ADITELnews

LE JOURNAL D'INFORMATION DE L'ASSOCIATION ADITEL | #10 | JANVIER 2020

UNE MENACE PROTÉIFORME

Édito de Didier Moreau, président d'Aditel

Ce nouveau numéro d'AditelNews est l'occasion, en début d'année, de remercier ceux qui font le succès de notre association : exposants, participants, organisateurs. En 2020, notre 30e Forum poursuivra toujours le même but, celui de donner aux responsables sécurité toutes les clés pour réussir leurs missions aujourd'hui, et plus encore demain. Nous avons choisi pour cet anniversaire de vous recevoir à Vichy, sur les bords de l'Allier, charmante ville aux airs de « French Riviera » continentale.

COMPRENDRE POUR S'ADAPTER

Le Forum abordera cette année le thème des métiers de la sécurité bancaire face à l'évolution de la menace. Les risques de sécurité sont en effet de plus en plus atomisés et pas toujours identifiés, alors qu'ils se concentraient auparavant sur les valeurs entreposées dans les agences. Dans ce contexte, la profession doit s'adapter et déployer de nouvelles technologies pour détecter les signaux faibles, freiner et/ou empêcher les passages à l'acte, accélérer la prise de décision et améliorer l'efficacité des interventions. Tous les métiers de la sécurité sont concernés : sécurité mécanique, électronique, et même celle reposant sur le capital humain. Les solutions passent souvent par le numérique, et la sécurité bancaire est une activité de plus en plus transversale. Nous vous donnons rendez-vous les 24 et 25 septembre pour en parler.

NOUVEAUTÉ

C'est un nouvel équipement utilisant les technologies d'intelligence artificielle. Flir Systems a développé un modèle de caméra intégrant l'apprentissage en profondeur (deep learning). Avec sa petite taille, son faible poids, sa consommation électrique minimale et ses capacités d'apprentissage profond, Flir Firefly DL est facilement intégrable dans des systèmes mobiles, de bureau et portables. La nouvelle caméra permet aux fabricants, aux ingénieurs et aux constructeurs d'équipements de développer et de déployer rapidement des solutions pour des tâches d'automatisation complexes.

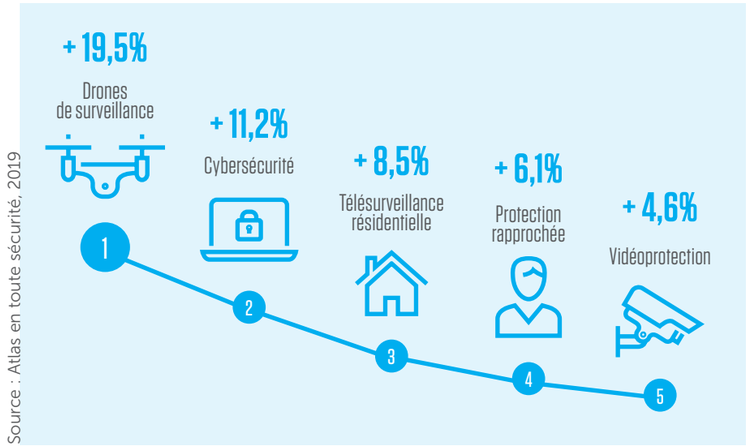
EN BREF

C'est une véritable innovation dans le domaine des contrôles de sécurité, développée par la société Rostaing. Scanforce est un gant détecteur de métaux invisibles, de conception, de technologie et de fabrication françaises. Il permet le contrôle et la filtration des personnes sans contact physique, laissant à l'opérateur les mains libres pour intervenir. Ce nouvel équipement est capable de détecter une arme de poing, une arme blanche ou toute autre pièce métallique de la taille d'un trombone.

