



Considérations IT pour la mise en place d'un système de vidéo IP

Neuf problèmes IT critiques à anticiper lors de la conception d'un système vidéo IP

Sommaire

Introduction	3
1. Le rôle de l'expertise IT dans les systèmes vidéo	4
2. Adapter l'équipement aux exigences de la vidéosurveillance	5
3. Le rôle fondamental de la gestion du réseau	6
4. Privilégier la qualité au coût	7
5. Enjeux et solutions en matière de cybersécurité	7
6. Les limites de la sécurisation par « air gap »	8
7. Garantir la protection des données vidéo	9
8. Gestion du cycle de vie des systèmes de surveillance IP	10
9. Comprendre l'écosystème informatique des systèmes vidéo	10

Alcatel-Lucent Enterprise a mandaté l'élaboration de ce document à SourceSecurity.com.



Introduction

Un système de vidéosurveillance présente des besoins spécifiques en matière de technologies de l'information (IT). Même si un système vidéo numérique peut utiliser les mêmes technologies que d'autres systèmes informatiques, il est configuré différemment, de façon à tenir compte des besoins spécifiques de la vidéosurveillance.

La vidéo est un environnement plus exigeant qui sollicite une charge de travail plus lourde sur l'ensemble des composants d'un système informatique. Compte tenu du stress, et en particulier dans le cas d'un système d'entreprise de grande envergure, des défaillances peuvent commencer à se manifester. Ainsi, le choix d'un équipement adapté garantit une plus grande fiabilité dans le temps.

Alcatel-Lucent Enterprise a collaboré avec des experts du secteur de SourceSecurity.com et Stone Security dans le but d'identifier les 9 problèmes IT majeurs à prendre en compte lors de la conception d'un système vidéo IP. Dans ce livre blanc, nous examinons comment les besoins spécifiques d'un système de vidéosurveillance influencent les technologies de l'information déployées et la manière dont elles sont utilisées.

Livre blanc

Considérations IT pour la mise en place d'un système de vidéo IP



1. Le rôle de l'expertise IT dans les systèmes vidéo

La conception et la création d'un système de vidéosurveillance basé sur le protocole Internet Protocol (IP) requièrent un niveau élevé d'expertise informatique au sein de la communauté des intégrateurs.

Certains intégrateurs sont dotés des compétences suffisantes pour lancer un système vidéo sur IP avec expertise, tandis que d'autres peuvent rencontrer des difficultés.

Des formations et certifications supplémentaires connues de la plupart des acteurs du monde informatique peuvent permettre aux intégrateurs de fournir le niveau élevé de service requis. Pour commencer, les installateurs doivent disposer des aptitudes adéquates et d'une compréhension de base de la mise en réseau ainsi que de compétences en matière de résolution des pannes.

Les intégrateurs peuvent s'assurer une main-d'œuvre qualifiée en limitant leur choix de technologies et en veillant à ce que chaque employé soit convenablement formé au nombre réduit de technologies. En choisissant les meilleures solutions de leur catégorie et en veillant à ce que ses employés soient des experts de ces produits, un intégrateur est en mesure de fournir un système de qualité supérieure à ses clients.

Limitier la gamme de produits permet également à l'intégrateur de mieux comprendre l'étendue des fonctionnalités offertes par un produit donné. Trop souvent, un client achète un système qui offre un éventail de fonctionnalités mais il n'en utilise qu'un nombre limité au quotidien, réduisant ainsi la valeur du système qu'il a financé.

Les intégrateurs peuvent aider leurs clients en les éduquant à tirer pleinement parti du système qu'ils achètent, quel qu'il soit.

Les intégrateurs peuvent également compter sur les services de préconsultation des fabricants d'équipements pour les guider. Dans certains cas, les fabricants de matériel possèdent des connaissances spécifiques sur divers marchés verticaux, acquises au cours de leur histoire au service de ces marchés.

Les fabricants qui s'intéressent sérieusement à un marché vertical spécifique emploieront des experts de ce domaine afin de garantir un support spécifique aux besoins de chaque client. Leurs conseils peuvent aider les intégrateurs à conquérir de nouveaux marchés et/ou à rationaliser les meilleures pratiques pour les marchés sur lesquels ils opèrent.

