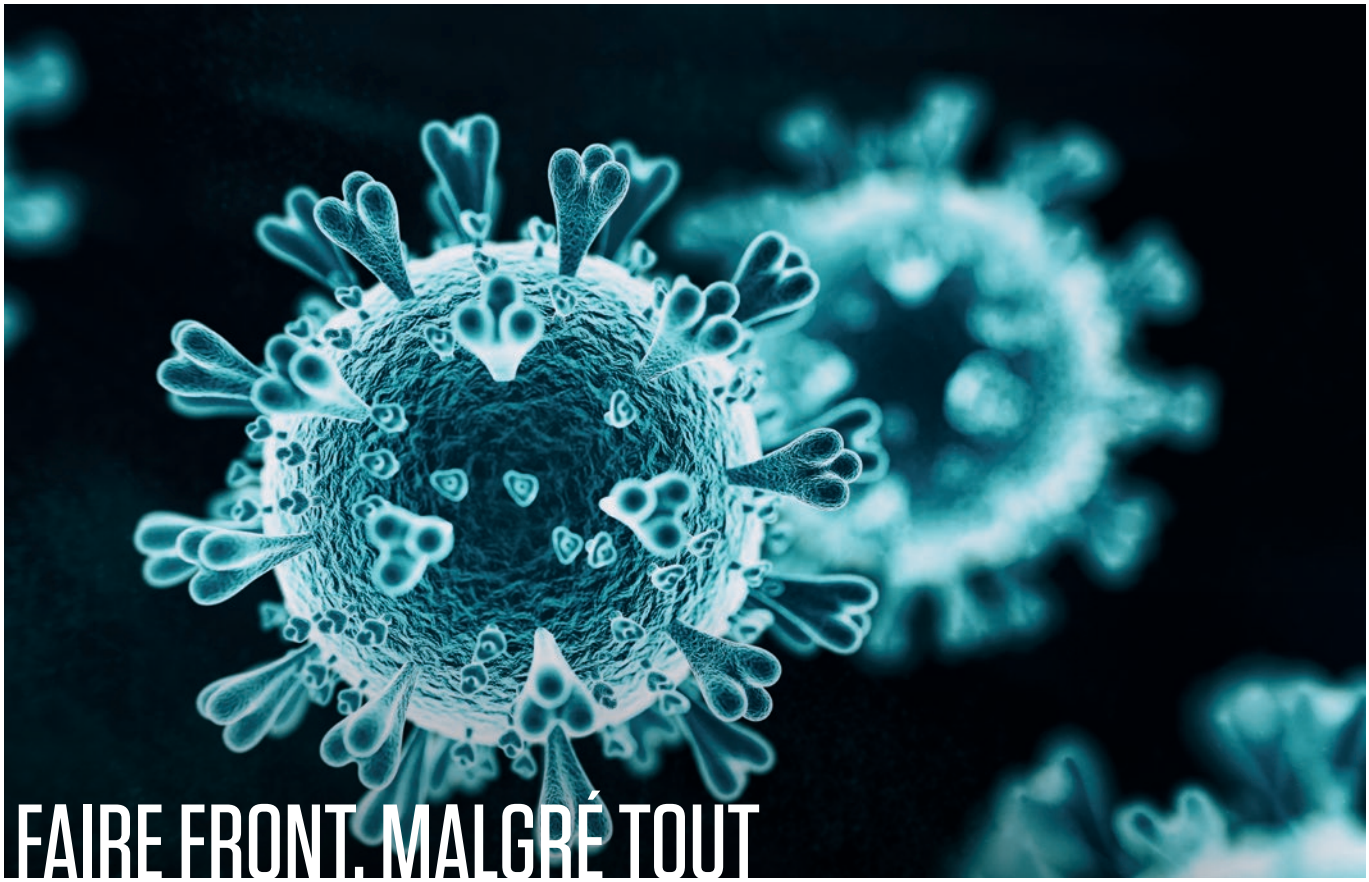
ADITEL news

LE JOURNAL D'INFORMATION DE L'ASSOCIATION ADITEL | #11 | JUIN 2020



FAIRE FRONT, MALGRÉ TOUT

Édito de Didier Moreau, président d'Aditel

Lorsque nous avons choisi pour thème de notre futur forum « La sécurité bancaire face à l'évolution des nouvelles menaces », nous étions loin d'imaginer à quel point le monde serait désuni face à la menace commune du Covid-19. Tous les plans de continuité d'activité que nous avions envisagés, chacun dans nos établissements, se sont effondrés devant l'ampleur de la crise. Il nous a fallu faire preuve de beaucoup de réactivité et de beaucoup d'imagination pour faire face aux différentes problématiques qui se sont posées à nous. Nous avons appris à vivre dans l'incertitude. Certains de nos prestataires ont essayé de nous apporter des solutions pour rompre la chaîne de propagation du virus avec des caméras thermiques qui mesurent la température du corps. D'autres, comme les sociétés de surveillance, ont continué à assurer leurs missions malgré les risques encourus par leur personnel. Tout le monde a fait front.