INNOVATION

En pointe dans l'innovation en matière de transports publics, la SNCF a lancé son propre projet de vidéo intelligente après les attentats de novembre 2015. Celui-ci a pour objectif d'identifier avant le déclenchement d'une attaque les individus dont le comportement semble suspect en utilisant les caméras de protection et des algorithmes de détection. Ce projet développé avec la start-up grenobloise Smart Me Up fait appel à des technologies d'analyse de données vidéo, mais aussi d'autres types de données comme la température corporelle (obtenue à l'aide de caméras thermiques) ou le ton de la voix. Celles-ci pourraient caractériser des signaux de comportements suspects, comme une température corporelle élevée, un haussement du ton de la voix ou des mouvements saccadés. Ces signaux restent néanmoins flous et difficiles à détecter, et ne préfigurent pas nécessairement de mauvaises intentions, ce qui laisse présager un risque de nombreux faux positifs pour cette technologie.

SÉCURITÉ : TOP 5 DES DOMAINES DE CROISSANCE



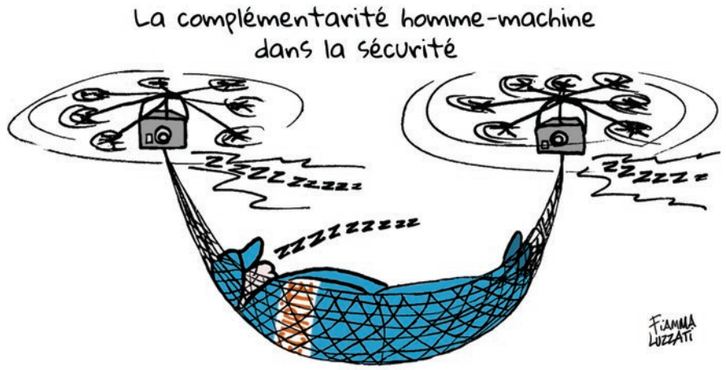
Source : Atlas en toute sécurité, 2019

EN CHIFFRE

1 736

En 2018, le CNAPS a procédé à 1 736 contrôles d'entreprises. Ceux-ci ont donné lieu à 7 194 signalements de manquements et à 347 interdictions temporaires d'exercice.

Nouveaux risques : comment faire face



Dans un monde qui change, les entreprises sont exposées à de nouvelles menaces, plus difficiles à appréhender et à contrer. Cette évolution entraîne nécessairement une redéfinition de leurs stratégies sécuritaires et la mise en place de nouvelles méthodes et de nouveaux outils. Notre dossier lance la réflexion sur ce sujet crucial pour l'avenir.

Quand les manifestations cassent l'ambiance

Alors que les manifestations s'accompagnent presque systématiquement de violences dirigées contre leurs agences, les banques doivent imaginer des aménagements pour continuer à garantir à leurs clients un accueil de qualité et la sécurité.

La violence est au cœur des mouvements de revendication d'aujourd'hui. Le fil des actualités en apporte chaque jour de nouvelles preuves, et les dégradations commises depuis le début du mouvement des Gilets jaunes ne font que refléter cette évolution. On peut s'attendre à ce que les faits violents continuent d'occuper une place importante dans les manifestations publiques. Les banques, cibles privilégiées des « black blocs », subiront à nouveau des dommages lourds financièrement. De fait, elles doivent repenser leur politique de sécurité pour protéger les agences vitrées, ouvertes et facilement accessibles à la clientèle. Cela évitera de voir des agences ou des guichets automatiques protégés par des panneaux de bois, mis à la hâte la veille des manifestions.

