ADITEL news

LE JOURNAL D'INFORMATION DE L'ASSOCIATION ADITEL | #04 | MARS 2018

ANTICIPER LES RADICALISATIONS

Édito de Pascal Dufour, président d'Aditel

Dans un kit de formation élaboré par le ministère de l'Intérieur pour donner une meilleure connaissance du phénomène de radicalisation, on peut lire la chose suivante : « On s'accorde aujourd'hui pour désigner par "radicalisation" le processus par lequel un individu développe des croyances extrêmes et en vient à considérer la violence comme un moyen d'action légitime voire souhaitable. » Cette violence, nous y sommes confrontés à chaque fois qu'un groupe essaie d'imposer ses certitudes par la force, par exemple pour empêcher la construction d'un nouvel aéroport. Elle prend un tour beaucoup plus dramatique lorsqu'il s'agit d'imposer sa loi, dans le cas de l'intégrisme religieux.

AU CŒUR DU PROCHAIN FORUM

C'est dans le but de mieux comprendre ces processus de radicalisation, afin de devancer la violence et de mieux la combattre, qu'Aditel a décidé de consacrer son prochain Forum à ce sujet. L'objectif sera de donner des clés pour anticiper les phénomènes de radicalisation dans nos établissements et de proposer de nouveaux dispositifs pour y faire face. Nous invitons à participer à nos débats les responsables sécurité, qui sont concernés au premier chef, mais aussi les responsables des ressources humaines qui ont un rôle de prévention essentiel. Le succès du dernier Forum et les appréciations que vous nous avez fait remonter nous encouragent à faire mieux encore ! Pour revenir à l'actualité de nos métiers, nous avons souhaité consacrer une large part de ce nouveau numéro d'Aditel News à deux sujets majeurs qui concernent au plus haut point les utilisateurs de la télésurveillance membres de notre association : l'évolution du référentiel APSAD et l'intervention gardiennage. Vous en trouverez notre analyse détaillée dans les pages suivantes.

EN BREF

L'armement des agents de sécurité privée va-t-il connaître un nouvel essor ? Le 1er janvier est entré en vigueur un décret précisant les conditions d'exercice des missions de surveillance armée. Ce texte découle de la loi de sécurité publique de février 2017 dont le principal apport était de modifier les règles d'ouverture du feu pour les agents de la force publique. Il vient mettre de l'ordre dans un domaine où la réglementation n'avait pas évolué depuis plus de trente ans.

IL L'A DIT

Directeur du Conseil national des activités privées de sécurité, Jean-Paul Celet se demande dans une interview pourquoi le secteur de la sécurité incendie échappe au CNAPS. « Dans certains grands établissements, des agents de sécurité privée n'interviennent pas partout, mais doivent faire l'objet d'un contrôle de moralité et d'un contrôle de compétences ; de l'autre côté, il y a des agents de sécurité incendie qui interviennent partout, mais qui n'ont pas de contrôle de moralité, ni de contrôle de compétences. » Le CNAPS a engagé une réflexion pour savoir dans quel cadre intégrer un contrôle et une réglementation de la sécurité incendie.

EVOLUTION

RTC, LA FIN D'UN MONDE

Le réseau téléphonique s'apprête à basculer complètement dans le monde de l'Internet. Orange, qui ne souhaite pas maintenir le vieux réseau RTC pour des raisons de coût, a établi un scénario sur plusieurs années.

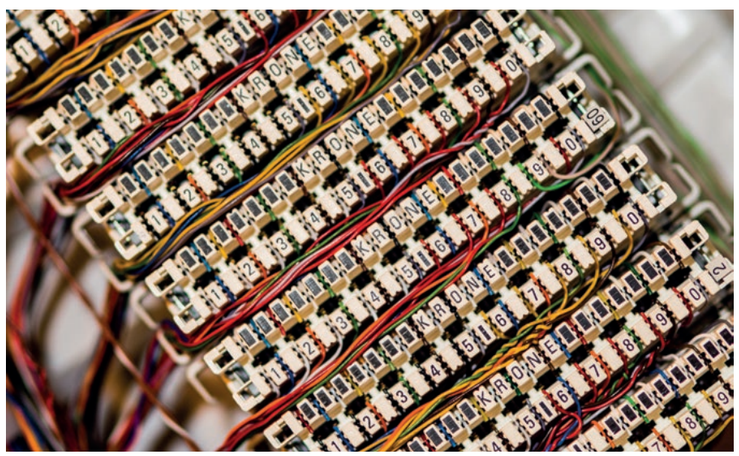
La fin du Réseau Téléphonique Commuté (RTC) approche, tous les opérateurs de téléphonie dans le monde l'ont prévue. Autrement dit, le téléphone fixe ancien modèle vit ses derniers mois, au mieux ses dernières années. Pour les opérateurs historiques comme Orange, ce réseau à bas débit coûte de plus en plus cher à maintenir et reste gros consommateur d'énergie, puisque les câbles autoalimentent les postes terminaux en énergie (en 12 ou 48V, donc sans connexion avec le réseau électrique).

