27 février 2007

Evolution de la sûreté des biens et des personnes

La convergence dans le monde de la sûreté

Lorsque nous évoquons la convergence, nous pensons à la capacité de transporter les données, la voix et la vidéo sur un même réseau. En réalité, la convergence s'étend désormais sur les domaines des systèmes du bâtiment (contrôle d'accès, vidéosurveillance, gestion technique du bâtiment, signalétique et affichage numérique…) et redessine de nouveaux espaces d'applications. La sûreté des biens et des personnes est probablement le secteur en plus rapide transformation. Nous vous proposons de découvrir cette évolution et les perspectives qu'elle ouvre. Cette convergence s'inscrit dans une évolution en trois étapes : consolidation sur une infrastructure commune qui permet la mutualisation des ressources et impacte directement les coûts, échanges d'information étendus qui augmente les capacités de diagnostics et actions combinées entre des systèmes différents qui définit un nouveau champ de la sûreté des biens et des personnes.

Aujourd'hui, la sûreté des biens et des personnes s'organise principalement autour de la vidéosurveillance, le contrôle d'accès et la détection d'intrusion. Les centres de supervision disposent de murs de moniteurs pour visualiser les caméras et utilisent des manettes et des claviers pour contrôler les caméras orientables. Les caméras, majoritairement analogiques, sont reliées au poste central de sécurité à travers un réseau dédié. Les flux vidéo sont soit enregistrés sur des magnétoscopes à cassette, soit sur des enregistreurs numériques. Les systèmes de contrôle d'accès et de détection d'intrusion aboutissent chacun sur un serveur propre. Chaque système possède son réseau dédié. Lorsqu'une intrusion est détectée, elle déclenche une alerte sur le serveur et l'opérateur doit chercher dans son mur d'image la caméra qui couvre la zone. L'opération est manuelle, lente et sujette à des erreurs d'appréciation. L'alerte reste bien sûr cantonnée au centre de supervision.

Les avantages de la convergence

1) Consolidation

Le premier avantage de la convergence est de tirer parti d'un réseau mutualisé. Elle permet d'inscrire les informations liées à la sûreté avec les autres informations qui circulent dans l'entreprise. Les informations sont disponibles au poste central de sécurité, mais aussi depuis n'importe quel endroit du réseau, dès lors que les conditions de sécurité sont assurées. Le stockage des informations peut également se consolider dans des centres informatiques : le coût de stockage de l'information est réduit et la sécurisation de ces données sensibles est améliorée. Cette consolidation demande une architecture de réseau adéquate vis-à-vis des exigences de la vidéosurveillance et du caractère sensible et critique des informations transportées. Le design doit inclure la mise en œuvre de réseaux virtuels sécurisés (VLAN et VPN, éventuel

chiffrement), de règles de QoS particulières pour transporter des flux vidéo, d'une architecture hautement disponible, d'une adaptation au transport des flux multicast pour assurer des déploiements à grande échelle.

2) Corrélation

Le deuxième avantage de la convergence consiste à enrichir les informations traditionnelles (vidéo, contrôle d'accès, détection d'intrusion) avec les informations d'alarmes incendies, de détection environnementales (fuites de gaz, liquide, augmentation de températures…), de gestion des visiteurs, de sécurité informatique, de gestion d'identité. La gestion de la sûreté physique s'intègre dans une politique plus élargie à toutes les facettes d'activités de l'entreprise : une vision consolidée de la sécurité se dessine qui mêle la sûreté physique et la sécurité informatique. L'application d'un changement de politique de sécurité prend en compte l'ensemble des biens de l'entreprise, physiques ou immatériels. La caractérisation des alertes s'effectue de manière plus fine et plus rapide. La corrélation des informations est facilitée en ramenant les images, le contrôle d'accès et la détection d'intrusion sur un même serveur. Le lever de doute est ainsi accéléré ; en cas d'alerte, les images liées à l'événement sont immédiatement affichées. Des conditions d'alertes plus élaborées peuvent se définir : augmentation de température anormale dans un local, tentative d'accès sur un réseau informatique sans identification physique préalable, etc. et les diverses technologies disponibles sont mises en œuvre simultanément pour préciser le niveau d'alerte : récupération des images des zones concernées, comptage des occupants, reconnaissance faciale, évaluation des activités en cours, analyse de l'historique (traçabilité)…