TÉMOIGNAGES D'EXPERTS

Certains responsables sécurité ont déjà cherché des solutions. Voici quelques remarques ou réflexions de certains d'entre eux.
François Bourguet (HSBC) : « Après les attentats de 2015 nous avions entamé une réflexion pour équiper nos grosses agences, dites "flagships", de rideaux métalliques sur portes et vitrines. A ce jour, seuls 10 sites sont équipés de la sorte. Est ensuite venu le mouvement des Gilets jaunes. Une dizaine d'autres sites, essentiellement parisiens, mais pas seulement, ont été choisis en fonction de la fréquence des circuits de manifestation. Ce n'est pas simple d'équiper des sites avec des architectures et emplacements différents, des statuts différents (propriétaires, locataires, baux commerciaux…), les contraintes des Bâtiments de France ou des municipalités, des coûts, bien sûr. »
Jean-François Renaut (CEIDF) : « Certains prestataires proposent des solutions pérennes ou temporaires : SFCC (panneau amovible), Demelud (façade automate et rideau métal vitrines), Portalp (rideau métal vitrine et porte agence). Nous avons fait poser un rideau sur la porte d'entrée lors de la rénovation de l'agence Paris Bastille. Mais la pose de rideaux sur les vitrines nécessite une autorisation de modification de façade qui peut être problématique dans certains cas, notamment à cause des Bâtiments de France. »
Claude Pace (CNCM) : « La pose de volets métalliques, que nous avions envisagée devant une de nos caisses, nous a été refusée par la Mairie de Paris. Ne perdons pas de vue que même si les vitres ne sont pas cassées (ou pas tout de suite !), les lames des rideaux et des volets, malgré leur résistance, peuvent subir des dégâts les empêchant de s'enrouler pour les retirer. »
Pascal Dufour (BPGO) : « Avant de quitter la BPGO, j'avais équipé une agence du centre de Nantes de rideaux métalliques motorisés sur toutes les baies vitrées, y compris celles du hall d'accueil. Difficile de le faire sur toutes les agences concernées en raison du coût. »

UNE RÉFLEXION DE FOND À MENER

Malgré ces quelques tentatives pour protéger momentanément ou de façon pérenne les agences, ces professionnels rappellent que la banque est une entreprise commerciale qui doit porter une attention particulière à l'accueil de ses clients et assurer leur sécurité ainsi que celle de ses collaborateurs. Si ce type de menace perdure, une réflexion de fond s'imposera pour faire évoluer les politiques de sécurité des agences bancaires, tout en restant fidèle aux règles indispensables d'accueil et de convivialité qui prévalent dans le domaine commercial.

La nécessité d'une action transversale

A nouveaux risques, nouvelles réponses : la sécurité des banques est devenue une problématique globale de l'entreprise dont le traitement dépasse désormais la seule compétence des responsables sécurité.

Confrontées à l'évolution de la menace, les banques doivent déployer de nouvelles solutions qui passent pour la plupart par le numérique. La multiplication des risques rend indispensable l'intervention de techniciens hautement qualifiés, afin de conserver en permanence une longueur d'avance sur des criminels. De ce fait, la réflexion sur les problématiques sécuritaires devient transversale au sein des établissements.

UNE GOUVERNANCE PLUS INNOVANTE

Tout ne repose plus sur le responsable sécurité, et ces questions concernent aussi bien les informaticiens chargés de la cybersécurité, ceux ayant en charge la protection des biens et des personnes, que le service du personnel, le mieux placé pour prévenir les risques liés à la radicalisation.

> La meilleure réponse à apporter à la multiplication des risques consiste à renforcer la coopération entre les différents services de l'entreprise.

Sans compter tous les métiers qui n'existent pas encore, mais dont on pressent le développement sous l'effet de la digitalisation de l'entreprise. De fait, les spécialistes des questions de sécurité ont du mal à appréhender l'ensemble des risques dans leur complexité et leur globalité. La lutte contre ces nouveaux risques nécessite un renforcement de la coopération entre les différents services concernés.
A l'heure de l'accroissement de la menace imprévisible (malveillances, terrorisme, cyberattaques…), de la multiplication des situations de crise (catastrophes naturelles, pandémies…), c'est la seule réponse à apporter pour être capable d'anticiper. Il est donc indispensable d'innover en matière de gouvernance afin d'aborder les risques avec une approche globale. Cela demande peut-être de recruter de nouveaux types de profils, comme les « calamity forecasters » (prévisionnistes de catastrophe), qui seront à n'en pas douter très recherchés dans les années à venir. Chargés de surveiller, détecter et prévoir les menaces et d'anticiper leurs impacts, ils seront des interlocuteurs essentiels pour coordonner l'ensemble des collaborateurs chargés de la sécurité au sein de la banque.