Les fabricants proposent également des formations et des certifications afin de garantir que les intégrateurs soient bien équipés pour installer leurs systèmes. Une formation efficace et approfondie devrait être présentée dans des sessions plus courtes.

2. Adapter l'équipement aux exigences de la vidéosurveillance

Des questions telles que les exigences en matière de bande passante et d'alimentation par Ethernet (PoE) représentent des variables importantes dans un système vidéo. En outre, le serveur vidéo est plus sollicité, surtout lorsqu'il s'agit d'une vidéo en direct. Chaque bit de données atterrit sur le serveur, y compris les données qui ne sont pas enregistrées.

La vidéo est mise en mémoire cache, ce qui permet d'en conserver au moins quelques secondes avant que son enregistrement ne déclenche une alarme. Dans le cas de l'identification d'une image s'approchant à une plus grande distance, il peut être nécessaire d'avoir des périodes de mise en mémoire tampon plus longues. Toutes les entrées et sorties passent par le serveur, même si une quantité limitée de données est enregistrée sur un support à long terme.

Il existe une différence fondamentale entre la façon dont les intégrateurs de systèmes de sécurité envisagent la taille des systèmes et la façon dont les experts informatiques l'envisagent. Les intégrateurs sont plus susceptibles de parler en termes de nombre de caméras, tandis que les professionnels de l'informatique sont plus enclins à parler en termes de gestion des données du système. Bien sûr, les deux sont intrinsèquement liés mais le lien n'est pas linéaire. En général, un plus grand nombre de caméras équivaut à une plus grande quantité de données à gérer pour le service informatique. Toutefois, d'autres facteurs influent sur les besoins en données, tels que le nombre d'images, les exigences en matière de qualité d'image, les besoins de stockage, les applications diurnes/nocturnes et l'utilisation de l'analyse vidéo.

Lors de la spécification d'un système de sécurité IP, il est essentiel de traduire les exigences en matière d'équipement et de fonctionnalité de ce dernier en données nécessaires pour répondre à ces besoins. Pour un système sur site, cela signifie qu'il convient de spécifier un serveur informatique en mesure de maximiser les performances du système tout en réduisant les coûts. Des questions telles que la virtualisation et les systèmes cloud peuvent à la fois compliquer l'équation et apporter une nouvelle flexibilité.

Une autre variable liée à la conception du système est l'utilisation de caméras à la périphérie du réseau pour enregistrer des vidéos à l'aide de cartes SD. Aujourd'hui, il existe même des systèmes « sans serveur », où par exemple, tous les enregistrements sont exécutés à la périphérie. En effet, une telle approche décharge la charge de calcul du serveur vers la périphérie, réduisant alors les besoins en capacité du serveur. Les caméras actuelles fournissent des données au-delà du flux vidéo, telles que des métadonnées et des données audio, qui ont également un impact sur la conception du système.

Les experts informatiques doivent disposer d'une vue d'ensemble du système, notamment des éléments qui seront connectés, des taux de rafraîchissement, de la résolution et des codecs vidéo des caméras. Grâce à ces informations, ils peuvent calculer les besoins concernant le réseau, l'alimentation, les serveurs, la capacité des disques, la mémoire, le stockage et la question de savoir s'il est préférable d'utiliser des systèmes cloud ou sur site. Cela permet de garantir une approche approfondie et réfléchie de la conception et du déploiement.

Les fabricants fournissent des « calculateurs » logiciels destinés à aider les intégrateurs à concevoir des systèmes en traduisant les exigences du système en spécifications matérielles. Gardez à l'esprit que les calculs doivent répondre aux attentes, voire les dépasser, et permettre une croissance future.

La mise en œuvre de systèmes cloud constitue une autre variable dans la conception des systèmes de vidéosurveillance. La tendance pour la vidéosurveillance est clairement à l'utilisation de systèmes cloud. Toutefois, la décision de privilégier le cloud aux solutions sur site doit être prise au cas par cas. Les concepteurs de systèmes et les utilisateurs finaux devraient résister à l'apparente inévitabilité du cloud et plutôt prendre des décisions basées sur les besoins du client.