UN CALENDRIER DE FERMETURE PROGRESSIVE

En 2016, Orange a soumis à l'ARCEP un calendrier de fermeture progressive de ce réseau RTC, confirmé en 2017. L'autorité des télécoms avait en effet exigé une période de préavis de 5 ans. De ce calendrier prédictif, il ressort que dès la fin de 2018, il ne sera plus possible de commander de ligne de téléphone analogique sur l'ancien modèle, ni d'installer une centrale d'alarme sur une ligne analogique dédiée.

VERS LE TOUT IP

A partir du quatrième trimestre 2018, en métropole, les nouvelles lignes téléphoniques fixes ne seront plus construites sur le RTC mais sur la technologie Voix sur IP. Le quatrième trimestre 2019 verra en métropole l'arrêt des offres « multi-lignes » pour les clients professionnels et entreprises, c'est-à-dire les lignes T0 ou services Numéris (nom de l'offre RNIS d'Orange). A partir de 2022 « au plus tôt », sera enclenchée la « migration progressive, année par année et zone géographique par zone géographique, des lignes téléphoniques RTC existantes vers le tout IP ».



DU NOUVEAU POUR LA FORMATION DES SALARIÉS

Qu'il s'agisse d'aptitude professionnelle, de sécurité ou de qualité de vie au travail, nos entreprises ont la responsabilité de renforcer les compétences de leurs salariés par la formation. Voici les dernières initiatives dans ce domaine.

UN NOUVEAU TITRE POUR LES OPÉRATEURS EN TÉLÉSURVEILLANCE

En raison de l'imprécision de la loi du 13 juillet 1983, qui faisait peu de différence entre les agents de sécurité et les opérateurs de télésurveillance, un seul et même titre qualifiait jusqu'à présent ces deux métiers aux caractéristiques pourtant bien distinctes. Ce n'est plus la cas : le métier d'opérateur en télésurveillance a été reconnu dans le livret VI du Code de la sécurité intérieure, ce qui a conduit le Groupement professionnel GPMSE à créer un nouveau titre inscrit au RNCP par arrêté du 6 mai 2015, reconnu comme valant aptitude professionnelle. Ce titre d'Opérateur spécialisé en traitement de l'information de sécurité à distance (OSTISD) est délivré après 156 heures d'une formation très spécifique à la profession.

LE CAMION FORMATEUR QUI SE DÉPLACE SUR LE LIEU DE TRAVAIL

Pour remplir leurs obligations légales en matière de sécurité incendie, les employeurs proposent généralement des formations courtes (2 à 3 heures) aux salariés, mais celles-ci génèrent de grosses pertes de temps de déplacement vers les centres de formation. Sotel a résolu ce problème en construisant une unité mobile très confortable qui se déplace sur le lieu de travail, en embarquant tout le matériel nécessaire aux exercices pratiques : maniement des extincteurs et du robinet d'incendie armé, évacuation en milieu enfumé. Ce camion est également transformable en véritable salle avec écran et vidéoprojecteur pour diffuser des films de sensibilisation aux risques d'incendie. Cette unité mobile se déplacera dans toute la France en fonction des besoins des clients.

À SAVOIR

Quand Robocop devient réalité : les autorités de Dubaï ont présenté un prototype de robot policier, destiné à patrouiller dans les rues de la ville émiratie. Faisant appel à l'intelligence artificielle, l'humanoïde étiqueté « Dubaï Police Robot » est monté sur des roulettes, mesure 1,70 m pour un poids d'environ 100 kg. Il permet notamment de signaler des délits et de payer ses amendes. La police de Dubaï souhaite acquérir suffisamment de robots d'ici 2030 pour couvrir au moins 25% des effectifs humains dans la police.

À NOTER

En application du décret n° 2016-515 du 26 avril 2016, les conditions de renouvellement de la carte professionnelle des agents privés de sécurité ont été modifiées. Les titulaires d'une carte professionnelle ayant expiré depuis 1er janvier 2018 doivent obligatoirement présenter une attestation de formation continue correspondant aux activités indiquées sur la carte initiale. A défaut, celle-ci ne pourra pas être renouvelée. Une nouvelle obligation qui va dans le sens de la professionnalisation des métiers de la sécurité.