UN GISEMENT D'EMPLOIS

Depuis plusieurs années, la filière de la cybersécurité est en pleine croissance. Alors qu'elle emploie déjà autour de 25 000 salariés, les perspectives d'emploi restent florissantes… à condition de trouver les bons profils. Dans un secteur faisant appel à des compétences très spécifiques, la formation est un enjeu majeur pour répondre aux besoins des entreprises de toutes tailles et de tous secteurs.

Les drones, une solution miracle ?

Les petits aéronefs sans pilote sont plébiscités par tous les acteurs de la sécurité pour la surveillance et le contrôle à distance. Seul obstacle à leur généralisation, la réglementation qui limite encore leur utilisation.

Depuis une quinzaine d'années, la police utilise des modèles issus de l'aéromodélisme pour surveiller certaines manifestations à risques. De nombreux pays ont intégré les drones dans leur arsenal de surveillance et de renseignement. Dans le domaine civil par exemple, ils facilitent le contrôle visuel à distance des installations nucléaires, des éoliennes, des ponts et barrages, permettant d'intervenir plus rapidement en limitant les risques.

AVANTAGES MULTIPLES

Les experts prédisent la généralisation des drones, mais aussi des robots terrestres, dans tous les domaines de la sécurité. Les pompiers les enverront sur les sites de catastrophe pour évaluer les dangers et les besoins et retrouver des victimes. Les acteurs de la sécurité privée envisagent de leur côté des salles de surveillance associées à des drones assurant la veille sur des quartiers entiers. Ces appareils auraient également la capacité d'empêcher les intrusions. C'est au sein de la police, dans le cadre de la lutte contre la délinquance, que les usages potentiels sont les plus nombreux (patrouille, renseignement, immobilisation des malfaiteurs), mais ces missions pourraient être assurées par des sociétés privées. L'avantage des drones est de permettre de faire de la prévention et non de la constatation comme cela se passe avec les agents d'intervention. A condition cependant que la législation évolue, car l'utilisation des drones reste très réglementée. Le Certificat d'aptitude théorique de télépilotage rend possible leur usage professionnel, mais sauf autorisation spéciale de la préfecture, il n'est toujours pas possible de survoler un espace public en agglomération.

Onet Sécurité et Azur Drones unissent leurs forces dans la sécurité privée

Onet Sécurité et Azur Drones ont conclu un partenariat pour créer un dispositif innovant de sécurité augmentée assurant la convergence entre l'humain et la technologie. « La concurrence exacerbée sur le segment de la surveillance humaine nous amène à réfléchir à un nouveau modèle économique. Un positionnement qui rapproche homme et technologie pour augmenter le niveau de sûreté chez nos clients. L'objectif : une parfaite maîtrise budgétaire et un recentrage de nos équipes de surveillance sur la prise de décision », indique Pascal Pech, directeur général d'Onet Sécurité.

> Un positionnement qui rapproche homme et technologie pour augmenter le niveau de sûreté chez nos clients.

COMPLÉMENTARITÉ HOMME-MACHINE

Onet Sécurité a fait le choix stratégique de s'adosser au leader européen du drone autonome. Avec son système Skyetech, Azur Drones est en effet la seule société à avoir une autorisation générique de la DGAC pour effectuer des vols hors vue et sans télépilote (vols de jour comme de nuit sur des sites privés sous contrôle d'accès). Une spécificité qui permet à tout agent d'Onet Sécurité de déployer une surveillance aérienne en pilotant une caméra mobile, visible et thermique. Ce dispositif autonome répond au mieux aux besoins des clients ayant de vastes domaines à protéger tout en valorisant le travail des agents de sécurité. « Nous y voyons une application directe aujourd'hui pour surveiller les sites centraux des banques qui se sont construits en dehors des agglomérations. Demain, lorsque l'utilisation des drones sera différemment régulée, il sera possible de réaliser des missions de levée de doute et des rondes périmétriques pour les agences, solutions basées sur la complémentarité homme-machine. » Source : communiqué Onet Sécurité.