PENSER L'APRÈS-COVID-19

Dans ce moment où beaucoup de nos repères ont volé en éclats, nous sommes sûrs d'une chose, c'est que la façon de voir l'avenir a changé. Nous ne pourrons pas, lors d'un prochain forum, faire l'impasse sur les questions que pose l'après-Covid-19, même si notre quotidien sera toujours fait de tentatives d'effraction, de cyberattaques, de black blocs, etc. Car en matière de menaces, la nouveauté ne fait jamais que s'ajouter à l'existant.

EN VUE

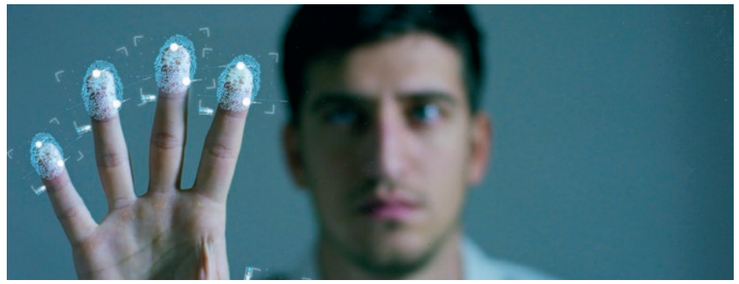
La startup Veesion propose une solution de détection automatique et en temps réel des gestes de vol à destination dans la grande distribution. Le système s'adapte aux équipements de sécurité existants et analyse en temps réel tous les flux vidéo avec un algorithme de reconnaissance de gestes. Cette solution innovante pourrait trouver une application dans l'analyse des comportements anormaux devant les distributeurs de monnaie (www.veesion.io).

NOUVEAUTÉ

Connu depuis de nombreuses années pour ses caméras, Axis se lance dans l'audio avec un ensemble de nouveaux produits. Ces solutions fonctionnent en réseau contrairement aux différents micros analogiques qui sont encore utilisés dans les agences bancaires. La société indique qu'elles peuvent être utilisées dans différentes situations. Elles améliorent notamment la sécurité dans les agences grâce aux annonces déclenchées par des événements et des appels directs. Mais elles permettent également de diffuser des annonces en direct ou programmées dans différentes zones, et même de créer une ambiance avec la programmation simple et flexible de musique de fond.

INNOVATION

Idemia, leader mondial de l'identité augmentée, vient d'équiper le nouveau siège social de Digital Garage, au Japon, de sa solution de contrôle d'accès biométrique MorphoWaveTM Compact. Il s'agit d'un lecteur biométrique équipé de technologies d'empreintes digitales 3D utilisant l'intelligence artificielle (IA), capable de scanner quatre doigts en moins d'une seconde. Les algorithmes du système garantissent un haut niveau de précision et permettent d'identifier jusqu'à 100 000 utilisateurs sur un seul appareil. Cette solution rend inutile l'utilisation d'une carte d'accès ou la mémorisation d'un code. Elle évite également les attroupements et limite les risques sanitaires liés aux surfaces touchées par de nombreuses personnes.



SOLUTION

FoxIntruder, la solution Edge déjà disponible dans les caméras Axis, s'intègre désormais également dans les caméras thermiques Hikvision DS-2TD2136, annonce la société Foxtream. Totalement embarquée dans la caméra, FoxIntruder détecte les intrusions et envoie les alarmes avec le détourage (OSD, « On Screen Display ») aux télésurveilleurs ou vers des VMS (Vitual Memory System), pour une protection périmétrique en temps réel et une levée de doute immédiate.

EN CHIFFRE

77,3% Homme

22,7% Femme

D'après le Baromètre des ingénieurs et chargés de sécurité version 2016 du CNPP, la profession de chargé de sécurité reste à forte dominante masculine, avec 77,3 % d'hommes et 22,7% de femmes. Néanmoins, les femmes exerçant cette profession sont beaucoup plus jeunes en moyenne que les hommes (37 ans et demi pour les femmes contre 43 pour les hommes). Cette différence d'âge semble indiquer une féminisation progressive de la fonction. Document à télécharger sur le site du CNPP (www.cnpp.com).

Covid-19... et après ?

S'il est encore trop tôt pour dresser le bilan complet de la crise sans précédent qui s'est abattue sur le monde au printemps dernier, on peut d'ores et déjà en tirer quelques enseignements. Dans les entreprises, dans la société tout entière, de nouvelles pratiques adoptées pour limiter la propagation de l'épidémie sont sans doute appelées à devenir demain la norme.

Vers une installation durable des technologies de surveillance

Introduits en urgence dans certains pays pour lutter contre la pandémie, les outils de traçage pourraient s'installer durablement dans nos vies. Leur acceptation sociale préfigure peut-être des changements dans le domaine de la vidéosurveillance.

