LIVRE BLANC

Des données vidéo comme preuves légales

Sécuriser l'intégrité des données vidéo avec AXIS Camera Station

Juillet 2021

AXIS COMMUNICATIONS

Table des matières

1 Avant-propos

Des données vidéo de haute qualité, crédibles et non falsifiées peuvent être utilisées comme preuves légales. Meilleures pratiques de traitement de données vidéo pour produire des preuves légales à l'aide d'AXIS Camera Station :

- Concevoir, configurer et valider correctement le système pour fournir l'image, l'enregistrement et la sécurité que vous souhaitez.
- Effectuer une maintenance régulière
- Traiter toute preuve selon des procédures définies

2 Introduction

La vidéo de surveillance est pratiquement conçue pour servir de preuve au tribunal. Un événement filmé ne peut être réfuté en soi, n'est-ce pas ? Un juge acceptera donc probablement des données vidéo de haute qualité, crédibles et non falsifiées.

Mais dans certains cas, la valeur de preuve de la vidéo est réduite involontairement. Par exemple, des séquences de surveillance comportant des interruptions, et où des personnes ou des véhicules disparaissent soudainement ou « sautent » dans l'image, peuvent ne pas être considérées comme suffisamment fiables pour être utilisées comme preuves légales. La vidéo peut également être remise en question si ses métadonnées, telles que l'horodatage ou l'adresse MAC de la caméra, sont incohérentes. Tout soupçon portant à croire que la vidéo a pu être modifiée, supprimée ou trafiquée peut réduire la crédibilité de son propriétaire.

Le présent livre blanc conseille sur la façon d'utiliser la vidéo comme preuve légale. Il définit plus précisément le rôle du logiciel de gestion vidéo AXIS Camera Station dans la chaîne de production de preuves légales, ainsi que celui du propriétaire de la vidéo.

Figure 1. La vidéosurveillance d'endroits stratégiques peut produire des preuves valables légalement, si elle est bien configurée et gérée

3 Meilleures pratiques pour que des données vidéo servent de preuves légales

Les entreprises et les organisations qui utilisent la vidéosurveillance doivent mettre en place des processus et des procédures qui déterminent comment traiter et stocker les données vidéo. Pour être parfaitement préparé lorsque l'une de vos caméras filme un incident, vous devez vous assurer que la vidéo est protégée contre l'écrasement, la falsification ou le vol. Il doit également être possible d'exporter les séquences en toute sécurité vers un stockage sécurisé et de les remettre aux autorités légales.

Mais la production de preuves vidéo de haute qualité est un processus qui commence par une conception ciblée de votre système vidéo. Il est également de la plus haute importance que vous teniez votre système à jour et que vous gardiez trace de toute irrégularité. Ce chapitre présente les étapes de ce processus et la manière dont elles peuvent être suivies à l'aide d'AXIS Camera Station et de sa boite à outils AXIS Camera Station Integrator Suite.

Si vous réalisez des vidéos de surveillance en respectant ces principes de conception et de maintenance du système, ainsi que de traitement des incidents, elles seront conformes aux exigences actuelles en matière de cybersécurité et, très probablement, elles auront valeur de preuves, le cas échéant.

Figure 2. Le logiciel AXIS Camera Station software facilite à la fois la mise en place, l'exploitation quotidienne et la gestion stratégique d'un système de vidéosurveillance.

3.1 Concevez votre système correctement

Un système de vidéosurveillance doit être conçu avec soin. Vous devez choisir l'équipement en fonction de vos besoins et le configurer pour qu'il fournisse simultanément l'image, le type d'enregistrement et la sécurité que vous voulez. AXIS Site Designer fournit une aide importante pour cela.

3.1.1 Pour obtenir l'image que vous souhaitez

La qualité de l'image dépend de la caméra et de son positionnement. La résolution de l'image, ou plus précisément la densité de pixels sur la scène des événements, peut être calculée si vous connaissez le modèle de la caméra, l'objectif, ainsi que la distance et l'angle de la caméra par rapport à la scène. Pour obtenir une densité de pixels adéquate sur le visage d'une personne dans la scène, vous devrez peut-être déployer davantage de caméras ou utiliser des caméras à plus haute résolution. Vous devez étudier le champ de vision, les besoins d'éclairage et d'autres paramètres pour des caméras données sur votre site spécifique. Tout cela peut être réalisé de façon simple dans AXIS Site Designer.

3.1.2 Pour obtenir les enregistrements que vous souhaitez

Pour enregistrer vos vidéos, vous devez utiliser du matériel performant, validé et redondant. Pour accroître la fiabilité du système, AXIS Camera Station prend en charge l'enregistrement de secours en stockant temporairement les images sur la carte SD de la caméra réseau. Si vous utilisez l'analyse de détection de

mouvement vidéo, veillez à ce que les enregistrements soient suffisamment longs pour permettre de vérifier l'incident dans son intégralité. Un enregistrement de détection de mouvement qui n'est pas calibré de façon optimale peut présenter des écarts de temps et des séquences disjointes. L'enregistrement continu peut s'avérer le meilleur choix dans de nombreux cas, mais il nécessite beaucoup plus de capacité de stockage ainsi qu'une disponibilité permanente de bande passante suffisante.