DOSSIER

TÉLÉSURVEILLANCE

Un guide des bonnes pratiques pour les professionnels

Le nouveau référentiel APSAD

Depuis le mois de septembre 2017, le référentiel APSAD R31 a été remis au goût du jour pour mieux prendre en compte certains manques constatés sur la précédente version. Un travail nécessaire auquel Aditel a contribué, mais qui ne permet pas de répondre à tous les enjeux de la sécurité informatique.

Aditel a apporté sa pierre au nouveau référentiel APSAD pour la télésurveillance, qui vient d'entrer en vigueur. Celui-ci a en effet été élaboré sous la conduite de Christophe Bodin (CNPP), avec la contribution, notamment, de Laurent Michel (Critel), Marc Pourcellié (Sotel) et Marie-Isabelle Salmeron-Santi (Sotel).

LES RÉFLEXIONS D'ADITEL ENTENDUES

Il faut rappeler que des représentants de notre association avaient déjà été reçus par le CNPP il y a trois ans pour évoquer les différents points de faiblesse de l'ancien référentiel, en particulier les solutions de continuité d'activité et la sécurité informatique des réseaux utilisés dans le cadre de la télésurveillance. Il est satisfaisant de constater que le nouveau référentiel prend en considération ces deux points, même si les exigences en matière de sécurité informatique ne sont pas encore à la hauteur de celles des DSI des banques. Chaque responsable sécurité aura donc la charge, avec le concours de sa DSI, de vérifier que le niveau de sécurité du prestataire est en adéquation avec les règles sécuritaires de son établissement.

TROIS NIVEAUX D'EXIGENCE POUR LES TÉLÉSURVEILLEURS

De quoi s'agit-il précisément ? Le référentiel définit les niveaux d'exigence auxquels doivent répondre les stations de télésurveillance pour garantir leur efficacité dans toutes les circonstances préalablement établies. Plus le niveau est élevé, meilleure sera la continuité de service en cas d'incident. Alors que l'ancien référentiel se limitait à deux niveaux d'exigence, le nouveau en définit trois, P2, P3 et P5, ce dernier assurant la meilleure continuité de service. Le P5 convient plus particulièrement aux risques lourds concernant par exemple la banque. Il se différentie par l'architecture du système d'information du télésurveilleur, qui doit permettre le fonctionnement en mode miroir entre la station principale et la station secours, tel que décrit dans le référentiel. Le principe général est que pour toute défaillance d'un composant du système de télésurveillance, on puisse lui substituer un module qui prenne le relais de façon à garantir la continuité de service sans interruption.
En plus de cette mise à jour des niveaux d'exigence, le comité de révision a apporté des précisions nécessaires sur un certain nombre de points. En effet, il était apparu lors des audits de contrôle que certaines règles avaient fait l'objet d'interprétations qui les éloignaient de l'objectif initial, notamment celles touchant aux modules opérateurs complémentaires (MOC). Pour rappel, un MOC peut être installé dans une structure allégée, implantée dans le même bâtiment que la station ou dans un bâtiment différent.

UN VRAI PLUS POUR LA SÉCURITÉ

Au final, le véritable apport de cette version concerne les nouvelles exigences en matière de sécurité informatique. On l'a dit, elles restent en deçà de celles que demandent les DSI dans les banques, mais elles apportent l'assurance que le télésurveilleur a mené un minimum de réflexions sur les risques informatiques encourus. Cela doit se matérialiser par un référent qui définit sa politique de sécurité, celle-ci devant prendre en considération le cloisonnement des réseaux et la maîtrise des flux, la sécurité des postes de travail, la politique en matière d'authentification des utilisateurs, les précautions prises pour prévenir et détecter l'introduction de logiciels frauduleux (antivirus), les éventuels moyens de détection des tentatives d'intrusion. De nouvelles exigences ont été ajoutées pour des services couramment utilisés depuis des années, comme la levée de doute vidéo, la télévidéosurveillance, la géolocalisation et l'alarme vidéo, service qui consiste à faire remonter une alarme par un système vidéo et non plus par une centrale d'alarme.

En attendant la norme européenne

La révision du référentiel APSAD R31 intègre des ajustements qui lui permettront de répondre à certaines exigences de la norme européenne en cours d'élaboration, appelée NF EN 50518 « Centre de contrôle et de réception d'alarme », qui en est encore au stade de projet.

