Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 14 février 2013

N° 524/ANSSI/SDE

RECOMMANDATIONS DE SECURITE
POUR LA MISE EN ŒUVRE DE DISPOSITIFS DE VIDEOPROTECTION

Les dispositifs de vidéoprotection constituent une mesure classique de sécurité physique, mise en œuvre au sein d'un grand nombre de sites sensibles. Généralement constitués d'un ensemble de caméras qui transmettent, à travers un réseau support, des images à un centre de supervision où elles sont analysées ou stockées, ces dispositifs ont longtemps reposé sur des protocoles spécifiques et des transmissions essentiellement analogiques. Cependant, les évolutions récentes ont amené l'offre en matière de vidéoprotection à faire largement appel à des protocoles standards, en particulier des communications de type IP, et parallèlement à proposer des fonctionnalités, notamment de télé-administration, de plus en plus évoluées.

De ce fait, les dispositifs de vidéoprotection s'apparentent désormais, dans une large mesure, à des systèmes d'information classiques, aussi bien en termes de protocoles (diffusion de flux en vidéo sur IP, administration basée sur HTTP), que de systèmes d'exploitation, ou encore de mécanismes d'authentification et de contrôle d'accès. A ce titre, ces dispositifs sont potentiellement exposés aux mêmes vulnérabilités que les autres systèmes d'information, vulnérabilités dont l'exploitation pourrait porter atteinte à la fonction de sécurité que ces dispositifs assurent. Ce risque est d'autant plus significatif que l'utilisation de protocoles standard peut inciter les entités qui déploient ces dispositifs à mutualiser le réseau support correspondant avec le reste de leur système d'information. Une telle mutualisation est susceptible d'augmenter la surface d'attaque des dispositifs de vidéoprotection eux-mêmes, et d'exposer par ailleurs le reste du système d'information à des attaques issues des équipements de vidéoprotection.

Le présent document décrit un ensemble de mesures et de principes d'architecture, dont la mise en œuvre vise à contrer ces vulnérabilités potentielles, ou du moins à en limiter l'impact. Les recommandations qu'il formule portent sur l'ensemble des composants d'un dispositif de vidéoprotection : déploiement physique des capteurs, architecture du réseau support, configuration des équipements et du centre de supervision. Il ne traite en revanche en aucun cas de l'efficacité du dispositif de vidéoprotection, et ne recommande pas de produits en particulier. Enfin, l'application de ces recommandations techniques ne dispense pas du respect des réglementations en vigueur, et ne doit pas se substituer à une analyse de risques détaillée propre à chaque déploiement.

1 Analyse succincte des menaces

Les risques liés à l'exploitation d'éventuelles vulnérabilités dans les dispositifs de vidéoprotection relèvent pour l'essentiel des trois catégories suivantes :

- **Atteinte à la confidentialité des données de vidéoprotection** : les flux vidéo et éventuellement audio captés par les caméras peuvent être interceptés, par écoute passive sur le réseau support ou interception de rayonnements parasites compromettants. La sensibilité des flux qui sont susceptibles d'être interceptés dépend naturellement du positionnement des caméras à l'intérieur ou à l'extérieur des locaux qu'elles contribuent à protéger.
- **Atteinte à la disponibilité de la vidéoprotection** : l'exploitation de vulnérabilités logiques dans les différents équipements actifs du réseau de vidéoprotection (caméras, équipements de routage, serveurs de collecte) peut permettre à un attaquant de désactiver tout ou partie du dispositif. Une attaque de ce type peut par ailleurs être dissimulée par l'injection de flux vidéo illégitimes créés par l'attaquant ou le rejeu de flux légitimes antérieurs.
- **Intrusion dans le reste du système d'information** : lorsque le réseau support des équipements de vidéoprotection est mutualisé avec le système d'information de l'entité utilisatrice (réseau bureautique, serveurs internes ou externes), la prise de contrôle d'un équipement de vidéoprotection par un attaquant peut permettre à ce dernier de mener dans un second temps une intrusion plus générale au sein du système d'information. Ce risque est d'autant plus significatif que, de par la nature même de leur fonction, les caméras de vidéoprotection sont souvent plus exposées à des attaques physiques que les autres équipements du système d'information (caméras déployées à l'extérieur des bâtiments, ou dans des zones peu fréquentées).

2 Architecture du réseau support

Afin de contrer les risques d'intrusion au sein du système d'information, et de limiter les possibilités d'atteinte généralisée à l'ensemble du dispositif de vidéoprotection, il est primordial d'isoler le réseau support associé, et de mettre en œuvre un cloisonnement adapté au sein de ce dernier. Ce principe d'isolation et de cloisonnement se décline selon plusieurs modalités pratiques :

