale de la sécurité des systèmes d'information, rattachée au Premier ministre):
« Un fort cloisonnement logique doit être établi entre les capteurs au sein du réseau support*. En particulier, dans la mesure où les différents capteurs n'ont pas de raison légitime de communiquer entre eux directement, il est recommandé de configurer les équipement de routage et commutateurs d'accès de telle sorte que chaque caméra ne puisse établir de communication qu'avec les serveurs d'administration et de collecte des flux, et en aucun cas avec les autres caméras. Un tel cloisonnement peut par exemple être obtenu par la mise en œuvre sur les commutateurs d'accès d'un mécanisme d'isolation de type PVLAN (RFC5517), empêchant les dialogues directs entre caméras, voire de VLAN dédiés à chaque caméra dans un dispositif de taille limitée. »*

Par ailleurs, les liaisons non permanentes, que ce soit la liaison entre les caméras et le centre d'enregistrement ou le déport éventuel vers les services de Police/ Gendarmerie, posent un problème lié à l'intrusion. En général l'accès n'est pas protégé par un moyen fort (type certificat électronique) mais par un simple login/ mot de passe qui n'est pas infaillible. Le risque est qu'un hacker pénètre dans le serveur du CSU et rapatrie les images qui l'intéressent, ou introduise un virus qui plante le système. Une parade face à ce genre de risque est d'examiner régulièrement les « logs » du système qui permettent de garder la trace de tentatives d'intrusions, ou de connexions à des heures anormales. L'ANSSI recommande également de désactiver les interfaces locales d'administration qui ne sont pas rigoureusement indispensables, et de remplacer les mots de passe par défaut par des mots de passe spécifiques et robustes.

Les déports des CSU vers les CORG (Gendarmerie) utilisent parfois Internet (plutôt que des liaisons spécialisées dédiées) pour des raisons de cout, mais cela induit une fragilité.
L'ANSSI précise :

« Le dispositif de vidéoprotection ne doit pas être directement accessible depuis Internet*. En particulier, les éventuelles interfaces d'administration des équipements ne doivent pas être accessibles depuis Internet. »*

Le cas des accès aux images depuis des mobiles (véhicules de police sur le terrain) par GSM est voisin mais présente moins de risque dans la mesure où l'authentification des mobiles GSM entre eux peut être vérifiée lors de la connexion (encore faut il que cela ait été spécifié par le maitre d'ouvrage).

Recommandation 2 : Lorsqu'il existe des liaisons non permanentes du Centre d'enregistrement avec les caméras ou avec un déport, il est important de mettre en place des dispositifs de protection anti-intrusion et de surveiller régulièrement les traces de connexions et les journaux d'incidents.

cf ANSSI : *« **Les flux réseau émis et reçus par les équipements doivent autant que possible être chiffrés et authentifiés, avec un protocole cryptographique interdisant le rejeu de flux antérieurs**. »*

2.2. Cas des réseaux de voie publique

L'ANSSI recommande de privilégier une connectivité filaire pour les équipements de vidéoprotection. , la radio (Wifi, Wimax, les FH relevant de la catégorie précédente) introduisant plusieurs types de risques :

- Le risque de compromission (écoute des images Vidéo) est à prendre en compte, et il faut veiller à chiffrer correctement le réseau radio : le réseau doit être chiffré s'il s'agit de Wimax et utiliser un chiffrement WPA2 (et non un chiffrement WEP trop faible) s'il s'agit de Wifi.
- Le risque de brouillage : il peut être non intentionnel, comme c'est le cas dans les grandes villes où les fréquences sont relativement saturées, ou malveillant. Dans le cas d'un brouillage malveillant, les services techniques de l'Etat (ANFR) sont en général à même de détecter les brouilleurs et de les neutraliser, mais cela peut prendre plusieurs semaines.
- Dans le cas particulier du Wifi, le risque d'intrusion existe car la sécurité d'accès, basée sur la diffusion ou non du SSID et le filtrage par adresse MAC, est relativement faible.

Recommandation 3 : L'utilisation de liaisons Wifi présente plusieurs risques liés à l'intrusion et à la confidentialité sur lesquels il faut être vigilant lors de la phase de spécifications. Le chiffrement doit être au minimum du WPA2.

2.3. Architecture novatrice avec enregistrement dans la caméra

Compte tenu des progrès sur le stockage et la transmission par les réseaux publics mobiles (3G et 4G), une nouvelle architecture commence à voir le jour :

Caméra avec enregistrement local → liaison 3G ou 4G activée uniquement si le CSU souhaite visionner les images (ou par la caméra intelligente détectant une anomalie)

- La problématique du risque est assez différente, le risque induit n'existant en principe plus. Le risque d'écoute des images sur la liaison est très faible puisque les liaisons GSM ou 4G sont chiffrées par les opérateurs et leur accès est protégé.
Le risque d'une copie pirate des images au niveau de la caméra (sur son disque dur) existe mais reste marginal.

Le risque principal, beaucoup plus réel, est celui de perdre les images par destruction de la caméra et de son stockage local (notamment après un délit, pour effacer les traces de preuves). Il convient donc de mettre en place un test automatique régulier des liaisons avec les caméras et des alarmes si ces tests sont négatifs.

Recommandation 4 : Pour les architectures avec enregistrement local, prévoir une sécurisation de l'enregistreur de la caméra, des alarmes en cas d'effraction et des tests périodiques du bon fonctionnement des liaisons. Si l'abonnement avec l'opérateur Télécom le permet, prévoir le rapatriement des images au CSU en heures creuses, afin d'avoir une sauvegarde supplémentaire des images.

2.4. Aspects organisationnels

L'ANSSI rappelle qu'une bonne sécurité repose sur quelques principes d'application stricte des règles classiques d'hygiène informatique :

- la journalisation des événements et l'exploitation des journaux, déjà citée
- un contrôle d'accès au centre de supervision, et l'authentification des exploitants du CSU
- éventuellement un audit de sécurité du centre de supervision
- et, en cas de sous traitance, la localisation des données (cf guide ANSSI www.ssi.gouv.fr/externalisation)