LA NÉCESSITÉ D'UN VOTE FORMEL

Pour devenir officielle, elle devra être adoptée dans sa version définitive par les membres du CENELEC (Comité de Normalisation Européen Electrotechnique), dont fait partie la France. Ces derniers seront alors tenus de se soumettre au règlement intérieur du comité, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à cette norme européenne. A compter de ce moment, elle s'appliquera à tous les centres de contrôle et de réception d'alarme (MARC, monitoring and alarm receiving centres) qui contrôlent et/ou reçoivent et/ou traitent les messages exigeant une intervention d'urgence.
Ce projet est subdivisé en trois parties, dont les deux premières ont été publiées en 2010, et la troisième en 2011. Une modification mineure leur a été apportée en 2013, essentiellement pour clarifier que la série de normes ne devrait pas être utilisée isolément.

CONSIDÉRATIONS TECHNIQUES ET QUALITÉ DE PRESTATION

La partie 1 traite des conditions relatives à l'emplacement et à la construction d'un ARC (Alarm Receving Center), la partie 2 des exigences relatives à l'équipement technique, la partie 3 des processus de fonctionnement. Concrètement, on retrouve dans les parties 1 et 2 des exigences comme la résistance à l'effraction des murs, plafonds et dalles, ou encore la protection contre les projectiles au niveau des portes, fenêtres et surfaces en verre, alors que la partie 3, qui concerne davantage la qualité de la prestation, met l'accent sur la description et documentation des processus fonctionnels, la formation et le perfectionnement.
Dans le projet de norme, l'AMS (système de traitement des alarmes) fait l'objet d'une annexe C spécifique importante, intégrée pour l'instant à titre informatif, dont l'objet est de décrire les différentes fonctionnalités du système.
Il faut espérer que les rédacteurs n'auront pas la tentation d'imposer des logiciels certifiés, comme on impose aujourd'hui des composants électroniques certifiés.

Il faut espérer que les rédacteurs n'auront pas la tentation d'imposer des logiciels certifiés, comme on impose aujourd'hui des composants électroniques certifiés.

POUR L'HEURE, SEUL L'APSAD COMPTE

En raison de l'agenda procédural du CENELEC, la nome NF EN 50518 ne fait pas encore office de référent en France, puisqu'elle est en cours de révision. A l'issue de cette révision, dont l'objectif est de réunir l'ensemble des exigences dans un seul document et d'en corriger certaines du fait de l'évolution du marché, elle fera l'objet d'un vote de validation.
Cependant, le dernier vote avant sa publication ayant été négatif, les travaux sur cette nouvelle norme sont toujours en cours. On peut donc anticiper qu'elle ne sera pas publiée avant plusieurs mois, d'autant plus qu'il est nécessaire de reconstituer un groupe de travail. Cela signifie que, pour l'instant, le référentiel APSAD R31 est le seul reconnu en France.

ZOOM

C'est le CNPP, acteur de référence en prévention et maîtrise des risques totalisant 320 collaborateurs en France et à l'international (Belgique, Maroc, Océan Indien), qui participe pour la France aux différents groupes de travail chargés de constituer cette norme européenne.

Encore un effort sur la sécurité informatique !

Par Pascal Dufour, président d'Aditel

Nous avons accueilli avec un grand plaisir la parution du nouveau référentiel APSAD sur la télésurveillance. Avec d'autant plus de plaisir que nous avions alerté le CNPP il y a quelques années sur les manques de la version antérieure, qui correspondait assez mal aux exigences du terrain.

LE RISQUE DE LA FAILLE

Les responsables sécurité ont besoin d'un service sans interruption et sans faille ; or, concernant les failles, nous avions fait remarquer que les risques d'introduction dans le système du télésurveilleur pouvaient être plus importants que ceux générés par l'attaque d'une station de télésurveillance, compte tenu du fait qu'il n'y avait aucune exigence en matière de sécurité informatique. Quelqu'un qui s'introduit dans le système du télésurveilleur peut ainsi agir en toute discrétion en mettant par exemple un site en panne et faire le casse du siècle. Si en plus il a piraté la centrale d'alarme, plus besoin de creuser un tunnel pour casser la chambre forte. Nous sommes satisfaits qu'un niveau de certification supplémentaire P5 s'ajoute aux P2 et P3. En effet, les responsables sécurité n'ont pas forcément la compétence pour juger de l'efficacité d'une station de télésurveillance. En conséquence, la norme doit être une référence. Malheureusement, le dernier référentiel permettait d'attribuer le niveau le plus haut en matière de qualification (P3) à des télésurveilleurs qui pouvaient avoir des solutions de continuité ne fonctionnant pas avec le nombre de raccordements gérés aujourd'hui par une station de télésurveillance, sachant aussi qu'il faut prendre en compte de nouveaux services comme la vidéo.