De nombreux fabricants sont contraints de faire passer leurs systèmes dans le cloud, mais l'idéal serait qu'ils puissent proposer à leurs clients un choix de systèmes variés, et non une solution unique.

Les fabricants sont bien placés pour conseiller leurs clients sur l'intérêt d'une configuration dans le cloud par rapport à une conception sur site. Les intégrateurs doivent également être bien informés sur les avantages de l'une ou l'autre approche ou faciliter la décision du client dans les deux cas. Le marché ne devrait pas pousser les applications vers le cloud s'il ne s'agit pas de l'approche optimale pour chaque client.

3. Le rôle fondamental de la gestion du réseau

Un système de vidéosurveillance ne peut être plus solide que son maillon le plus faible. Les commutateurs de réseau ne sont peut-être pas aussi visibles que les caméras et les VMS, mais ils n'en sont pas moins essentiels.

Ce qui a tendance à se produire, c'est que les clients considèrent le fonctionnement d'un réseau comme allant de soi, ne prêtant guère attention à son fonctionnement ou à la manière d'en maximiser l'utilité. En effet, certains clients souhaitent installer un système vidéo en utilisant une infrastructure réseau existante. Cela est possible, mais la capacité d'optimiser la partie réseau d'un système vidéo peut être limitée.

Idéalement, le client optera pour les meilleurs commutateurs de vidéosurveillance, ce qui assurera le fonctionnement fiable et efficace du système.

Chaque système vidéo étant différent, une attention particulière doit être accordée à ses exigences individuelles afin qu'il puisse remplir sa mission unique. Lors de la mise en service d'un système, le réseau ne doit pas être considéré comme un élément de second plan. Il doit au contraire être soigneusement assemblé à l'aide des meilleurs composants pour à la fois permettre les opérations à l'échelle du système et les améliorer.

Les commutateurs qui fonctionnent à « vitesse fil », c'est-à-dire que leur puissance de traitement est suffisante pour gérer la vitesse complète de l'Ethernet avec des paquets de taille minimale, sont désormais la norme dans l'industrie. Un nouveau point de différenciation entre les commutateurs est la capacité à comprendre et à gérer leur trafic.

Des commutateurs non gérés sont disponibles sur le marché, mais ils ne sont généralement pas utilisés pour les applications commerciales et/ou d'entreprise. Ils sont conçus pour être utilisés dans des réseaux de petites taille qui présentent des besoins de base, sans paramètres à configurer.

Inversement, les commutateurs gérés permettent de détecter et de diagnostiquer les problèmes de performance et garantissent la fiabilité des systèmes de vidéosurveillance. Ils permettent aux utilisateurs de voir de manière granulaire ce qui peut causer des problèmes dans le système et de comprendre à quoi ressemblent ces informations.

L'importance des commutateurs gérés, totalement configurables et personnalisables, réside dans leur capacité à fournir des données sur les performances tout au long de la vie du système. Ces informations essentielles permettent une identification rapide des problèmes et facilitent leur résolution.

Les commutateurs doivent être conçus pour répondre aux besoins des systèmes vidéo sur IP. Par exemple, dans le cas d'un commutateur à 16 ports, la puissance doit être suffisante pour faire fonctionner toutes les caméras vidéo connectées au commutateur. Les caméras PoE actuelles consomment plus d'énergie que celles des générations précédentes. Les intégrateurs doivent savoir qu'un commutateur fournit suffisamment de puissance pour gérer le nombre de caméras et la croissance future.

« Lorsque nous sélectionnons notre matériel, nous voulons que chaque commutateur soit géré, qu'il ait les capacités de bande passante et la puissance nécessaire, ce qui nous permet de gagner énormément de temps lors des dépannages. Il nous permet, ainsi qu'à nos clients, d'économiser de l'argent. Cela représente un investissement plus important au départ, mais qui se révélera rentable à long terme par la création d'un système plus facile à entretenir ».

Aaron H. Simpson,
Président et CTO,
Stone Security

4. Privilégier la qualité au coût

Dans le domaine de la vidéosurveillance, la fiabilité est essentielle, et cela commence par le choix des équipements. Pour des raisons économiques, choisir des composants de moindre qualité semble être le meilleur choix. Cependant, à long terme, le fonctionnement du système en sera affecté. En effet, opter pour une performance sous-optimale lors de la conception d'un système peut sembler économique au départ, mais les coûts cachés apparaîtront avec le temps.