« Les mesures de surveillance high-tech contre l'épidémie de Covid-19 survivront au virus et pourront devenir permanentes. » C'est Edward Snowden, le lanceur d'alerte américain et ancien employé de la CIA, qui l'affirme. Plusieurs pays, en Asie notamment, ont en effet massivement recouru aux nouvelles technologies de surveillance pour lutter contre le virus. A Singapour par exemple, afin de contrôler le respect des périodes d'isolement prescrites par les autorités, il est demandé aux citoyens d'activer les services de géolocalisation de leur smartphone. Les personnes concernées doivent cliquer de façon périodique sur un lien envoyé par SMS qui signale leur position. Les autorités procèdent à des contrôles réguliers sur le terrain pour confirmer la localisation des personnes placées en quarantaine.

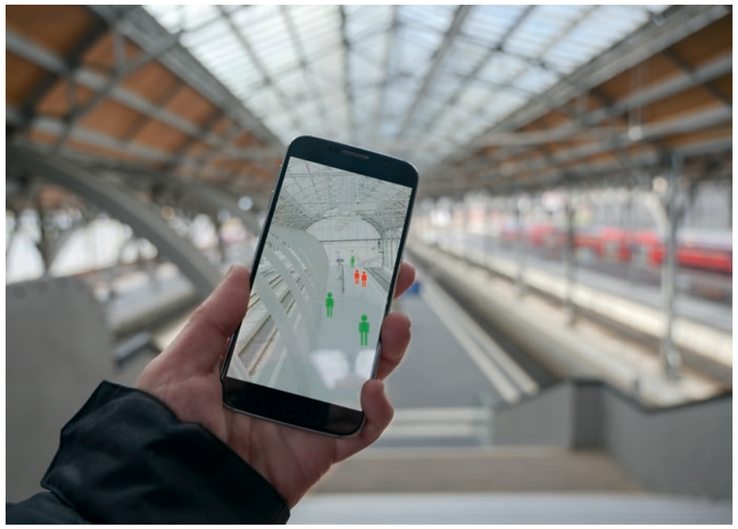
EVOLUTION DES RÉGLEMENTATIONS

Edward Snowden souligne que l'utilisation de ces technologies pour la bonne cause peut soulever des interrogations. Car ces moyens seront difficilement mis de côté une fois la crise passée. Et de fait, en temps normal, l'usage des nouvelles technologies de surveillance, jugé le plus souvent intrusif dans la vie privée des citoyens, suscite de nombreuses oppositions. La crise actuelle bousculant les résistances, on peut imaginer que cette surveillance accrue s'installera durablement, la crise mondiale faisant évoluer les réglementations dans ce sens. La CNIL, garante de nos libertés, aura plus de mal à s'opposer à ces mesures de lutte contre le risque sanitaire. Le spectre d'un pouvoir « Big Brother » déterminé à surveiller les faits et gestes des citoyens ne générera plus les mêmes inquiétudes. Au profit de leur santé, de nombreuses personnes seront davantage disposées à accepter les contraintes et les intrusions des nouvelles technologies de surveillance et de contrôle. Cette possible évolution sociétale pourrait bien avoir des répercussions sur les métiers de la sécurité, facilitant l'assouplissement de la réglementation sur la vidéosurveillance, notamment en ce qui concerne les caméras des agences bancaires qui débordent sur la voie publique.

L'utilisation de ces outils pour la bonne cause peut soulever des interrogations, car ils seront difficilement mis de côté une fois la crise passée.

UN VIRUS AUSSI INFORMATIQUE

La peur du Covid-19 donne aux cybercriminels un nouveau moyen de s'introduire dans les ordinateurs. Les utilisateurs, souvent angoissés, n'hésitent pas à ouvrir des mails qui contiennent un mot lié au coronavirus, surtout si les messages prétendent fournir des masques ou des solutions hydro-alcooliques. Les experts de la société de cybersécurité Barracuda ont noté une augmentation de 667 % des attaques de courriers électroniques liées au Covid-19 entre fin février et le 23 mars 2020.



Demain, la vidéo omniprésente dans les entreprises ?

L'expérience du confinement a généralisé l'utilisation de la vidéo pour les communications au quotidien. Alors que les vidéoconférences font déjà partie de la vie de certaines entreprises, cette évolution pourrait changer durablement les habitudes.

L'épidémie de Covid-19 a montré que les rencontres physiques, jugées hier indispensables au fonctionnement des organisations, pouvaient être remplacées par des vidéoconférences tout aussi efficaces. Diagnostic médical à distance, comité d'attribution de prêts, gestion de crise, entretien psychologique, réunion professionnelle… tous les pans de la vie économique et sociale ont été touchés.
Or, avant la crise, des groupes comme Orange avaient déjà commencé à transformer autant que possible les réunions extérieures en téléconférences. La probabilité est forte que les pratiques en vigueur dans ces établissements deviennent le quotidien des entreprises après l'expérience du confinement. « On va se rendre compte qu'une vidéoconférence n'est pas si différente d'une réunion physique », assure Jacques Gripekoven, Managing Director ALLOcloud chez Orange.