J'engage les responsables sécurité à se faire aider de leurs DSI pour réaliser un audit sur les risques informatiques que peut encourir leur prestataire. Car là est le prochain véritable danger.

LES PIRATES EN EMBUSCADE

Un grand pas vient d'être fait, mais en matière de sécurité informatique, on peut vraisemblablement aller plus loin. J'engage les responsables sécurité à se faire aider de leurs DSI pour réaliser un audit sur les risques informatiques que peut encourir leur prestataire. Car là est le prochain véritable danger. Le nombre de victimes de cyberattaques ne cesse de croître – 79 % des entreprises dans les 12 derniers mois – et les pirates informatiques disposent d'outils de plus en plus automatisés leur permettant de détecter de nouvelles failles de sécurité quotidiennement et de les exploiter à grande échelle.
Les attaques par ransomware sont de plus en plus régulières.
Dans l'hypothèse ou un télésurveilleur en ferait l'objet, les établissements bancaires risquent d'être concernés indirectement pour continuer à assurer la protection des agences, et on sait que dans ce cas, les montants demandés pourraient atteindre des valeurs dépassant l'entendement. C'est une raison de plus pour être vigilant sur ces problèmes de sécurité informatique.

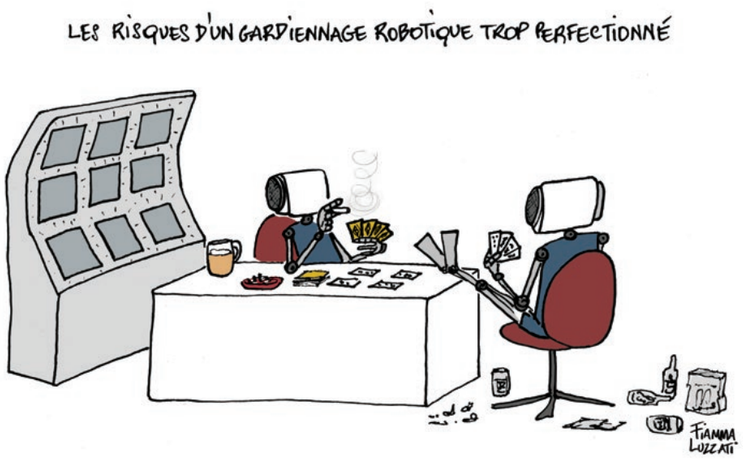
LE CHIFFRE

52%

C'est le pourcentage d'entreprises françaises qui admettent avoir subi une attaque par ransomware au cours des 12 derniers mois (étude mondiale du cabinet Vanson Bourne).

DOSSIER

L'INTERVENTION GARDIENNAGE



C'est un domaine de la sécurité privée où les attentes des clients sont légitimement élevées, mais où les prestations sont délicates à réaliser, soumises à de nombreux aléas. Aditel News fait le tour d'un métier, l'intervention gardiennage, qui pourrait rapidement évoluer avec les progrès de la robotique.

« Une prestation directement liée à notre dispositif de sécurité »

Christian Dethève, est responsable sécurité au Crédit Agricole Languedoc. Il explique à Aditel News ses attentes vis-à-vis des prestataires d'intervention gardiennage en faisant référence à son récent appel d'offres dans ce domaine.

Pourquoi avez-vous lancé un appel d'offres sur l'intervention gardiennage ?
Nous devons repositionner fréquemment les offres tarifaires de nos prestataires afin d'optimiser nos budgets. Il est important de pouvoir compter sur l'efficacité d'une prestation directement liée à notre dispositif de sécurité et pour cela de mener une étude de comparaison afin d'obtenir le bon service au bon prix. Notre groupe exige la consultation en appel d'offres lorsque le budget est important, et encore plus dans le cadre du PSEE.

Qu'est-ce qu'une défaillance dans ce domaine ?
C'est clair : ne pas respecter les délais d'intervention, ne pas être capable d'apporter une solution conforme au cahier des charges, avoir un mauvais suivi et n'être pas structuré. Lorsque qu'il y a une défaillance au niveau de ce dernier maillon, c'est la télésurveillance dans son sens le plus large qui perd en efficacité.

Qu'est-ce qu'un contrat respecté au niveau des délais d'intervention ?
Un contrat est respecté lorsque le maximum a été fait pour respecter le cahier des charges et que le prestataire réalise ce qui est demandé dans les temps.