Choisir un meilleur équipement - même plus coûteux - deviendra rentable.

Il est essentiel d'évaluer les coûts (tels que le prix d'un équipement plus performant) par rapport aux risques d'inadéquation ou de défaillance du système. Lors de l'évaluation des coûts et des risques, la meilleure stratégie consiste à adopter une approche fondée sur le total cost of ownership (TCO). Un autre facteur de coût à long terme à prendre en compte est la valeur des systèmes ouverts, qui peuvent garantir la flexibilité lors de l'extension ou de la modification d'un système à l'avenir.

Il est toujours préférable de travailler avec un fournisseur qui propose un produit dans lequel il a confiance et pour lequel il peut fournir un support sur une longue période.

5. Enjeux et solutions en terme de cybersécurité

Historiquement, l'industrie de la sécurité physique a été marquée par un manque de considération pour la cybersécurité des systèmes IP.

Heureusement, les acteurs de la sécurité physique accordent désormais davantage d'attention aux questions de cybersécurité à tous les niveaux et tout au long de la chaîne d'approvisionnement de la sécurité physique. En fait, la cybersécurité est devenue l'un des principaux piliers du processus de prise de décision pour les grands systèmes de sécurité vidéo.

Pour se prémunir contre les cybermenaces et restreindre l'accès à un système, il convient au minimum d'éviter d'utiliser les mots de passe proposés par défaut. Ces derniers sont moins sûrs et peuvent être devinés plus facilement par un pirate ou un robot. D'ailleurs, les mots de passe par défaut ont été interdits en Californie.

Les risques de cybersécurité commencent dans la chaîne d'approvisionnement, où les attaques peuvent compromettre un produit avant même qu'il ne soit livré. L'analyse d'un produit pour détecter d'éventuelles attaques par « porte dérobée » ou « débordement de mémoire tampon » avant sa livraison peut atténuer la menace. Les clients peuvent également choisir d'installer virtuellement un « bon code » après la livraison des produits matériels, garantissant ainsi la cybersécurité et écrasant tout code malveillant qui aurait pu être installé lors de l'expédition.

Il existe aussi une série de mesures de cybersécurité à prendre lors de l'installation et à différents stades de la mise en œuvre du système. Par exemple, la « sécurité des ports par apprentissage » garantit que seuls les appareils autorisés peuvent accéder aux ports. Si un appareil non autorisé tente de se connecter au système (par exemple, pour connecter une nouvelle caméra), une alerte se déclenche et l'accès au port est refusé jusqu'à ce qu'une personne l'autorise.

La technologie SPB (Shortest Path Bridging) peut empêcher les activités malveillantes de passer d'un système à l'autre. Des règles sont mises en place pour qu'une caméra ne puisse diffuser que vers l'enregistreur. D'autres technologies de segmentation puissantes sont par ailleurs déployées sur les réseaux multi-IoT.

Les systèmes devraient désactiver les protocoles non sécurisés tels que FTP et Telnet qui, certes, facilitent la communication à travers un réseau, mais qui peuvent offrir des opportunités supplémentaires aux pirates. Ces capacités devraient être « sécurisées par défaut » afin de ne pas autoriser de connexion au réseau à moins que cette dernière ne soit intentionnelle.

Une cybersécurité efficace nécessite également de restreindre l'accès physique à un système. Si un commutateur est déployé dans l'armoire d'un gardien dont l'accès physique est ouvert à tous, il n'est pas bien protégé. En autorisant l'accès physique à un système, il est facile pour n'importe qui - y compris un employé représentant une menace interne - de brancher un ordinateur portable et d'accéder à l'ensemble du système.

Les caméras doivent enregistrer l'accès aux équipements du réseau dans le cadre d'un principe de « défense en profondeur ».



6. Les limites de la sécurisation par « air gap »

Lorsqu'il s'agit de protéger les systèmes vidéo contre les attaques de cybersécurité via Internet, une approche courante a toujours consisté à créer des systèmes sécurisés à l'aide d'un « air gap ».