- **Une connectivité filaire est à privilégier pour les équipements de vidéoprotection**. En effet, si certaines caméras récentes supportent différents modes de communication sans-fil (wifi ou téléphonie 3G essentiellement), la mise en œuvre de ces fonctionnalités augmente très significativement l'exposition des équipements à des attaques logiques.
- **Le réseau support du dispositif de vidéoprotection ne doit en aucun cas être mutualisé avec d'autres composantes du système d'information de l'entité utilisatrice**. Une isolation physique complète (câblage et équipements de routage dédiés) doit être privilégiée par rapport à une simple isolation logique (VLAN par exemple), qui n'offre pas un niveau de robustesse comparable. Au-delà de l'isolation par rapport au système d'information généraliste, il est également recommandé de ne pas mutualiser le réseau de vidéoprotection et celui associé au contrôle d'accès physique (lecteurs de badges, serrures électroniques, etc.). En effet, au-delà de la différence de finalités et des rôles complémentaires de ces deux types de dispositifs, les équipements qui y sont respectivement raccordés présentent souvent des niveaux d'exposition différents à de potentielles atteintes physiques. C'est le cas par exemple lorsque les caméras de vidéoprotection sont positionnées exclusivement à l'intérieur du périmètre à accès contrôlé, tandis que certains lecteurs de badges sont par construction à l'extérieur de celui-ci.

- **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.
- **Il est recommandé, lorsque cela est possible, d'isoler entre eux les réseaux de vidéoprotection interne et externe**, lorsque des caméras sont positionnées aussi bien à l'intérieur des bâtiments protégés que dans leur périmètre extérieur. En effet, les caméras extérieures sont naturellement plus exposées, et une action malveillante sur celles-ci ne doit pas permettre de porter atteinte à la confidentialité des flux intérieurs. Lorsque cela est possible, l'emploi d'équipements différents au sein des deux dispositifs de vidéoprotection apporte une sécurité supplémentaire, en limitant les risques de voir une même vulnérabilité exploitée sur les deux réseaux.
- **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.
- **Il est souhaitable de contrôler les accès directs au réseau support**. La prévention des accès illégitimes doit s'appuyer sur un contrôle des points d'accès physiques, en évitant de laisser apparents et accessibles des ports d'accès au réseau. Lorsque les équipements le supportent, il est également souhaitable d'imposer une authentification cryptographique des accès au réseau, par exemple par la mise en œuvre du protocole 802.1X pour le contrôle d'accès aux ports réseau.

3 Choix et configuration des équipements de vidéoprotection

Les considérations de sécurité doivent également intervenir dans le choix des capteurs de vidéoprotection, ainsi que dans la configuration de ces équipements. Il est rappelé ici que les modèles récents de caméras IP s'apparentent très largement, en dépit d'un facteur de forme différent, à des ordinateurs classiques, aussi bien au niveau du matériel lui-même (micro-processeurs usuels, connectivité standard de type USB ou port série, etc.) que des composants logiciels qu'il exécute (système d'exploitation de type Linux, serveur web ou console d'accès distant, etc.). A ce titre, les recommandations de sécurité portant sur ces équipements rejoignent largement celles qui sont plus généralement conseillées pour des matériels informatiques de type PC. On retiendra plus particulièrement les mesures suivantes :

- **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**. Cette mesure doit porter aussi bien sur les flux de remontée vidéo que sur les connexions d'administration distante des caméras. De nombreux modèles de caméras IP supportent des options de protection cryptographique des flux réseaux, mais il est en général nécessaire de les activer spécifiquement dans la configuration des équipements. Il est par ailleurs souhaitable de privilégier dans ce cadre des protocoles cryptographiques génériques et éprouvés comme TLS ou IPsec, plutôt que des protocoles propriétaires spécifiques à un type d'équipement, dont il est difficile de vérifier la robustesse *a priori*. Le lecteur est par

ailleurs invité à consulter les recommandations du Référentiel général de sécurité[1] pour le choix et le dimensionnement des mécanismes cryptographiques.

- **On veillera à désactiver, si cela est possible, les interfaces locales d'administration des équipements déployés**, lorsque de telles interfaces existent. Il est notamment courant que les caméras IP proposent une administration par port série, avec ou sans authentification. Si de telles interfaces trouvent toute leur utilité dans la configuration initiale des équipements, il est en revanche souhaitable, au regard des possibilités d'accès physique que pourrait avoir un attaquant, de les désactiver logiquement lors du déploiement effectif des capteurs.
- **Les mots de passe par défaut des caméras doivent être remplacés par des mots de passe spécifiques, robustes[2], et dans la mesure du possible diversifiés**. Le ou les mots de passe contrôlant l'accès aux fonctions d'administration sont généralement pré-positionnés à des valeurs par défaut lors de la fabrication des équipements. Il est primordial de remplacer ces valeurs par défaut par des mots de passe robustes avant le déploiement des équipements. Il est également recommandé de ne pas utiliser les mêmes mots de passe sur l'ensemble des capteurs du dispositif de vidéoprotection. De même, lorsque l'authentification repose sur des certificats, il est recommandé de remplacer ceux installés par défaut sur les équipements par des certificats produits par une infrastructure de gestion de clé maîtrisée par l'organisme.
- **De manière générale, il est recommandé de désactiver les fonctions et interfaces d'administration qui ne sont pas réellement utilisées dans le cadre du déploiement considéré**. Il est en effet courant pour les équipements récents de proposer un ensemble de fonctionnalités avancées (par exemple réorientation de la caméra) dont la mise en œuvre n'est pas forcément nécessaire dans un cadre donné. Dans ce cas, la désactivation de ces fonctionnalités, lorsqu'elle est possible, réduira d'autant la surface d'attaque des équipements.