Pourquoi avoir ajouté les clés dans les causes de défaillance ?
Pour qu'une intervention soit efficace, il faut que le prestataire soit en possession de tous les moyens pour entrer dans l'agence. Cela pose une double difficulté : savoir que le prestataire a bien les dernières versions d'ouvrants, mais surtout savoir qui les détient, car aucune entreprise ne possède une flotte suffisante pour intervenir en tout point de notre territoire. Si le prestataire ne fait pas preuve de rigueur ou n'a pas les bons outils pour gérer le stock d'ouvrants, cela peut poser des problèmes.

Avez-vous posé des conditions à la sous-traitance ?
Nous avons demandé que la sous-traitance se limite au premier niveau, en raison de ce problème des clés, mais aussi pour pouvoir identifier les sociétés qui interviennent dans nos agences. Ce sont là des précautions indispensables en matière de sécurité qui, de plus, obligent le prestataire à rechercher le sous-traitant au plus près de l'endroit où il doit intervenir s'il veut respecter les délais contractuels.

Qu'en est-il des demandes spécifiques ?
Les prestataires connaissent bien leurs activités et sont les mieux placés pour faire leurs propres propositions. Toutefois, nous avons une grosse exigence en matière de reporting sur le pilotage de l'activité. C'est la seule façon de savoir, lorsqu'un problème survient, s'il est dû à un accident de fonctionnement ou à une dérive qui est en train de s'opérer.

Comment avez-vous choisi au final ?
Notre choix s'est porté sur un prestataire qui a su montrer toute une organisation, et qui était le moins-disant sur la tarification. Les renseignements pris étaient corrects. En résumé, il s'est vraiment démarqué des autres challengers.

Lorsque qu'il y a une défaillance au niveau de ce dernier maillon, c'est la télésurveillance dans son sens le plus large qui perd en efficacité.

Pourquoi la professionnalisation du secteur est difficile

Par Philippe Brethous, Sotel

Si on peut penser que le gardiennage, grâce au législateur qui a imposé certaines contraintes à l'exercice de cette activité, a atteint un niveau de professionnalisme suffisant, il n'en va pas de même pour l'intervention. Les raisons en sont simples : le gardiennage repose entièrement sur la qualité de l'intervenant et nécessite peu de moyens. Pour l'intervention, au contraire, la qualité de la prestation se mesure aux moyens mis en place, en fonction de l'objectif visé et des particularités de la banque, qui couvre par ses agences un territoire très étendu.

EXIGER L'OBLIGATION DE MOYENS PLUTÔT QUE L'OBLIGATION DE RÉSULTAT

Aucune des sociétés qui pratiquent l'intervention n'a les moyens de répondre sans aucune défaillance à l'attente de ses clients. Les aléas ou les contraintes sont trop nombreux : circulation difficile, intempéries, pic de demandes, mesures conservatoires à assurer en attendant qu'un gardien arrive, problème de véhicule, intervention sur site démesurément longue à cause d'une agression… et surtout le nombre de kilomètres à parcourir. A cela s'ajoute la problématique des moyens d'accès. Le tout, dans les conditions économiques imposées par le marché, sans abonnement récurrent ou à des prix excessivement bas qui ne permettent pas d'avoir une flotte de véhicules suffisante. Dans tous les cas de figure, on demande d'une certaine manière aux prestataires de résoudre la quadrature du cercle. Si l'obligation de résultat ne paraît pas possible, notamment en matière de délais, il vaut mieux demander une obligation de moyens que l'on pourra facilement contrôler et qui permettra d'agir si nécessaire.

DES SOLUTIONS POUR DES INTERVENTIONS DE QUALITÉ

Voici quelques pistes pour améliorer la qualité :

- contrôler régulièrement les sous-traitants, car il est matériellement impossible qu'une société soit présente sur l'ensemble des sites qui lui sont confiés.
- demander un reporting journalier et mensuel sur les incidents de fonctionnement : délais trop longs, moyens d'accès qui ne fonctionnent pas…
- mettre en place un outil de gestion des clés qui permet de savoir prestataire par prestataire qui les détient.
- présenter une solution pour mesurer les temps d'intervention (application smartphone, serveur vocal…).
- demander un inventaire des stocks régulier, chez chaque sous-traitant, ou avoir un système pour connaître en temps réel les mouvements de clés.
- définir le temps théorique d'intervention par site, base de départ pour définir un temps maximum d'intervention qui, lorsqu'il est dépassé, fait l'objet d'un reporting.