Un système protégé par « air gap » consiste à isoler un ordinateur ou un réseau et à l'empêcher d'établir une connexion externe. Étant donné qu'un ordinateur sécurisé par « air gap » est physiquement isolé et incapable de se connecter physiquement ou sans fil à d'autres ordinateurs ou périphériques de réseau, cette approche est considérée comme un moyen de protection pour garantir la cybersécurité du système vidéo.

Cependant, il est risqué de compter sur un air gap comme seule protection en matière de cybersécurité.

Il existe toute une série de situations dans lesquelles un système protégé par air gap peut être exposé à Internet, même pour une courte période. Lorsque cela se produit, le système dépend des autres mesures de cybersécurité - si elles existent - pour le protéger d'un désastre.

Partir du principe qu'un système restera toujours sécurisé grâce à un « air gap » n'est pas une solution pour la cybersécurité. Il s'agit au contraire d'une menace en devenir.

Les systèmes sécurisés par « air gap » ne sont pas non plus en mesure de tirer parti de l'intelligence artificielle (IA) et d'autres fonctions qui dépendent de l'accès à de nombreux utilisateurs et de l'analyse d'expériences partagées. Les données d'un seul client ne sont pas aussi utiles que celles de centaines de clients, disponibles dans le cloud. Les systèmes sécurisés par « air gap » ne permettent pas aux clients d'exploiter la valeur ajoutée d'une analyse plus intelligente. Renoncer à certaines données (qui s'accompagne de considérations relatives à la protection de la vie privée) est le prix à payer par les clients pour bénéficier d'une plus grande valeur.

Compte tenu des exigences actuelles des clients en matière de connexion et d'accès permanent à leurs systèmes, les cas d'utilisation des systèmes sécurisés par « air gap » sont de plus en plus limités.

Les organisations ont également tendance à s'opposer à la perspective de créer une infrastructure réseau totalement distincte pour la vidéosurveillance. La notion d'un réseau « distinct et sécurisé » n'existe pas.

7. Garantir la protection des données vidéo

La perte de données constitue un réel problème pour tout système informatique, mais elle l'est encore plus pour les systèmes informatiques de vidéosurveillance. Un système de vidéosurveillance est essentiel, et il doit fonctionner 24h/24, 7j/7. L'absence de temps d'arrêt ne permet aux administrateurs de diagnostiquer et de résoudre les problèmes de perte de données ; au contraire, ces problèmes doivent être traités en continu et en temps réel.

D'où l'utilité des commutateurs gérés. Ces derniers peuvent permettre aux administrateurs système de diagnostiquer et de résoudre rapidement tout problème de perte de données. Ils peuvent également identifier facilement la ou les sources de la perte de données. Toutefois, il ne s'agit pas de pointer du doigt le composant du système qui est en cause.

Des paquets peuvent être perdus lors de la conversion des données de la transmission fibre au cuivre et à l'Ethernet. Des convertisseurs électriques sont utilisés pour traduire les données de la transmission fibre à la transmission électrique, et ces dispositifs peuvent être une source de la perte des paquets de données.

Dans le domaine de la vidéosurveillance, la perte d'un paquet de données revient à compromettre une image vidéo, qui est, en effet, perdue à jamais. Il n'existe aucun moyen de restaurer les images vidéo perdues pendant les interruptions de service. Prenons l'exemple d'un casino, où un système vidéo défaillant a pour conséquence la perte de la couverture d'une table de jeu, ce qui peut entraîner une perte de revenus.

Dans la grande variété d'applications de vidéosurveillance, la redondance est nécessaire pour assurer un fonctionnement continu 24h/24, 7j/7.

Le besoin de fiabilité doit être évalué dans le contexte du risque par rapport au bénéfice. Un système peut être moins coûteux, moins complexe et/ou moins tolérant aux pannes, mais il risque de ne pas fonctionner comme prévu, entraînant alors des coûts supplémentaires.