L'enjeu est que la vidéo permette aux utilisateurs d'accéder aux mêmes informations que la téléphonie.

LA VOIX NE SUFFIT PLUS

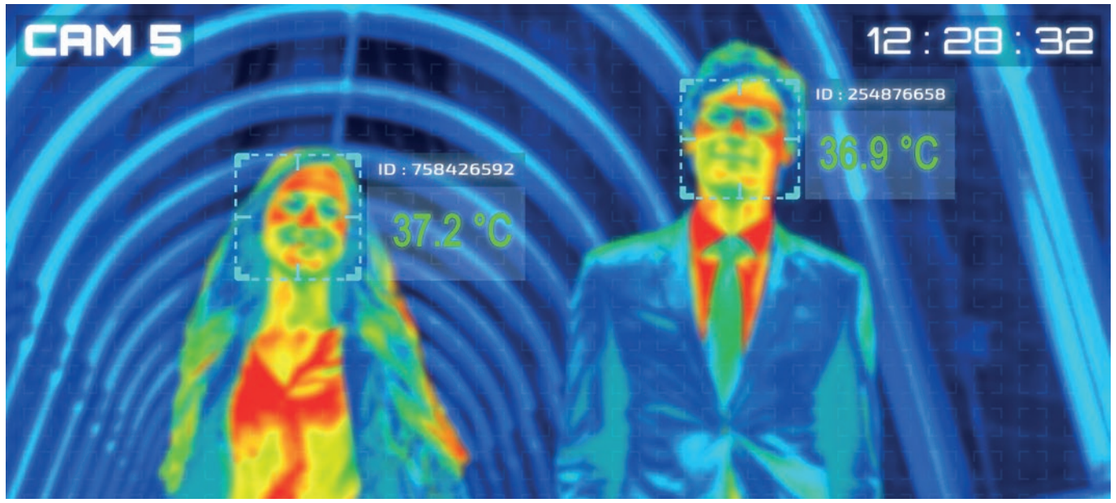
Par ailleurs, pendant cette période de confinement, chacun a ressenti le besoin de garder le contact avec ses proches. Le téléphone n'a pas suffi, et beaucoup ont utilisé les applications proposant de la vidéo (Skype, Facetime, WhatsApp, Jitsi). Car il ne suffisait pas d'entendre la voix de son interlocuteur, mais il fallait aussi le voir pour se rassurer sur son état de santé.

A l'avenir, les salariés voudront certainement bénéficier des avantages de la vidéo qui ont fait leur quotidien durant le confinement. L'enjeu est que la vidéo permette aux utilisateurs d'accéder aux mêmes fonctionnalités que la téléphonie. Si elle y parvient, elle deviendra aussi omniprésente que la téléphonie traditionnelle dans les entreprises. Les constructeurs de solutions de sécurité, les télésurveilleurs, la sécurité humaine doivent s'y préparer dès à présent.

200 MILLIONS

C'est le nombre d'utilisateurs quotidiens de Zoom dans le monde pendant la crise sanitaire, au plus fort du confinement, multiplié par 20 par rapport aux semaines précédant la crise. L'application plébiscitée dans les entreprises et dans les établissements d'enseignement a été téléchargée 600 000 fois le 15 mars. En France le nombre d'utilisateurs a augmenté de 80% les deux premières semaines de mars (source : Les Echos).

Comment les caméras thermiques peuvent protéger les entreprises et leurs collaborateurs ?



Dans le cadre de la lutte contre la pandémie de Covid-19, les caméras thermiques permettent de détecter simplement et immédiatement les personnes qui ont de la fièvre. Les explications d'Olivier Pradel, directeur de Neoxpert.

« Les caméras thermique à faible rayonnement permettent de mesurer des températures aussi bien sur des matériaux que sur le corps humain. Plusieurs entreprises fabriquent ce type de caméras. Chez Neoxpert, nous avons référencé plusieurs modèles proposés par Hikvision, à la suite de demandes reçues de la part de clients industriels et administrations pour la mise en sécurité de leurs locaux et de leurs collaborateurs dans le cadre de la lutte contre le Covid-19. L'objectif avec ce matériel est de détecter les personnes qui entrent dans un établissement et qui ont de la fièvre. Ces caméras permettent de déterminer un seuil d'admission ou de prévenance. Les acteurs de la sécurité peuvent ainsi prévenir les personnes qui passeraient devant ces caméras avec une température élevée.

UNE UTILISATION LIMITÉE À L'INFORMATION

Celles-ci, en prenant conscience de leur état, peuvent ainsi se protéger et protéger les autres. Mais conformément à la réglementation technique et au RGPD, il ne s'agit en aucun cas de mettre en place des systèmes de contrôle d'accès. Ce sont des systèmes d'information utiles pour connaître son état de santé et sécuriser l'ensemble du personnel. L'employeur n'a d'ailleurs pas le droit de refuser l'accès à un salarié pour cette raison.