Au vu de ce qui précède, on comprend qu'il est difficile de juger de la qualité de l'intervention sur le seul critère des délais d'intervention et qu'il est impératif de réfléchir à d'autres outils d'évaluation. Un effort de réflexion qui concerne au premier chef les prestataires : cette activité ne se professionnalisera que s'ils cessent de considérer que le seul but de leur intervention est de dépêcher au plus vite un agent.

LE CHIFFRE

9806

C'est le nombre d'entreprises de sécurité privée en France (elles étaient 9392 en 2010). 90% d'entre elles emploient moins de 20 salariés. 30% des salariés du secteur travaillent les 10 plus grandes entreprises.

De nouvelles perspectives avec la robotique

Ce n'est plus de la science-fiction, les robots sont désormais utilisés partout et par tous, même pour passer l'aspirateur, tondre la pelouse ou nettoyer les vitres. La robotique a envahi notre quotidien et a naturellement trouvé des applications sécuritaires, que ce soit dans le domaine militaire, de la sécurité civile ou dans celui de la sécurité privée (entrepôts, chantiers…). Depuis plusieurs années, le marché des drones et des robots a explosé avec le développement exponentiel de l'intelligence artificielle. Leur rôle dépasse désormais largement celui de simple soutien, ils peuvent dans certaines missions remplacer un combattant, un pompier et pourquoi pas un gardien, surtout s'il a des missions d'accueil. L'exemple du robot policier Dubaï en apporte une illustration spectaculaire (lire page 3).

DES ATOUTS INCONTESTABLES DANS LES INTERVENTIONS À RISQUE

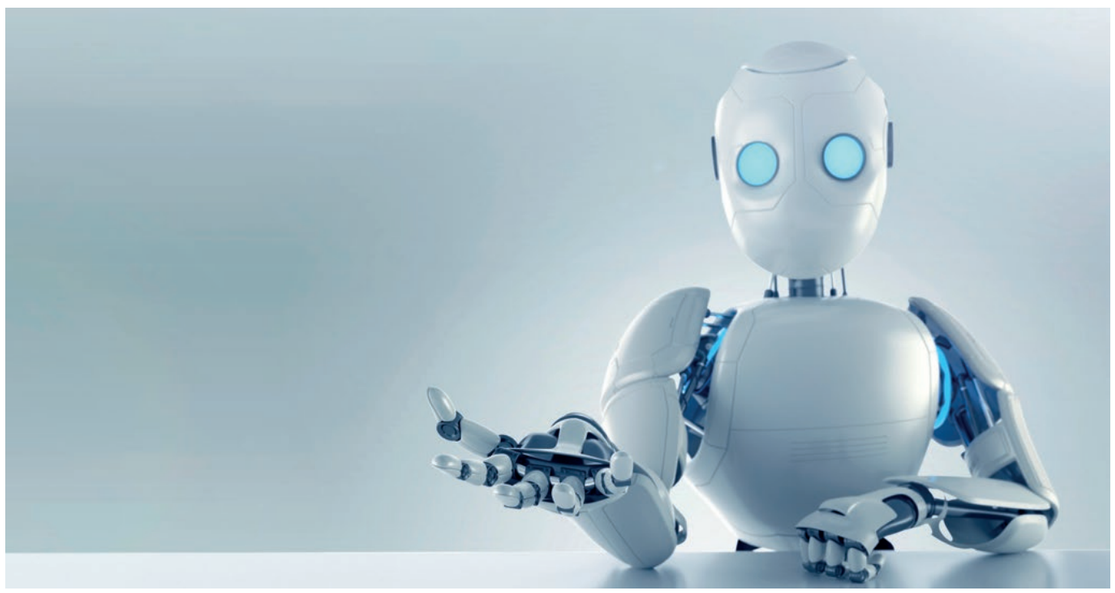
La robotique de surveillance (robots terrestres, maritimes ou drones) appliquée à la surveillance générale des sites offre un intérêt par la capacité d'observation en tout temps que lui confèrent les différents types de capteurs embarqués et par sa capacité à fonctionner en réseau. La grande souplesse d'emploi des robots et leur rapidité de mise en œuvre permettent de préciser à moindre coût le renseignement dans une zone donnée avant d'y engager des éléments d'intervention. La fourniture d'imagerie aérienne en temps réel, en s'affranchissant des obstacles (naturels ou artificiels), permet en outre de maintenir l'observation sur l'ensemble d'un secteur d'intervention.