3.1.3 Pour obtenir la sécurité que vous souhaitez

Vous devez doter le système de la sécurité physique nécessaire pour empêcher tout accès non autorisé. Tous les éléments matériels, notamment les caméras, les équipements et les câbles réseau, les serveurs, le stockage des données, les dispositifs d'alimentation et les câbles doivent être protégés. Les mesures de sécurité peuvent consister à restreindre l'accès à la salle des serveurs, à verrouiller l'armoire du serveur, à placer le serveur en rack dans l'armoire, à désactiver les ports physiques du serveur et à ne pas exposer les câbles réseau.

Vous devez également vous efforcer de doter le système de la cybersécurité nécessaire pour minimiser les risques de violation de données, de tentatives de falsification des données et d'attaques malveillantes. Ce qu'on appelle durcissement peut être assuré en partie par des outils logiciels et la technologie, et assure que le système respecte les normes de sécurité actuelles. Mais le durcissement requiert aussi de la part du propriétaire du système d'adopter un état d'esprit de cybersécurité et de travailler activement à sa diffusion dans l'entreprise. Par exemple, tous les utilisateurs du système doivent être conscients de l'importance d'utiliser des mots de passe forts et difficiles à deviner, et veiller à ne pas les révéler. Les accès des utilisateurs doivent être limités, ainsi que les permissions utilisateurs, selon la méthode du moindre privilège par exemple. Il incombe au propriétaire du système d'éduquer le personnel sur les meilleures pratiques et de s'assurer qu'elles sont bien mises en place. Un intégrateur autorisé peut durcir le système mais certaines mesures de cybersécurité ne peuvent être effectives que si les personnes qui l'utilisent coopèrent activement.

Une manière importante d'arriver à augmenter la cybersécurité globale est de protéger la vidéo par le cryptage des données pendant leur transfert. Pour transférer les données entre le client et le serveur, AXIS Camera Station utilise le cryptage AES pour la vidéo, l'audio et les métadonnées, et le cryptage TLS 1.2 pour les autres données. AXIS Camera Station peut aussi être configurée de manière à crypter également les flux de données entre les caméras et le serveur, via HTTPS. Parmi les autres meilleures pratiques de protection logicielle, on peut citer la désactivation de tous les services inutilisés, l'utilisation du filtrage des adresses IP/MAC, la prise en compte de la norme IEEE 802.1X, la prise en compte de la surveillance SNMP, le réglage de la date et de l'heure correctes avec un serveur NTP fiable (pour garantir l'exactitude des horodatages dans vos données vidéo).Il est également recommandé de n'utiliser que l'accès distant sécurisé d'Axis pour les connexions à distance (au lieu du transfert de port ou du bureau à distance). Pour approfondir les mesures et les recommandations, consultez le guide de durcissement de la cybersécurité d'Axis.

3.1.4 Configurez et validez votre système

Il est possible de configurer les éléments clés du système dès sa conception à l'aide d'AXIS Site Designer, avec des noms de caméras, des résolutions et des temps de rétention spécifiques. Après conception et installation de votre système, les configurations définies dans AXIS Site Designer peuvent être exportées dans AXIS Camera Station, à partir de laquelle vous pouvez continuer à affiner et régler les paramètres si vous le souhaitez.

Une fois l'installation terminée, vous pouvez valider votre système à l'aide d'AXIS Installation Verifier, qui fait partie de la boite à outils AXIS Camera Station Integrator Suite. Le vérificateur d'installation teste le système en mode normal ainsi qu'en mode nuit, afin de vérifier que la largeur de bande est suffisante en cas de faible luminosité, lorsque les niveaux de bruit sont plus élevés et qu'une plus grande largeur de bande est requise. AXIS Installation Verifier effectue alors un test de résistance en augmentant régulièrement

le volume de données générées dans le système jusqu'à trouver le premier goulot d'étranglement. Cela révélera la capacité de réserve du système et indiquera s'il faut l'améliorer.

3.2 Effectuer une maintenance régulière

Lorsque votre système est opérationnel, vous devez continuer à le surveiller et à le mettre à jour.

Assurez-vous que le matériel ainsi que les logiciels fonctionnent comme prévu. Contrôlez la qualité de la vidéo, nettoyez les objectifs des caméras selon un calendrier précis, vérifiez qu'il n'y a pas d'altération physique et que le champ de vision et la direction des caméras restent tels qu'ils le devraient. Examinez régulièrement les journaux système, car ils fournissent des informations sur les connexions, les branchements et les problèmes rencontrés par les dispositifs. AXIS Camera Station fournit des notifications lorsque des irrégularités sont détectées et les enregistre dans ces journaux. Transférez ces journaux en lecture seule vers un stockage distant, en particulier après un incident important. Axis fournit également un suivi en ligne de l'état du système dans la boite à outils AXIS Camera Station Integrator Suite, qui vous permet de surveiller toutes vos installations et donne l'état du système pour faciliter le service et la maintenance.