Conformément à la réglementation, il ne s'agit en aucun cas de mettre en place des systèmes de contrôle d'accès.

Ce système mobile et simple d'utilisation s'installe sur un trépied ou se tient à la main. La prise de température s'effectue en ciblant les visages à une distance de 1,50 m et le résultat s'affiche automatiquement sur le viseur de la caméra. Il faut souligner que les données collectées ne sont pas enregistrées. La mobilité de ces caméras rend possible leur utilisation sur une durée limitée, le temps de gérer un événement. Elles peuvent ensuite être mises en stand-by une fois la crise passée. »

LE REGARD D'ADITEL

Jusqu'à présent, la technologie utilisée dans les établissements bancaires avait pour but de protéger les collaborateurs et les clients contre les risques d'agression physique. L'extension de la surveillance aux risques de santé serait un héritage néfaste de cette crise. Il s'agit en effet une mission qui incombe aux médecins, et non aux responsables sécurité.

Les plans de continuité d'activité butent sur la centralisation des pouvoirs

Face à un événement aussi inconcevable que la crise du Covid-19, c'est la cellule de crise qui s'est imposée dans les organisations pour piloter la continuité des structures. L'efficacité des PCA a pu pâtir d'une concentration excessive des centres de décision.

Par sa soudaineté et son ampleur, la crise du Covid-19 a pris au dépourvu de nombreuses entreprises et administrations malgré la mise en place de plans de continuité d'activité (PCA). L'événement imprévisible s'est finalement produit, plus violent même que la crue centennale de la Seine qu'on avait déjà du mal à imaginer. Quels enseignements faut-il en tirer ? Face à une situation critique d'une telle ampleur, la cellule de crise est devenue le seul instrument au service de la décision à prendre.

AMÉLIORER LA CIRCULATION DE L'INFORMATION

Que faut-il penser d'une organisation aussi centralisée composée des principaux cadres de l'entreprise ? Elle a tendance à centraliser les décisions et à restreindre le principe de subsidiarité. L'Etat lui-même s'est trouvé confronté à cette difficulté. Devant la nécessité de prendre des mesures rapides, arbitrages on été faits au détriment des échelons locaux qui auraient pu adapter et mettre en application des décisions prises au plus haut niveau. C'est ainsi que la tenue des marchés a été interdite sur tout le territoire national, alors que certains d'entre eux ne présentaient sans doute pas de danger. Ou que des joggeurs ont été verbalisés alors qu'ils s'entraînaient sur des plages désertes. L'enseignement que l'on peut en tirer est qu'il est tout aussi important de porter attention à son PCA qu'à l'organisation de la cellule de crise, en se dotant d'outils permettant de diffuser facilement de l'information sortante et les décisions arrêtées, mais aussi de recevoir de l'information entrante de toutes parts pour faciliter la prise de décision.

Une organisation aussi centralisée composée des principaux cadres de l'entreprise a tendance à centraliser les décisions au détriment du principe de subsidiarité.

27%

C'est la chute de l'activité économique estimée en France au mois d'avril par la Banque de France. Ce chiffre fait suite à une chute de 32% pour la seconde quinzaine de mars. Sur l'ensemble du premier trimestre, l'INSEE a constaté pour sa part une baisse du PIB de 5,8% dans notre pays.

VOS RÉPONSES AUX NOUVELLES MENACES

Les risques évoluent, les réponses s'adaptent. Pour prolonger le précédent dossier sur les nouvelles menaces auxquelles les entreprises sont confrontées, Aditel News a interrogé plusieurs sociétés sur leurs solutions pour faire face.

50%

Le déverrouillage des smartphones par empreinte digitale n'est pas si infaillible que l'affirment les promoteurs de ce système de sécurité. Des chercheurs américains ont en effet développé une empreinte universelle. Selon eux, elle serait capable de déverrouiller plus de 50% des téléphones portables.

Caradonna : des solutions pour faire barrage aux « black blocs »

Dans le dernier numéro d'Aditel News, des responsables sécurité avaient évoqué les difficultés qu'ils rencontraient pour mettre en place des protections contre les attaques de « black blocs ».
La société Caradonna a développé deux solutions permettant de remédier à ce problème. La principale est l'obturateur blindé pour protection de façades GAB/DAB DEMELUD®, simple à mettre en œuvre, et qui ne génère pas de frais d'intervention. Doté d'une encoche et d'une poignée amovible, cet équipement léger (il pèse environ 5,9 kg) s'installe en une dizaine de secondes, se transporte et se range tout aussi facilement. Un kit d'aimants forts est proposé en option pour faciliter le rangement côté agence, au pied du DAB/GAB.