3) Actions coordonnées

Le troisième avantage de la convergence est la mise en place d'actions combinées. Dès qu'une alerte sérieuse est identifiée, tous les éléments permettant de contrôler l'environnement se mettent en œuvre et tous les moyens de communication sont utilisables de la manière la plus transparente. Une intrusion est détectée : les caméras couvrant la zone sont automatiquement pointées sur l'ouvrant et les images sont transmises aux opérateurs du centre de surveillance. Dès lors que l'alerte est confirmée, les opérateurs géolocalisent à travers le réseau WiFi les agents d'intervention les plus proches de la zone. Ils sont notifiés de leur action immédiate et grâce à leurs PDA, ils récupèrent les images et les informations liées à leur mission. Avec des équipements mobiles de vidéocommunication tels que le Frontline Communicator, le PC sécurité récupère en temps réel la vision de la scène des agents d'intervention et garde le contact en permanence. Le central isole la zone où l'effraction s'est produite : les systèmes de contrôle d'accès sont immédiatement reprogrammés pour ne laisser entrer que les agents d'intervention. Les lumières de la zone sensible sont activées et réglées à la puissance maximale. Les occupants du bâtiment sont notifiées sur leurs téléphones IP à l'aide d'un message XML qu'une effraction a eu lieu et qu'une évacuation partielle de zone est en cours. Les systèmes d'affichage numériques et les écrans peuvent également diffuser des messages aux occupants du bâtiment. Si des forces de police sont amenées à intervenir, des systèmes tels qu'IPICS permettent de mettre en relation les agents d'intervention de l'entreprise avec la police.

4) Intéropérabilité et ouverture

Enfin, l'approche de la sûreté des biens et des personnes intégrée repose sur une interopérabilité étendue et une ouverture des systèmes sur les standards. L'intéropérabilité autorise une migration en douceur des systèmes. Un dome de surveillance d'un fournisseur est contrôlable par un joystick d'un autre fournisseur. Les habitudes de travail des opérateurs ne sont pas modifiées et le remplacement d'un système par un autre ne change pas les modes opératoires. Il est également possible de piloter d'une manière identique des caméras depuis un joystick ou un poste informatique. Cisco a entrepris la création d'un programme d'ouverture et d'interopérabilité autour de ses solutions de sécurité à travers le Cisco Technology Developer Partner Program afin de permettre l'intégration et l'interaction de solutions tierces avec les produits de sécurité Cisco. Nous verrons ainsi apparaître sur le marché tout un écosystème de solutions de sécurité interopérables et qui autorisera la mise en œuvre de services avancés de sécurité sur étagère.

La sûreté des biens et des personnes a longtemps été un domaine à part dans l'entreprise. A l'heure de la dématérialisation, la protection des biens devient aussi la protection de l'information et les frontières s'estompent. Une nouvelle dimension de la sûreté des biens et des personnes apparaît, mêlant sécurité physique et sécurité des systèmes d'information. Comme dans tout cycle de convergence, si les premiers avantages semblent centrés autour de la consolidation, principalement pour

des raisons financières, le changement de modèle interviendra surtout autour des nouvelles capacités liées à la corrélation et aux actions coordonnées. Et Cisco entend bien conduire de manière active cette évolution…

Pour aller plus loin

Solutions de vidéosurveillance Cisco :

http://www.cisco.com/en/US/products/ps6918/Products_Sub_Category_Home.html

Cisco Technology Developer Partner Security :
http://www.cisco.com/web/partners/pr46/tdp/solutions_security_and_vpn.html

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camilles Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante : www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France • Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas Pérou • Philippines • Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine Russie • Singapour • Slovaquie • Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe

205534.E_ETMG_JD_02/07