LES DRONES, UN MARCHÉ EN FORTE CROISSANCE

Le seul marché des drones militaires et de sécurité devrait presque doubler d'ici à 2024 et dépasser les 10 milliards de dollars. Au ministère de l'Intérieur, leur usage s'impose comme une aide nécessaire à la reconnaissance ou aux interventions et tend à devenir omniprésent. On les emploie systématiquement en cas de catastrophe aérienne pour appréhender la zone de l'accident et en tirer les premiers enseignements. Il en est de même pour les secours en montagne : le Peloton de Gendarmerie de Haute Montagne (PGHM) se dote progressivement de drones pour la recherche de victimes lors d'avalanches ou d'accidents de randonnée.

EN SAVOIR PLUS

Deux arrêtés du 11 avril 2012 définissent la réglementation concernant les drones : l'un porte sur les conditions d'insertion dans l'espace aérien et l'autre sur la conception, les conditions d'utilisation et les capacités requises pour les télépilotes.



CARTE BLANCHE À...

Virginie Boivin

Acheteur sécurité à la Société Générale, Virginie Boivin a participé au dernier Forum d'Aditel. Une expérience qu'elle qualifie d'enrichissante, aussi bien pour la qualité des échanges que pour la convivialité des rencontres.

Depuis maintenant 5 ans, la direction des achats de la Société Générale, membre actif de l'association, est invitée à participer au Forum annuel d'Aditel. A titre personnel, en tant qu'acheteur de prestations et d'équipements de sécurité bancaire, j'ai accepté avec plaisir et intérêt cette invitation.
Cet événement est particulièrement enrichissant en termes d'échanges avec les prestataires du secteur de la sécurité. Au-delà de rencontres formelles lors d'appels d'offres ou de comités de suivi de contrats, cela me permet de mieux appréhender les tendances du marché, ainsi que les innovations présentées par ces prestataires sur leurs stands dédiés.
Les discussions avec les Responsables Sécurité d'autres banques sont aussi l'occasion de mettre en commun nos actualités, contraintes, bonnes pratiques, etc. Enfin, les interventions en tables rondes et conférences organisées avec les professionnels du secteur, représentants du gouvernement et même philosophes et juristes spécialisés sur les questions de sécurité, apportent un éclairage et une prise de recul pertinents sur les sujets d'actualité. Le dernier thème sur l'évolution du cash était particulièrement intéressant car il nous a permis de nous faire notre propre opinion sur un sujet qui est au centre des préoccupations de toutes les banques.
Je recommande vivement d'élargir la cible de participants à d'autres directions des achats qui y trouveront, comme moi je pense, un sourcing élargi de professionnels du secteur, des contacts avec leurs homologues acheteurs sécurité et renforceront par la même occasion leurs interactions avec leurs partenaires métiers en charge de la sécurité !

PROCHAIN FORUM

Le prochain Forum d'Aditel se déroulera les 27 et 28 septembre à Caen.
L'édition 2018 aura pour thème « Nouveaux risques et phénomènes radicaux ».
Nous vous y attendons nombreux !

NOUVEAU BUREAU

Le conseil d'administration d'Aditel accueille deux nouveaux représentants :
- Sylvain Proux, de la Société Générale, qui remplace André Molinengo appelé à d'autres fonctions
- Vincent Andrin, président du directoire de Sotel, en remplacement de Marc Pourcellié qui continuera à s'occuper de la communication d'Aditel en tant que conseiller

LE FORUM ADITEL

Détail à partir des enquêtes de fin de Forum

47,05 %	très satisfaits
47,39 %	satisfaits
3,38 %	peu satisfaits
0,13 %	pas satisfaits
2,05 %	abstention

Le taux de satisfaction est en hausse par rapport aux années précédentes : 92,5% en 2016 (La Rochelle), 90,5% en 2015 (La Baule) et 80,5% en 2014 (Grenoble).

Dans les propositions de thème les plus appréciées, on trouve les nouvelles technologies (robotique, vidéo, etc.) avec les différents impacts sur la sécurité.

Aditel News est édité par l'association Aditel : BP 31012 - 54521 Laxou Cedex • Directeur de la publication : Aditel • Comité de rédaction : Pascal Dufour, Claude Pace • Rédaction : BC Publications • Direction artistique & mise en pages : Alexandra Pourcellié, Arekusu • Illustrations : Fiamma Luzzati • Photos : Istock • Contact : secretariat.aditel@orange.fr - Tél.: 0 820 90 11 44 • Impression : Delort Imprimerie, 4 Rue de l'Industrie, 31320 Castanet-Tolosan