Une application de gestion de crise en temps réel

En matière de gestion de crise, l'application Crisis Care propose une solution collaborative pour faire face à la croissance et à la diversification parfois imprévisible des risques et menaces. Témoignage de Xavier Malcher, responsable du service sécurité de la BPRI.

« La BPCE a choisi l'application Crisis Care, utilisée par la BPRI en cas de manifestations, incivilités graves ou incident gravissime. Cette solution mobile collaborative apporte réactivité et proximité et facilite la prise de décision en cas de crise. Elle présente l'avantage de permettre au service sécurité de déclencher des alertes en dehors des heures ouvrées, le weekend et les jours fériés. En cochant les différentes options proposées par Crisis Care, nous pouvons alerter les personnes concernées directement via l'application, par messagerie ou appel sur téléphone portable, ou bien par e-mail.

> « C'est une solution que nous avons régulièrement utilisée lors des manifestations violentes de Gilets jaunes et dans le cas d'incivilités particulièrement agressives.»

GÉRER LES ÉVÉNEMENTS VIOLENTS

L'application donne accès à un annuaire téléphonique des principaux responsables de la banque et aux numéros de téléphone utiles, et permet de faire une conférence téléphonique. Un suivi des alertes en cours est mis en place lorsqu'on identifie des événements pouvant avoir un impact sur l'entreprise, et une check-list préalablement enregistrée permet de vérifier que tous les problèmes qui avaient été anticipés sont bien traités. Crisis Care a été dernièrement enrichi de nouvelles fonctionnalités : intégration de vidéoconférence avec Jitsi, intégration de Chat War Room avec WhatsApp, prise de notes avec objectif 0 papier (démarche verte ISO 14001), main courante sur mobile. C'est une application que nous avons régulièrement utilisée lors des manifestations violentes de Gilets jaunes et dans le cas d'incivilités particulièrement agressives.
Cela a permis à notre direction d'être avertie pratiquement en temps réel des dégradations commises dans nos agences, des fermetures des locaux, et des replis et de la mise en sécurité de nos collaborateurs et clients.
De même, le pôle maintenance a pu faire intervenir ses prestataires dès la fin des manifestations pour la mise en sécurité des locaux. »

Le marquage codé, arme ultime contre les casseurs

Grâce à un procédé d'identification chimique inoffensif, il est possible de retrouver, même longtemps après les faits, les auteurs d'actes violents. Une expérimentation a été lancée à Paris dans deux agences de la BPRI.

Les PMC (produits de marquage codé) sont des dispositifs indétectables à l'œil nu, inodores et incolores (non toxiques) permettant le marquage des biens, des personnes et des lieux. Ce n'est qu'une fois révélés, sous une lampe spéciale, qu'ils émettent une fluorescence caractéristique détectable dans le domaine du visible. Accessibles aux professionnels comme aux particuliers, les produits actuellement commercialisés se matérialisent sous différentes formulations chimiques. Mais quel que soit le type de formulation, cette technologie confère à tout support marqué une identification par un code unique. Initialement développés pour repérer les contrefaçons, les PMC ont vu leurs domaines d'application se diversifier. Ils offrent en particulier des moyens de lutte dissuasifs et discriminants contre les atteintes aux biens en établissant un lien fort entre des faits délictuels et un individu mis en cause par le marquage de sa personne ou de ses vêtements.

La technologie PMC confère à tout support marqué une identification par un code unique.

