L'actualité de la Menace et de la Protection des Entreprises et des Etats

SECURITY DEFENSE
Business review

N° 126 • 21 Avril 2015

L'actu de la Menace

➔ La sécurité dans les aéroports français

Nous avons écrit souvent dans ces colonnes que la sécurité des aéroports parisiens était toute relative, eu égard à certaines populations qui travaillent en Zone Réservée ou à celles qui vont et viennent en Zone Publique sans aucun motif de voyage (particulièrement à Orly Sud). Nous avions alerté en 2001 les responsables d'Aéroports de Paris et les Autorités de l'Etat sur le danger de voir se généraliser, en Zone Réservée de Roissy CDG, un entrisme actif de la part de certains employés originaires de pays non européens. Nous avions souligné qu'il s'agissait là d'un baril de poudre à mèche lente, qui constituerait un jour une menace réelle que ne contiendraient pas les lignes Maginot de la sûreté qu'on s'évertue à dresser contre 100 % des voyageurs, alors que la menace est aussi à l'intérieur du périmètre. On nous avait objecté que, juridiquement, il n'était pas possible de discriminer, mais nous avions surtout constaté un total manque de clairvoyance et l'absence de courage de la part des responsables des directions et ministères concernés par l'aviation civile… Deux faits, parmi tant d'autres passés sous silence depuis 15 ans, viennent confirmer nos craintes. Lundi 30 mars, les douaniers de l'aéroport de Nice ont saisi plus de 21 kg de cocaïne dans un bagage à l'arrivée d'un vol en provenance de République Dominicaine. Les 18 paquets de cocaïne saisis ont été découverts dans une valise abandonnée sur le tapis roulant de l'aéroport. Sur l'étiquette d'enregistrement de la valise figurait le nom d'un voyageur présent dans le hall et en attente de ses bagages. Visiblement, les trafiquants n'avaient pas hésité à utiliser le nom d'un voyageur innocent présent sur le vol pour tenter d'importer les stupéfiants, en apposant son nom sur les étiquettes d'un bagage ne lui appartenant pas. Ceci éclaire de façon intéressante les pratiques des trafiquants en tous genres et ne peut être possible qu'avec la complicité, à l'arrivée, de salariés de l'aéroport (lorsque la livraison des bagages se fait en Zone Réservée) ou par l'accès libre de gens extérieurs (lorsque la livraison se fait à tous vents comme à Orly sud).

Autre fait encore plus grave : l'agression au couteau dont a été victime, le 10 avril après-midi, un militaire en mission Vigipirate dans l'enceinte aéroportuaire d'Orly. Heureusement, légèrement blessé au dos le sergent, qui était dans des toilettes du personnel de la plateforme (théoriquement donc en Zone Réservée) au moment de l'agression, a réussi à mettre en fuite son agresseur. Rapidement étouffée, cette affaire est néanmoins révélatrice de la présence, en Zone Réservée, d'individus radicalisés par les appels au meurtre de soldats ou policiers français lancés, entre autres, par les leaders de l'Etat Islamique. Plus inquiétant encore : on peut parier que l'enquête de police judiciaire n'aboutira jamais, faute de témoignages, tant il est vrai que sur les plateformes parisiennes l'omertà est la règle… *AE*

SOMMAIRE

AGENDA

➢**06 – 07 Mai 2015 – Doha, Qatar**
Trans Middle East 2015
➢**10 - 12 Mai 2015 - Dubai, EAU**
Airport Show
➢**20 – 21 Mai 2015 – Versailles/Satory, France**
Forum Entreprises Défense
➢**19 - 21 Mai 2015 – Barcelone, Espagne**
Critical Communications World
➢**19 - 21 Mai 2015 - Singapour**
IMDEX

Plus d'infos

➔ Guyane

Les forces armées en Guyane viennent d'achever 7 semaines d'opérations, engageant 300 militaires et 60 gendarmes, contre les orpailleurs illégaux. Résultat: 60 chantiers ont été neutralisés et un stock précieux de matériels logistiques a été détruit.