Il est souhaitable de prendre en compte ces recommandations dès la conception du dispositif de vidéoprotection. La possibilité de réaliser les différentes opérations de configuration évoquées ci-dessus, en particulier la définition des mécanismes cryptographiques à mettre en œuvre, doit constituer un critère pour la sélection des modèles d'équipements à déployer. Au-delà de ces considérations, il convient de souligner qu'il n'est en général pas possible de juger *a priori* du niveau de robustesse des mécanismes de sécurité mis en œuvre au sein d'un équipement. **Par conséquent, il est recommandé de faire mener une analyse indépendante de la sécurité des équipements sélectionnés, par exemple en les soumettant à une procédure de Certification de Sécurité de Premier Niveau (CSPN)[3].**

4 Sécurité du centre de supervision

Le centre de supervision du dispositif de vidéoprotection, typiquement localisé au sein du poste de sécurité de l'entité concernée, est en général constitué d'un ensemble de serveurs et de postes de travail qui réalisent la centralisation et le stockage des flux de vidéoprotection, et permettent leur analyse et l'administration du parc de capteurs. Élément central du dispositif, ce centre de supervision dispose de privilèges élevés et est le seul (sous réserve de respect des recommandations d'architecture énoncées plus haut) à pouvoir communiquer avec l'ensemble des capteurs. Il nécessite par conséquent une attention particulière en termes de sécurité.

En plus des mesures classiques de sécurité physique, en particulier la localisation des équipements dans des locaux – poste de sécurité ou salle machines – à accès restreint, le centre de supervision doit ainsi faire l'objet d'une isolation par rapport au reste du système d'information (au même titre que le

[1] www.ssi.gouv.fr/rgs.
[2] www.ssi.gouv.fr/mots-de-passe.
[3] www.ssi.gouv.fr/cspn.

reste du réseau support, voir supra) et **d'une application stricte des règles classiques d'hygiène informatique**[4]. On veillera ainsi plus particulièrement :

- à l'authentification nominative et sur la base de mécanismes robustes des utilisateurs ;
- à l'utilisation d'un réseau dédié à l'administration des équipements du centre de supervision, si ceux-ci sont administrés par le réseau ;
- à la mise en œuvre d'une politique adaptée de suivi des versions et de mise à jour des composants logiciels ;
- au strict contrôle des branchements de périphériques amovibles ;
- et enfin à la journalisation des opérations, notamment celles portant sur l'administration du parc de caméras et des serveurs de collecte des flux, et au contrôle régulier de ces journaux.

Il est par ailleurs souhaitable de faire vérifier le niveau de sécurité du centre de supervision par un audit indépendant.

5 Problématiques de signaux compromettants

Outre les menaces liées aux possibilités d'attaques physiques ou logiques, les équipements de vidéoprotection, comme tous les équipements électroniques, sont susceptibles de produire des rayonnements électromagnétiques parasites qui peuvent véhiculer des informations sensibles issues des traitements en cours d'exécution sur l'équipement.

En fonction de la sensibilité des locaux surveillés et de leur configuration géographique, ces problématiques de signaux compromettants devront potentiellement être prises en compte lors du déploiement de caméras intérieures, selon les modalités définies par la réglementation en vigueur[5].

6 Aspects contractuels en cas de sous-traitance

Enfin, au-delà des mesures techniques décrites dans les sections précédentes, il convient de signaler les risques inhérents au recours éventuel à un prestataire externe pour déployer et administrer un parc de caméras de vidéoprotection. Cette pratique relativement courante est notamment susceptible, selon la nature du prestataire et du contrat qui le lie à son client, d'entraîner la duplication de l'ensemble des flux des caméras en dehors du système d'information du client, voire en dehors du territoire national. La couverture de ces risques, lorsque le recours à une externalisation du service s'avère nécessaire, passe par le respect de bonnes pratiques organisationnelles et contractuelles, selon la démarche décrite dans le guide « Maîtriser les risques de l'infogérance – externalisation des systèmes d'information[6] » publié par l'ANSSI. Dans le contexte particulier d'un dispositif de vidéoprotection dont la centralisation des flux serait réalisée par un prestataire tiers, il convient notamment de porter une attention particulière :

- à la localisation des données collectées par le prestataire, aux mesures de sécurité liées à leur stockage, et à l'absence de duplication et de communication de ces données à des tiers (y compris dans le cadre des procédures de maintenance des équipements de collecte) ;
- à l'éventuelle mutualisation des services de collecte ou d'administration entre les différents clients ; il est en particulier souhaitable d'éviter toute mutualisation des équipements mis en place par le prestataire entre ses clients institutionnels et les autres clients.

[4] www.ssi.gouv.fr/hygiene-informatique.
[5] www.ssi.gouv.fr/fr/reglementation-ssi/signaux-parasites-compromettants-spc.
[6] www.ssi.gouv.fr/externalisation.