EN LIEN AVEC LES FORCES DE L'ORDRE

L'usage de tels dispositifs s'inscrit bien sûr dans un cadre légal : la révélation d'un PMC ne peut être dissociée de l'action des forces de l'ordre. A la BPRI, Xavier Malcher a pour projet d'utiliser cette technologie pour aider la police à retrouver les individus qui s'en prennent aux vitrines des agences, même lorsqu'ils sont entièrement cagoulés. Un test est en préparation avec la société Protect sur deux agences parisiennes de la banque situées boulevard Saint-Germain, qui entrent en travaux en 2020. Deux buses seront installées sur la façade des agences, à 3 m de haut et dirigées vers le trottoir, permettant l'éjection d'un ADN chimique sur les manifestants, déclenchée soit manuellement de l'intérieur, soit par la télésurveillance, soit par des contacts de chocs. Même si un agresseur n'est pas arrêté immédiatement, ses vêtements resteront marqués durablement, ce qui permettra son identification en cas de perquisition. Le produit pourra être éventuellement couplé à un brouillard opacifiant.

GILETS JAUNES

En mars 2019, après les violences qui ont émaillé certaines manifestations de Gilets jaunes, le gouvernement a annoncé son intention de recourir à l'avenir au marquage codé pour identifier les casseurs.

Pour des formations vraiment opérationnelles

Les entreprises de sécurité privée doivent s'engager davantage dans une formation concrète de leurs salariés, au plus près des réalités du terrain, explique le PDG de Goron sur le site cette société. Extraits.

« Pour répondre aux nouveaux enjeux de sûreté, la logique actuelle consiste à enfler les heures de formation initiale des agents et à empiler des cours théoriques. Ce n'est pas forcément la solution. Il convient de privilégier des formations et des entraînements concrets in situ qui correspondent aux besoins réels sur le terrain. En effet, face à un acte terroriste, peu importe qu'un agent ait suivi 600 heures de formation initiale, il faudra qu'il sache exactement comment réagir sur son lieu de travail. Quand on voit aujourd'hui l'accumulation erratique des CQP et l'incohérence parfois des réglementations applicables – le tout enserré dans la contrainte du financement et de la gestion du temps de travail –, on comprend la frustration des entreprises de sécurité privée. En réalité, elles se sont laissé confisquer le sujet de la formation par des prescripteurs externes depuis des années, sans vraiment réagir.

« Les entreprises de sécurité privée se sont laissé confisquer le sujet de la formation par des prescripteurs externes depuis des années. »

REPRENDRE L'INITIATIVE

Il est donc urgent que les entreprises de sécurité privée reprennent avec beaucoup d'ambition l'initiative de la qualification et de la formation concrète de leurs agents. Elles ne doivent pas se contenter de croire que leurs personnels – et particulièrement les nouveaux recrutés – sont compétents au seul motif qu'ils possèdent une carte professionnelle en bonne et due forme. »

A LIRE

Retrouvez ce texte dans son intégralité sur le blog « Rendre notre monde plus sûr » de la société Goron : https://rendre-notre-monde-plus-sur.goron.fr/trois-evolutions-indispensables-securite-privee-normalisation-formation-agents-unite-professionnelle/

Risques numériques : l'ANSSI, un tiers de confiance

L'ANSSI est l'organisme public qui aide les entreprises à lutter contre les nouvelles menaces numériques. Ses certifications apportent un gage de confiance aux utilisateurs publics et privés de produits informatiques.

L'évolutivité et la transversalité des risques numériques nécessitent de reconsidérer le modèle de gestion des risques. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose une démarche pour y parvenir. Ce service créé en 2009 est rattaché au secrétariat général de la Défense et de la Sécurité nationale (SGDSN).

La certification atteste de la robustesse des produits par une analyse de conformité réalisée sous l'autorité de l'ANSSI.