Interview du GAR Marc Watin-Augouard

Directeur du centre de recherche de l'Ecole des officiers de la gendarmerie nationale

♦ SDBR : Général, avec le recul quel bilan tirez-vous du FIC 2015* qui s'est tenu en janvier à Lille ?

M WA : Le bilan est très positif et nous avons eu un retour de nos partenaires et des participants tout à fait satisfaisant, montrant que le FIC 2015 était meilleur que le FIC 2014, qui lui-même avait progressé par rapport au FIC 2013. L'important est d'être sur une tendance toujours positive en termes de qualité. On nous demande de traiter de très nombreux sujets, ce qui amène à multiplier le nombre d'ateliers, l'inconvénient pour les participants étant de ne pouvoir tout voir et tout entendre, donc nous les incitons à revenir l'année prochaine. Le cadencement annuel du Forum s'articule avec l'observatoire FIC qui se réunit tous les mois (10 par an) pendant deux heures à Paris, sur des thématiques pointues : Internet des objets, sécurisation des données bancaires, etc. C'est une façon d'entretenir l'esprit FIC toute l'année. Par ailleurs, la tenue à Lille, la veille de l'ouverture officielle du FIC 2015, de la conférence sur la réponse aux incidents & l'investigation numérique (CORIIN**) a été l'occasion d'enrichir le FIC par une manifestation très complémentaire. L'objectif de CORIIN est de permettre aux enquêteurs spécialisés, experts judiciaires, chercheurs du monde académique ou industriel, juristes, spécialistes de la réponse aux incidents ou des CERTs de partager et d'échanger sur les techniques du moment.

♦ Est-ce que le FIC va continuer à œuvrer vers l'international ?

Comme vous l'avez constaté, les participants venus de l'Etranger étaient plus nombreux cette année que les années précédentes et plus de pays représentés. Il est important de pouvoir ancrer le FIC dans l'Europe. Nous avons des progrès à réaliser dans ce domaine, vis-à-vis de la Commission et du Parlement Européen, pour que leur participation soit plus forte dans le futur. La tenue à Lille, pendant le FIC, d'une session de la FIEP (association des gendarmeries d'Europe et de Méditerranée qui associe l'Argentine et le Qatar) a été l'occasion d'attirer sur le FIC des délégations étrangères qui ont axé leur réflexion sur les nouvelles technologies et en particulier celles qui sont concernées par la cybersécurité. Nous sommes convaincus que ces délégations reviendront lors de prochaines éditions. On vient au FIC par curiosité, on y revient pour son intérêt!

♦ Est-ce que le FIC d'aujourd'hui correspond à ce dont vous rêviez il y a 10 ans ?

Oui. Lorsque j'ai créé le FIC en 2007, le but était de décloisonner complètement le dialogue Etat / entreprises / collectivités territoriales / centres de recherche et universités, en créant un espace d'échanges. En 2007, j'avais utilisé la formule empruntée au monde médical « d'entretiens de Bichat de la cybercriminalité », pour souligner le caractère unique de ces rencontres entre spécialistes publics et privés, français et étrangers, autour d'un même sujet les concernant. Le FIC n'est concurrent de personne et ma préoccupation d'origine était justement de ne pas refaire ce que font très bien par exemple «les Assises de la sécurité et des SI» à Monaco. Les interventions de personnalités publiques et de responsables de l'administration sont en cela différenciantes. C'est aussi devenu un endroit de rencontres entre les employeurs du secteur de la cybersécurité et les étudiants: le besoin s'accroit de manière considérable pour des ingénieurs dont le temps de formation va de trois à cinq ans. Ce que je souhaite c'est que le FIC devienne plus un lieu d'échange de visions: ou va-t-on? Quelle est l'ambition en matière de cybersécurité? Quel est notre regard prospectif sur ce qui va se passer dans les 5 ans à venir? Que va apporter la 5G en termes de capacité, de traitement des données, d'absorption des informations véhiculées par l'internet des objets, etc.?