RÉSISTANCE AUX PROJECTILES ET AUX INCENDIES

Il existe aussi une version automatique, DEMELUD® STAR, équipée d'un volet blindé roulant qui peut être commandé à distance. La deuxième solution est inspirée du rideau anti-bélier ARIÈS R.M.B® utilisé pour la protection d'un local sécurisé (ETS). Il s'agit d'une version élargie, R.F.B®, réalisée à partir de la même conception technique qu'ARIÈS R.M.B®, conçue pour couvrir l'intégralité d'une devanture. Le système est adaptable à des façades de toutes dimensions. La motorisation du tablier en lames d'acier à renforts interne permet une descente rapide en quelques secondes. La distance entre le R.F.B® et la façade verrière apporte une résistance supplémentaire contre les jets de projectiles ou les tentatives d'incendie.

Critel : des systèmes d'alerte sur tous les canaux de communication

Depuis quelques années, de nombreux objets connectés apparaissent pour mieux répondre aux besoins sécuritaires de tous : caméras de surveillance de plus en plus sophistiquées, contrôles d'accès biométriques, capteurs spécialisés de toute nature, défibrillateurs cardiaques connectés, boîtiers de téléassistance connectés, traceurs GPS… Tous ces objets permettent de répondre à de véritables enjeux de performance et de compétitivité : géolocalisation, suivi de maintenance de machines (équipement industriel, ascenseurs…), supervision de boîtiers et de systèmes informatiques, contrôle de consommation en temps réel (d'eau ou d'énergie par exemple), sécurité des personnes en mobilité (suivi d'alertes à domicile, en clientèle ou sur des chantiers).
Quel que soit le secteur d'activité, le développement de ces solutions est très rapide. En effet, les investissements mondiaux les concernant devraient atteindre 745 milliards de dollars en 2020, et le nombre d'objets connectés doublerait entre 2015 et 2020 pour atteindre 50 milliards d'unités (source Cisco).

RÉACTIVITÉ ET FIABILITÉ

Le temps où les sociétés de télésurveillance recevaient des alarmes uniquement via une centrale analogique reliée exclusivement par le réseau téléphonique est révolu : « Nous devons nous adapter à ces nouvelles technologies, déclare Dominique Vilmin, directeur général

Les banques sont aujourd'hui exposées à des menaces qui n'ont plus grand-chose à voir avec celles qu'elles devaient affronter ces dernières années.

de Critel. Aujourd'hui, les alertes peuvent arriver de n'importe où et sont beaucoup plus complexes que celles envoyées par un transmetteur d'alarme. Il n'est plus impératif d'être dans un espace couvert par une centrale pour envoyer, par exemple, une alarme agression. Un smartphone suffit. Cela signifie que nous devrons être capables de recevoir une information quel que soit le moyen pour l'envoyer : SMS, messagerie sur tout type de réseau (Internet, IP, réseaux bas débit tels que Sigfox...). » Face à l'évolution de la menace, il faut être de plus en plus réactif, tout en restant dans le cadre réglementaire (en maintenant systématiquement les levées de doute) mais en l'adaptant (au-delà des seuls biens meubles et immeubles), et tout en s'assurant de la fiabilité de ces nouveaux vecteurs d'alerte. Certains médias moins sûrs que d'autres (SMS, mails) seront à réserver à des alarmes techniques, par exemple, alors que ceux concernant la sécurité des personnes (agressions, PTI...) devront être transmis sans délai et risque de perte par des voies robustes. Une station de télésurveillance est opérationnelle 24 h/24 7 j/7. Elle est donc toujours en capacité de traiter des informations multiformes et d'appliquer des consignes, notamment en sollicitant les forces de l'ordre si nécessaire, dans le but d'agir efficacement et au plus vite.