LABELLISATION DES PRODUITS ET DES PRESTATAIRES

L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée en direction des opérateurs d'importance vitale (OIV). L'agence est notamment chargée de promouvoir les technologies, produits et services de confiance, les systèmes et les savoir-faire nationaux auprès des experts comme du grand public. Elle contribue ainsi à développer la confiance dans les usages du numérique. Son action auprès des différents publics comprend la veille et la réaction, le développement de produits pour la société civile, l'information et le conseil, la formation ainsi que la labellisation de produits et de prestataires de confiance. L'ANSSI supervise notamment la certification CSPN, qui atteste de la robustesse des produits par une analyse de conformité et des tests de pénétration réalisés par un évaluateur tiers sous son autorité. Cette démarche répond à un schéma et à un référentiel adaptés aux besoins de sécurité des utilisateurs et tenant compte des évolutions technologiques.

SÉCURITÉ

En choisissant un produit certifié, son utilisateur s'assure que les fonctionnalités certifiées offrent un niveau de sécurité éprouvé et résistent aux attaques d'un niveau déterminé. Certaines sociétés qui fournissent des solutions de sécurité électronique ont déjà obtenu l'agrément.

Sécurité informatique, attention aux failles !

Nul système n'est totalement invulnérable, pas même les solutions dites sécurisées qui comportent des risques inhérents à leur conception. Le meilleur moyen de les surmonter est de faire preuve de la plus grande vigilance.

En matière de systèmes d'information, les technologies de sécurité se multiplient mais toutes les solutions ne mettent pas en sécurité. Vulnérabilités, portes dérobées et erreurs de conception et de configuration de certains de ces produits exposent les entreprises à un risque accru.

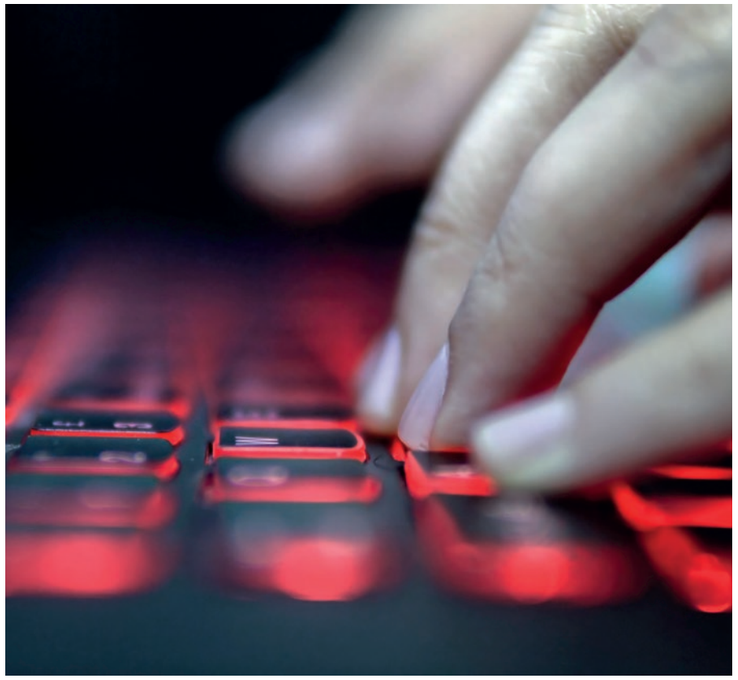
OBJETS CONNECTÉS MAL SÉCURISÉS

Deux exemples illustrent les cyber-risques provoqués par ces vulnérabilités. En 2016, de nombreux services ont été inaccessibles pendant plusieurs heures à la suite d'une attaque contre une entreprise de redirection DNS qui assure la correspondance entre l'adresse IP du serveur et le nom de domaine. La cause de cette indisponibilité ? Un logiciel malveillant s'était introduit dans des objets connectés mal sécurisés, notamment les caméras. En principe, dans la banque, toutes les caméras sont connectées sur le réseau d'entreprise, le risque augmente surtout lorsqu'elles le sont sur Internet. Or, il peut être tentant d'installer un jour une caméra pour un problème particulier et d'y accéder depuis son poste de travail par Internet, la plupart du temps poussé par les fournisseurs. Mais c'est justement là qu'est le danger.