♦ En termes de capacité technologiques n'avons-nous pas déjà une idée assez précise de ce qui va se passer ?

Certes, mais il est aussi important d'anticiper les usages qui vont en naître. Il n'y a que 8 ans que les gens ont commencé à disposer d'un Smartphone. Combien d'usages sont nés de ce téléphone intelligent en 8 ans? C'est considérable! La prospective par rapport aux usages n'est pas simple et l'un des objectifs du FIC est justement d'échanger autour de cette problématique.

Suite de l'interview page 3

** FIC : www.forum-fic.com*
*** CORIIN : http://www.cecyf.fr/activites/recherche-et-developpement/coriin*

Interview du GAR Marc Watin-Augouard

Directeur du centre de recherche de l'Ecole des officiers de la gendarmerie nationale

♦ Faut-il avoir peur du risque Cyber ?

Je dis toujours - il ne faut pas avoir peur d'avoir un peu peur - car le stress peut inciter à ne pas baisser la garde. Nous sommes en pleine transformation numérique et digitale, la société va changer de paradigme et nous allons assister à des évolutions considérables avec le Cloud, le Big Data, la Robolution, l'intelligence artificielle, etc. La donnée devenant le centre de gravité du cyberespace, nous allons complètement changer nos rapports à la Santé, à l'Education, à la Culture, à la Démocratie, etc. Tout va très vite. Rendez-vous compte que le Smartphone d'Apple date de 2007, que Facebook n'a été connu qu'en 2006, que Twitter atteint son premier million d'utilisateurs en 2008 mais explose réellement à partir de 2012…Tout cela il y a moins de dix ans! Aujourd'hui nous avons en outre des usages de ces outils qui n'étaient pas imaginés à leur démarrage. Le FIC est un des lieux qui participent à l'éveil des esprits sur cette mutation majeure.

♦ Avez-vous le sentiment que la France anticipe ces changements à venir ?

Le temps du politique est souvent celui de l'immédiat, avec les exigences du traitement des problèmes dans le monde réel. Il faut que nos dirigeants portent en même temps un regard sur le futur. C'est toute la difficulté de l'exercice! Il faut offrir une vision, tout en répondant à l'urgence du quotidien. Le Plan sur la Nouvelle France industrielle ne bénéficiera pas immédiatement à ceux qui l'ont lancé, mais c'est un investissement pour l'avenir. Il ne faut pas sacrifier la prospective face à la pression de l'instant, sinon on risque de prendre de plein fouet les conséquences de la transformation numérique... Incontestablement, la France a fait des efforts considérables sur le volet cyberdéfense depuis 2008 avec le premier Livre Blanc, conforté par le Livre Blanc 2013. En revanche, la lutte contre la cybercriminalité n'a pas bénéficié d'un soutien aussi fort au profit des acteurs (Justice, Intérieur, Finances). Sans doute faudra-t-il engager des moyens plus importants, car les prédateurs opèrent un transfert vers le cyberespace qui leur permet de réaliser des gains plus importants avec un risque pénal plus faible. Les menaces ne seront plus tout à fait les mêmes dans dix à quinze ans et il faut s'y préparer, sans abandonner les champs d'action qui sont toujours d'actualité. Par exemple, l'insécurité routière sera sans doute fortement réduite grâce à la voiture intelligente. Pour autant, nous ne pouvons oublier qu'il y a eu plus de 3000 morts sur nos routes en 2014. Voilà l'exemple type de la contradiction entre un présent qui s'impose et un futur qui se dessine.

♦ Est-ce que l'Etat est le mieux placé pour cette approche prospective ?