90%

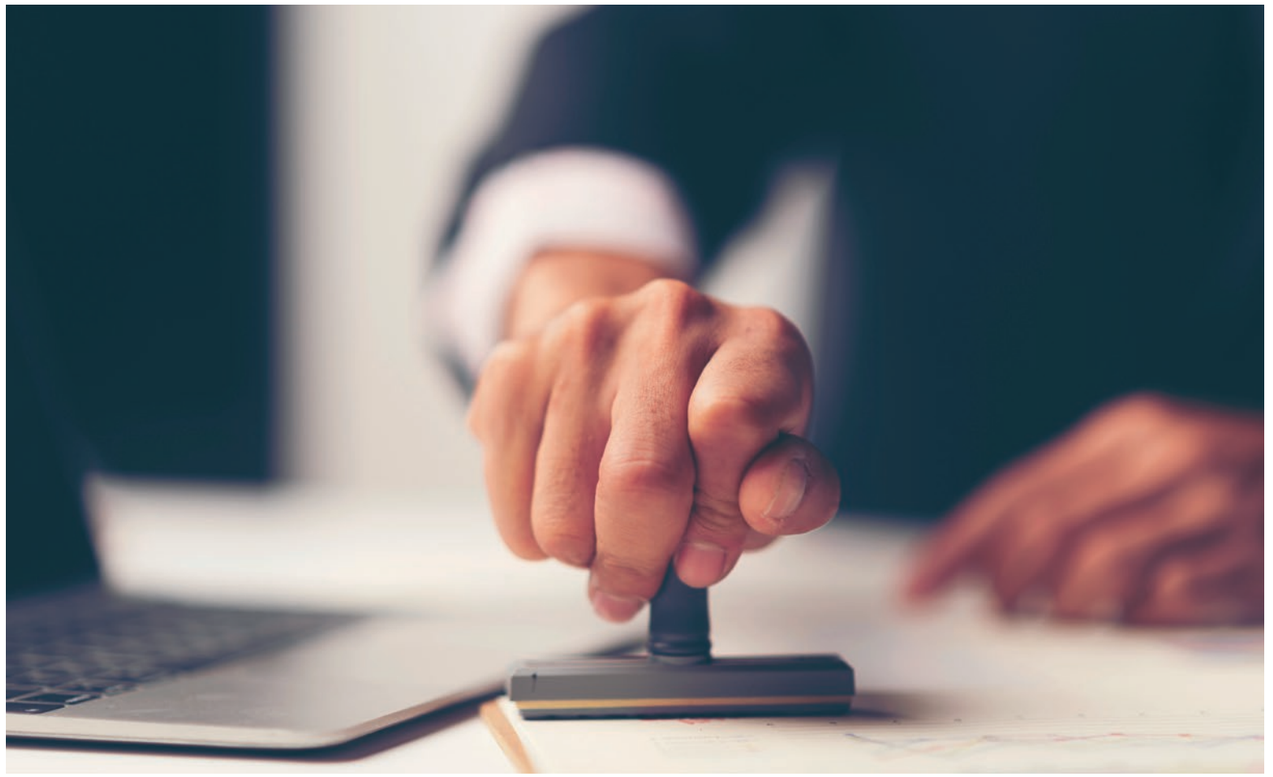
C'est la proportion des entreprises touchées par des cyberattaques ou des tentatives en 2019, parmi lesquelles 43% sont des PME. Or seulement 17% des PME disposent de moyens de défense et d'assurance. Il faut en moyenne 7 mois à une entreprise pour détecter une violation de données, et 75 jours pour reprendre une activité normale et sécurisée après une attaque.

Sotel : une expérimentation à généraliser contre les attaques « black box »

Le bilan des attaques « black box » au 8 avril 2020 est de 63 faits recensés et 13 attaques réussies pour un préjudice de 562 000 € depuis le début de l'année. Pourquoi ignorer encore qu'il y a des solutions pour faire face à cette menace ? Quand est-ce que les constructeurs d'automates, les informaticiens chargés de la gestion des automates et les fournisseurs de solutions vidéo se mettront autour d'une table pour généraliser une solution de même type que celle que LCL et Sotel avaient expérimentée sur l'automate d'une agence de Rennes avec Diebold-Nixdorf ?

L'APPORT DE L'IA

Cette solution consistait à établir un dialogue entre l'automate et un système d'analyse d'image, de façon à connaître le moment où un utilisateur introduisait sa carte bancaire et celui où il la retirait. Lorsque l'automate avait enregistré l'introduction d'une carte avec le bon code secret, il envoyait un signal sous forme de contact sec (le contact sec avait été choisi pour des problèmes de sécurité informatique), et un autre signal survenait lorsque la carte était retirée. Pendant toute cette période, la présence d'une personne devant l'automate était considérée comme normale, dans le cas contraire, une alerte était envoyée pour suspicion de tentative de fraude. Depuis cette expérience, l'analyse d'image a fortement évolué, elle peut aujourd'hui faire appel à l'intelligence artificielle sous forme de Deep Learning pour affiner le comportement des gens et déceler un acte de fraude. Il ne reste plus qu'à espérer que ce projet voie enfin le jour pour le bien de la communauté bancaire.



Gunnebo : un contrôle d'accès certifié par l'Anssi

Gunnebo a fait le choix de qualifier son système de contrôle d'accès. Les banques sont aujourd'hui exposées à des menaces qui n'ont plus grand-chose à voir avec celles qu'elles devaient affronter ces dernières années. Ce que confirme Jean-Charles Proskuryn (strategic business developer chez Fichet Group) dans PSM Magazine en expliquant son choix de faire qualifier Anssi le système de contrôle d'accès de son entreprise : « Les entreprises et organisations doivent aujourd'hui s'équiper avec des solutions qui les protègent contre des attaques de plus en plus virulentes et protéiformes, dont le risque cyber n'est pas le moindre. C'est pour cela que la double qualification Anssi que nous avons obtenue pour notre système de contrôle d'accès SMI Server est un réel atout. Ceci nous oblige à nous maintenir dans un process d'amélioration continue pour faire évoluer nos systèmes et respecter sur le long terme les critères de confiance définis par l'Anssi. » Les qualifications Anssi peuvent s'appliquer aux produits, aux prestataires de services, ou encore aux centre d'évaluation. C'est dans la catégorie produits qualifiés que se situe le système de contrôle d'accès de Gunnebo, tout comme celui de Micro-sesame de Til. Les prestataires qualifiés sont surtout de grandes entreprises comme ATOS, Cap Gemini ou La Poste pour son service recommandé électronique. Les entreprises qui souhaitent garantir un premier niveau de confiance peuvent obtenir la certification CSPN, également délivrée par l'Anssi. C'est le cas de Synchronic pour son système de contrôle d'accès XSecur.