Il peut être tentant de connecter une caméra à Internet pour des raisons pratiques, mais c'est là qu'est le danger.

CONNAÎTRE L'ORIGINE DES COMPOSANTS

Autre exemple, avec Huawei, l'une des plus grandes sociétés de technologie du monde, récemment accusée par le gouvernement des États-Unis d'espionnage au profit de la Chine. L'année dernière, l'entreprise s'est ainsi vu interdire de vendre de l'électronique aux agences gouvernementales américaines. Au même moment, soupçonné de fraude, son directeur financier était placé en résidence surveillée au Canada. Si les accusations de cyber-espionnage sont avérées, cela signifie que Huawei a la capacité de s'infiltrer profondément dans un pays ou une entreprise pour perturber les opérations électroniques sensibles. La vigilance s'impose donc sur la provenance des composants utilisés dans le matériel de sécurité des agences, centrales d'alarme, stockeur, contrôle d'accès. Tel est en tout cas le sens des recommandations de l'ANSSI pour que les entreprises se fassent agréer auprès d'elle.



LE CHIFFRE

141

A la date du 1er juin 2019, 320 produits étaient entrés en évaluation. Parmi eux, 141 ont été certifiés CSPN.

BIENVENUE À...

Audrey Cohade

Nouveau visage féminin au conseil d'administration d'Aditel, Audrey Cohade a rejoint le conseil en remplacement de Jean-Marie Capelli. Arrivée chez Nexecur en 2007, elle est actuellement membre du comité de direction élargi de l'entreprise. Audrey Cohade est responsable d'un département dont les missions sont les synergies au sein du Groupe Crédit Agricole et la représentativité de l'entreprise auprès des groupements et syndicats professionnels des métiers de la sécurité.
Dans son précédent poste, elle était responsable de l'organisation et de la qualité (process et normes métiers) pour l'ensemble des clients de Nexecur et responsable du département de télésurveillance (5 centres), chargée principalement du suivi de la clientèle bancaire. Bienvenue à elle dans ses nouvelles responsabilités chez Aditel.

ADITEL, LES BANQUES ADHÉRENTES

Banque Populaire ..... 9 caisses
Caisse d'Epargne..... 11 caisses
Crédit Agricole ..... 14 caisses
Crédit Mutuel..... 16 caisses
CIC ..... 6 banques
Crédit Coopératif.....
Crédit du Nord.....
LCL .....
HSBC .....
Société Générale.....
BNP Paribas .....

ADITEL REGROUPE

20 492 agences bancaires.....

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/**

30e FORUM, APPEL À CONTRIBUTIONS

Vous en avez eu un avant-goût à la lecture de ce numéro, Aditel souhaite pour son 30e Forum revenir à des thèmes qui concernent au plus près tous les métiers de la sécurité bancaire. Chaque entreprise participante, qu'elle soit spécialisée en sécurité mécanique, sécurité électronique et même en sécurité faisant appel à des moyens humains comme le gardiennage ou le transport, porte une expertise spécifique qui peut nourrir et inspirer les autres. Le but est de susciter un enrichissement mutuel en partageant les solutions déployées ou les projets en cours pour s'adapter à ces nouvelles menaces que sont le terrorisme, les dégradations d'agences, les incivilités, les cyber-attaques.... Que ces solutions passent par les technologies du numérique ou par des protections physiques ou humaines, toutes se complètent. C'est cette complémentarité que le Forum cherchera à mettre en évidence. Si vous avez des idées à partager, des propositions à faire, n'hésitez pas à nous en faire part.
Contact : Marc Pourcellié (m.pourcellie@arekusu.fr)

FORUM 2020

24 et 25 semptembre
Palais des congrès de Vichy
Au programme de cette édition : « Les métiers de la sécurité bancaire face à l'évolution de la menace »

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 • Contact : secretariat.aditel@orange.fr - Tél.: 0 820 90 11 44 • Impression : Delort Imprimerie, 4 rue de l'Industrie, 31320 Castanet-Tolosan