Pendant des années l'approche prospective en France a été une approche étatique, alors qu'à mon avis ce devrait être une approche complètement croisée entre l'administration, des organismes privés, des entreprises, des associations, des universités, etc. pour essayer d'imaginer ce que sera demain. Chacun a une clé de la réponse, mais personne n'a toutes les clés. Aujourd'hui nous sommes dans un système maillé; il faut donc se servir de ce maillage pour organiser des clusters de compétences, public/privé, lieux d'échange et de partage. Le nouveau préfet Cyber me semble parfaitement s'inscrire dans cette logique de maillage, ce qui est une très bonne chose pour le ministère de l'Intérieur. Il faut profiter de cette dynamique pour renforcer les liens avec la Justice, qui est particulièrement concernée par la transformation numérique.

♦ Finalement, n'y a-t-il pas une inadéquation des profils de la fonction publique aux enjeux de demain ?

Il faudra bien se poser la question du recrutement des personnes qui arrivent par concours d'administrations (ENA, Police, Gendarmerie, administrations diverses) et qui vont être en poste pendant plus de 30 ans. Dans 15 ans, si les profils recrutés ont été formés selon les archétypes du 20ème siècle ou qu'ils ont simplement subi une acculturation aux principes cyber du 21ème siècle, il y aura un grave problème pour la France. Cela signifie qu'il faut changer les modes de sélection et qu'il faut instaurer des concours plus axés sur les technologies numériques. Ce sont des enjeux de ressources humaines. Aujourd'hui, le gendarme est souvent doté des outils (tablettes, Smartphones, etc.) qui créent pour lui une bulle informationnelle en temps réel. Demain, les pratiques professionnelles vont encore évoluer. Cela signifie aussi que nous aurons de plus en plus des politiques de sécurité « bottom up » et non pas « top down ». De plus en plus, les personnels de terrain reviendront au centre du jeu et il faudra que la superstructure parisienne mette en perspective et donne du sens à une production de sécurité plus déconcentrée, avec des relations, entre le citoyen et les représentants de l'ordre public, très branchées sur les réseaux sociaux. C'est déjà embryonnaire au sein de la Gendarmerie, pour la prévention des cambriolages et pour la lutte contre les vols de matériels agricoles.

Suite de l'interview page 4

Interview du GAR Marc Watin-Augouard

Directeur du centre de recherche de l'Ecole des officiers de la gendarmerie nationale

♦ Constatez-vous une résistance au changement ?

La résistance au changement peut basculer lorsque la masse critique emmène la décision, sans que cette masse critique soit nécessairement constituée des chefs et des sous-chefs: cela peut être une diagonale, du bas vers le haut, qui a compris et qui peut amener le changement. Dans l'entreprise, c'est lorsqu'il y a eu une attaque importante que le niveau stratégique prend enfin vraiment conscience de la menace, sinon on se contente souvent de la mise en conformité (SSI, DSI, ISO) sans en faire un sujet stratégique. Grosse erreur. Dans la Gendarmerie, en cinq ans le sujet est monté au niveau stratégique, ce qui est peu pour une administration.

♦ Où en est le concept de souveraineté en matière de Cyber ?

La souveraineté ne sous-entend pas forcément d'être franco-français, car c'est souvent une vue de l'esprit. Etre souverain signifie que nous avons consenti à des abandons de souveraineté mais, pour pouvoir le faire, il faut un minimum de degrés de libertés: avoir des capacités technologiques, de la recherche et du développement, des capacités humaines. Nous avons les ingrédients, mais il faut les structurer et les organiser pour avoir au minimum une réponse, française ou européenne, et à défaut faire partie des réponses. Nous avons perdu la bataille du hardware (plus de fabrication d'ordinateurs), nous avons perdu la bataille du software (sauf cas particuliers), mais nous n'avons pas encore perdu la bataille des données sur lesquelles nous avons beaucoup de potentialités: Big Data, IoT, Robolution, réalité augmentée, intelligence artificielle, etc. S'il y a une volonté politique de faciliter ces développements, avec une vraie vision stratégique, nous pourrons peut-être reprendre le leadership. Pour cela, il faut que la start-up qui porte un projet novateur ne reste pas sur la touche, car les grandes entreprises de demain ne sont pas encore nées.