Le matériel et les logiciels (système d'exploitation et VMS) doivent être mis à jour régulièrement. En utilisant toujours les dernières versions des logiciels et des firmwares, votre système bénéficiera des derniers correctifs de sécurité et corrections de bugs. Idéalement le VMS trouve automatiquement toutes les mises à jour de logiciels et de firmwares, et le fait automatiquement ou bien vous invite à les installer. Tous les logiciels que vous téléchargez doivent provenir de sources fiables.

3.3 Traiter toute preuve selon des procédures définies

Si vous avez correctement appliqué les principes de conception et d'entretien à votre système de surveillance, AXIS Camera Station devrait être en mesure de fournir des preuves crédibles de tout incident capté par vos caméras. Ensuite, il vous faut mettre en place des procédures pour savoir comment procéder.

Vous devez suivre tous les conseils de l'autorité légale. En cas de délit grave, l'organisme chargé de l'application de la loi a le droit de décider comment protéger les preuves et vous devez suivre ses instructions.

Dans d'autres cas, le principal est d'exporter la preuve de façon sécurisée. Cela signifie qu'il faut pouvoir fournir cette preuve à l'extérieur de votre système sous la même forme, sans altération et avec une crédibilité suffisante.

L'exportation doit être effectuée par un opérateur désigné, de préférence avec un témoin. Cet opérateur peut être un professionnel externe, engagé uniquement dans le but de fournir et de documenter l'exportation de façon crédible. Le recours à un tiers indépendant pour l'exportation peut minimiser le risque pour le propriétaire de la vidéo d'être soupçonné d'avoir altéré les preuves. L'opérateur doit s'assurer d'exporter une vidéo qui couvre l'incident qui s'est produit, mais qui fournit également suffisamment d'informations sur les événements qui l'ont précédé, ainsi que sur les conséquences.

Les clips vidéo sélectionnés peuvent être exportés sur des disques à lecture seule, tels que des CD-R, DVD-R ou Blu-ray (-R), ensuite remis aux autorités concernées. Une autre solution consiste à exporter les clips vidéo vers des fichiers zip avec cryptage et protection par mot de passe. Les fichiers peuvent être signés numériquement avec une signature obtenue par hachage avec le mot de passe utilisateur. Pour confirmer le hachage et le comparer avec celui du fichier, la signature doit être saisie dans AXIS File Player. Si les hachages correspondent, c'est qu'aucune donnée de ce fichier n'a été modifiée.

Axis fournit également la fonction Rapport d'incident (Incident Report) d'AXIS Camera Station, dont les fonctions constituent un outil d'exportation avancé pour les opérateurs. L'outil doit être configuré à l'avance par un administrateur qui fournira des données, telles que des étiquettes d'incident et l'emplacement d'exportation. La fonction Rapport d'incident automatise alors l'exportation et l'organise par incident, en attribuant des noms de dossier à partir des étiquettes. L'emplacement peut être défini comme une ressource locale, par exemple un stockage en réseau (NAS), ou une ressource distante, par exemple un stockage sur cloud s'il est accessible par protocole SMB. Le rapport sera constitué de fichiers vidéo, des captures d'image en .jpg (créées manuellement par l'opérateur dans AXIS Camera Station lorsqu'il prépare le rapport), des signets en .txt et toutes les informations réunies dans un rapport en .pdf.

4 Ressources en cybersécurité

Axis applique des méthodes de durcissement de la cybersécurité en matière de conception, de développement et d'essai de ses dispositifs afin de minimiser les risques de failles de sécurité qui pourraient être exploitées lors d'une attaque. Nous suivons les meilleures pratiques en cybersécurité, par exemple en ce qui concerne la gestion des failles de sécurité, les exigences en matière de transmission et de stockage sécurisés des données et le cryptage. Nous nous efforçons de faire en sorte qu'il vous soit facile et rentable d'appliquer les contrôles de sécurité appropriés, et nos dispositifs prennent en charge le cryptage et la gestion de la sécurité.

Axis, en tant que fabricant et fournisseur du système, s'efforce d'offrir le système ou la solution la plus complète et la plus sûre, mais il vous incombe, en tant qu'utilisateur final, d'appliquer les meilleures pratiques en matière de sécurité. Pour vous aider, Axis fournit de nombreux outils, guides et tutoriels. Consultez www.axis.com/fr-fr/about-axis/cybersecurity, où vous trouverez par exemple des guides de durcissement, des informations sur la gestion de la sécurité et des articles de blog sur la cybersécurité.

À propos d'Axis Communications

En concevant des solutions qui améliorent la sécurité et les performances de l'entreprise, Axis crée monde plus clairvoyant et plus sûr. En tant qu'entreprise de technologie de réseau et leader de l'industrie, Axis propose des solutions de vidéosurveillance, de contrôle d'accès, d'interphonie et de systèmes audio. Les performances de ces solutions sont améliorées grâce à des applications d'analyse intelligentes et une formation de haute qualité.

Axis emploie près de 4 000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et d'intégration de systèmes dans le monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984 et le siège social se trouve à Lund, en Suède