Une autre variable susceptible d'entraîner des problèmes de performance dans les systèmes vidéo concerne la distinction entre la monodiffusion et la multidiffusion, qui sont deux méthodes d'envoi de données sur un réseau. La monodiffusion fournit un modèle de communication individuelle dans lequel un récepteur unique transmet des données à un destinataire unique. En contraste, la multidiffusion est un modèle d'« un vers plusieurs » dans lequel un seul émetteur fournit des données à plusieurs destinataires.

De nombreuses applications de vidéosurveillance fonctionnent en mode monodiffusion. Cela signifie qu'une caméra est surveillée en temps réel par une personne - un seul flux vidéo est concerné.

Cependant, certaines applications nécessitent une multidiffusion, dans laquelle un seul flux vidéo est visionné par plusieurs utilisateurs. Des problèmes surviennent lorsqu'un système passe de la monodiffusion à la multidiffusion. La transition ne se résume pas à un simple « actionnement de commutateur », et les nuances et les détails de la transition peuvent entraîner des problèmes de performance du système. Des problèmes apparaissent si des éléments d'un système sont configurés pour la monodiffusion alors qu'ils devraient l'être pour la multidiffusion, ou l'inverse. Une configuration correcte de ce point dans l'ensemble du système est cruciale.

Les capacités de conseil en réseau intelligent permettent à l'utilisateur final de comprendre ce qui est normal en termes de performances du réseau et de détecter ce qui est anormal ou hors des limites des attentes habituelles. Tout écart est signalé automatiquement, et des personnes peuvent intervenir si nécessaire pour résoudre les problèmes.



8. Gestion du cycle de vie des systèmes de surveillance IP

Dans le monde des technologies de l'information, le cycle de vie des produits peut varier de trois à dix ans, selon le secteur et le produit. Il existe des protocoles pour traiter des questions telles que l'intervalle entre deux pannes (MTBF), le micrologiciel et les correctifs de sécurité.

Dans le domaine de la vidéosurveillance, les cycles de vie des produits sont historiquement plus longs. Ainsi, certaines caméras vidéo datant de plusieurs dizaines d'années fonctionnent encore sur le terrain. L'adaptation des stratégies de gestion informatique aux systèmes vidéo sur IP peut révéler un décalage.

Le support informatique fourni par un fabricant apporte une valeur ajoutée considérable à l'intégrateur et à l'utilisateur final. Traditionnellement, les cycles de vie plus longs dans le domaine de la sécurité physique ont donné lieu à des systèmes qui continuent à fonctionner au-delà de la période prévue et dans un environnement non pris en charge.

Continuer d'utiliser un équipement qui n'est pas pris en charge par le fabricant peut présenter des risques inhérents. Par exemple, le fait de ne pas mettre à jour les logiciels peut ouvrir la porte à des menaces de cybersécurité.

La plupart des équipements bénéficient aujourd'hui d'une garantie de cinq ans et pourraient véritablement continuer à fonctionner pendant cinq années supplémentaires. Toutefois, compte tenu de l'évolution rapide du paysage technologique, la plupart des clients souhaitent bénéficier des capacités les plus récentes. En effet, l'accélération technologique équivaut à des cycles de vie plus courts en matière de sécurité, tout comme dans l'environnement informatique et de mise en réseau au sens large.

9. Comprendre l'écosystème informatique des systèmes vidéo

Un écosystème informatique unifié constitue la meilleure approche pour garantir la réussite d'un système vidéo sur IP. Le succès de toute nouvelle technologie repose sur un écosystème informatique qui la prend en charge. Des questions, telles que l'interopérabilité du matériel et des logiciels, garantissent le bon fonctionnement du système.

Les normes ouvertes assurent une flexibilité maximale pour les clients, aujourd'hui et demain. Des offres simplifiées sont également utiles. Par exemple, [Alcatel-Lucent Enterprise](#) dispose d'un système d'exploitation unique qui fonctionne avec tous les commutateurs Ethernet vendus par la société.

Pour garantir un réseau de système vidéo homogène et efficace, optez pour des produits qui s'intègrent parfaitement avec d'autres produits de votre écosystème. Des principes tels que l'ouverture et l'interopérabilité contribuent à l'écosystème informatique. Le succès stimule les performances de chaque élément d'un système et du système dans son ensemble.

En savoir plus sur les [solutions de vidéosurveillance d'Alcatel-Lucent Enterprise](#).