Interview réalisée par Alain Establier

ECA aide à localiser les minidrones malveillants

Depuis quelques mois, le repérage et la neutralisation de minidrones, survolant des sites interdits ou sensibles, par les forces de police et de gendarmerie ressemblait un peu à une course à l'échalote…

Le groupe ECA, filiale du Groupe Gorgé, spécialisée dans la robotique, a développé une technologie embarquée innovante sur son drone IT180 qui devrait apporter une aide efficace aux autorités pour localiser, identifier et poursuivre les pilotes et les vecteurs aériens malveillants en moins d'une minute.

Le système, mis au point avec un partenaire, est basé sur l'utilisation du drone IT180 d'ECA Group intégrant plusieurs charges utiles. Après détection du drone contrevenant par des moyens fixes au sol, la stratégie consiste à faire intervenir le drone IT180 qui, dans un premier temps, localise le pilote grâce à sa technologie embarquée puis, dans un second temps, s'en approche pour procéder à son identification par ses caméras, ne laissant ainsi aucune possibilité au pilote de se fondre dans la nature et de disparaître avant l'intervention des forces de l'ordre. Au contraire, cette solution permet d'appréhender le pilote en flagrant délit et de collecter des preuves nécessaires en vue de poursuites judiciaires ultérieures. Le système a d'ores et déjà été évalué avec succès par les autorités de l'Etat à deux reprises. www.ecagroup.com

Dans les secteurs

➔ HID Global a racheté Quantum Secure

HID Global, leader dans les solutions d'identification sécurisée, a annoncé avoir racheté Quantum Secure, fournisseur de solutions logicielles axées sur la gestion des identités, la conformité avec la législation et l'activation des accès dans le cadre d'une infrastructure de sécurité physique. Les principaux marchés d'HID Global sont le contrôle d'accès physique et logique, dont l´authentification forte et la gestion des identités, l'impression et la personnalisation de cartes, la gestion de visiteurs, les systèmes d'identification officiels, l'identification animale ainsi que diverses applications industrielles et logistiques. Ayant son siège social à Austin (Texas), HID Global emploie plus de 2200 personnes à travers le monde et possède des bureaux dans plus de cent pays. HID Global est une marque du groupe ASSA ABLOY. Avec ce rachat, HID Global sera à même de déployer une solution complète de gestion des identités. La société Quantum Secure, créée en 2004, est basée à San Jose (Californie). Parmi les clients de Quantum Secure: le ministère américain de l'Énergie (DoE), Oracle, le nouveau World Trade Center, Adobe Systems, NVidia, United Health Group, AMD, AT&T, eBay, Visa, SMU, PG&E, Juniper Networks, Symantec Corporation et les aéroports de San Francisco et de Toronto. www.quantumsecure.com www.hidglobal.com

➔ Motorola Solutions développe le concept de «smart cities» en achetant PublicEngines

Motorola Solutions a acheté PublicEngines, fournisseur privé de solutions dans le Cloud qui permettent de faire de l'investigation judiciaire, de l'analyse prédictive et de gérer les ressources citoyennes pour les agences de sécurité publiques et gouvernementales. Cette acquisition va donner aux clients de Motorola Solutions des possibilités supplémentaires dans la gestion de données massives (vidéos, photos, réseaux sociaux, capteurs, etc.), en particulier dans l'anticipation des interventions de forces de police et dans la réponse aux incidents: mapping des faits criminels permettant un meilleur partage de l'information avec les citoyens, tableaux analytiques des données permettant de partager l'information avec d'autres juridictions, allocation préventive de ressources policières (patrouilles ciblées en particulier). C'est la deuxième acquisition en 2015, de Motorola Solutions, de fournisseurs de solutions logicielles tournées vers la sécurité publique. En février, la compagnie avait racheté Emergency CallWorks, le fournisseur d'une solution logicielle d'appel du 911 de nouvelle génération basée sur le web.