A propos de la sécurité des stations de télésurveillance

Le référentiel APSAD qui qualifie les télésurveilleurs a été récemment modifié avec l'introduction d'un nouveau type de qualification (P5). Celui-ci renforce les contraintes en matière d'architecture des stations, mais sans aller au-delà des précautions élémentaires à respecter contre les cyber-attaques. Il existe par ailleurs un référentiel D32 qui a pour seul objectif d'accompagner ceux qui le désirent dans le renforcement de la sécurité de leur système d'information. Quand on sait que le nombre et la fréquence des attaques informatiques ont nettement augmenté au cours des dernières années, cela soulève des interrogations. Surtout quand on connaît les deux principaux points de vulnérabilité d'une station de télésurveillance. Le premier concerne l'éventuelle intrusion dans le système d'information. Il permettrait d'isoler facilement un site avant de programmer une attaque physique. Le second est de servir de rebond pour accéder au réseau de la banque. Force est de constater que les risques liés aux cyberattaques doivent plus que jamais être au cœur de nos préoccupations. Faut-il en arriver à demander que les stations de télésurveillance respectent la norme ISO/CEI 27001 démontrant la mise en place d'un système de management de la sécurité de l'information (SMSI) efficace, construit sur la base de la norme internationale de référence ISO 2700 ? Celle-ci définit une méthodologie pour identifier les cybermenaces, maîtriser les risques associés aux informations cruciales de chaque organisation, mettre en place les mesures de protection appropriées afin d'assurer la confidentialité, la disponibilité et l'intégrité de l'information. La question est ouverte et mérite d'être débattue lors d'un prochain forum.

BILAN DU FORUM 2019

Nous étions plus de 200 à nous retrouver à Mandelieu-La Napoule lors du dernier forum consacré à l'intelligence artificielle. Les échanges très riches qui ont eu lieu durant ces deux journées semblent avoir atteint leur objectif. C'est en tout cas ce qui ressort de vos réponses au traditionnel questionnaire, qui laissent apparaître un taux de satisfaction global de 96,8%. L'association est bien sûr heureuse de ce résultat, qu'elle reçoit comme un encouragement à travailler pour améliorer encore ce rendez-vous convivial et attractif !

+4,69%
de visiteurs en 2019

+1,36 %
des participants satisfaits par rapport à 2018

DÉTAIL À PARTIR DES ENQUÊTES DE FIN DE FORUM

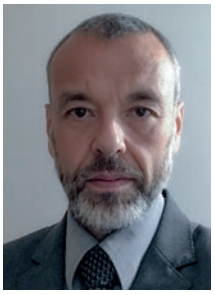
- **58,65 %** très satisfaits
- **38,19 %** satisfaits
- **0,17 %** pas/peu satisfaits
- **3 %** abstention

94,7%
d'exposants satisfaits en 2019

FORUM 2020

Le prochain forum d'Aditel est prévu à Vichy les 24 et 25 septembre prochain. Compte tenu de la situation sanitaire, il est à ce jour impossible de prévoir les mesures que prendra le gouvernement dans les mois à venir. Nous vous informerons dès que possible de la tenue de ce rendez-vous phare de la vie de notre association.

Alain Lapierre



Après 33 années au service des Caisses d'Epargne dont 12 au service sécurité de la CEIDF, Jean-François Renaut a fait valoir ses droits à la retraite. Aditel lui souhaite une bonne retraite ensoleillée sous un ciel bleu sans nuage. C'est Alain Lapierre, de la Caisse d'Epargne Côte d'Azur, qui le remplacera comme administrateur de l'association. Alain Lapierre est expert sécurité des personnes et des biens dans cet établissement après en avoir été responsable du Plan d'Urgence et de Poursuite de l'Activité (PUPA/BCM) de janvier 2006 à janvier 2017. Il était auparavant technicien spécialisé Réseaux et Sécurité.

PARTAGEZ VOTRE EXPÉRIENCE SUR LE COVID

Le Covid-19 a bouleversé nos habitudes, nous obligeant parfois à résoudre des équations difficiles. Si vous souhaitez partager votre expérience ou si vous aimeriez que certaines questions soulevées par cette crise soient abordées lors d'une table ronde, n'hésitez pas en nous en faire part à l'adresse suivante : m.pourcellie@arekusu.fr

RÉSEAUX SOCIAUX

Aditel, c'est aussi une communauté présente sur les réseaux sociaux. Vous pouvez suivre l'actualité de l'association sur notre compte LinkedIn : **https://www.linkedin.com/company/aditel-association/**

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