➔ DCNS a lancé la construction de la première corvette GOWIND 2500 de la Marine égyptienne

DCNS a procédé à la découpe de tôle de la toute première corvette GOWIND 2500 construite à Lorient, en présence de hauts représentants de la Marine égyptienne. Ce navire est le premier d'une série de quatre corvettes de dernière génération qui seront livrées à l'Egypte avant 2019. La première corvette GOWIND 2500 égyptienne sera réalisée au sein du site DCNS de Lorient, les trois unités suivantes seront construites à Alexandrie dans le cadre d'un transfert de technologie de construction. Depuis un an, DCNS a scellé des relations stratégiques avec l'Egypte, dans le cadre de la modernisation de la flotte de surface du pays, confortées par la vente d'une frégate multimissions FREMM en février 2015. DCNS avait déjà remporté un premier contrat pour la Marine royale malaisienne, qui porte sur la conception et la réalisation de six corvettes GOWIND 2500 en transfert de technologie, en Malaisie au sein du chantier Boustead Naval Shipyard.

➔ Deveryware contribue à l'avancement du projet ISAR+

Le projet européen ISAR+ porte sur la R&D de nouveaux usages des medias sociaux en gestion d'urgence et de crises (catastrophe naturelle, incident climatique…), avec communications mobiles entre autorités et citoyens. La dernière phase de test en grandeur réelle (pays) de ce projet européen s'est déroulée avec succès en février 2015 en Finlande et a mobilisé une équipe de Deveryware sur deux jours par moins 25 degrés! Trois scénarios ont été imaginés et simulés pour ce 3ème test: un train qui déraille, un crash d'avion et une tempête dans trois lieux différents. Spécialiste de la géolocalisation, Deveryware a fourni, aux autorités gérant la crise, des outils pour la détection des personnes en zone danger, dans le respect des autorisations de géolocalisation et de la protection des données personnelles, et du push vers les mobiles des citoyens en danger : alertes et informations émanant des institutions gérant la crise (Web-service myPublicAlerts). www.deveryware.com

Les marchés financiers

Le 7 mai, les citoyens britanniques éliront leur nouveau parlement. Les sondages ne permettent pas de dégager une tendance nette, le jeu habituel entre conservateurs et travaillistes étant troublé à droite par l'UKIP et à gauche par les indépendantistes écossais. Les milieux d'affaires peuvent s'inquiéter de l'issue du scrutin: une coalition autour d'Ed Miliband mènerait une politique fiscale peu «accommodante» et, de l'autre côté, David Cameron promet un référendum sur l'appartenance du Royaume-Uni à l'Union Européenne, dont le résultat aléatoire ferait peser un risque colossal sur la finance anglaise! Dans ces conditions, il est probable que les «bonnes» performances économiques du Royaume-Uni vont être analysées avec soin dans les prochains jours: si la croissance est robuste (2.9% en 2014, prévision de 2.7% en 2015), elle s'appuie essentiellement sur le développement d'une nouvelle bulle immobilière et sur l'activité de la City; la pression déflationniste est aussi forte que dans la Zone Euro; les déficits (budget et commerce) ne se contractent pas. Il serait étonnant que les marchés, complaisants ces derniers mois, restent passifs dans les prochaines semaines !

Les Leaders du secteur Security & Defense

Nom	Pays	Cours au 31/12/14	Cours au 03/04/15	Cours au 17/04/15	▲/▼	Depuis le 01/01/15
Rheinmetall	DE	36,27	45,4	46,93	▲	29%
Siemens	DE	93,75	100,85	100,95	▲	8%
ThyssenKrupp	DE	21,26	24,76	25,2	▲	19%
Airbus Group	FR	41,35	60,76	63,21	▲	53%
Alcatel-Lucent	FR	2,97	3,56	3,7	▲	25%
Atos	FR	66,3	64,48	68,34	▲	3%
Dassault Aviation	FR	1062,8	1110	1236,65	▲	16%
Safran	FR	51,25	65,95	67,96	▲	33%
Thales	FR	45	52,32	54,85	▲	22%
CNHI / ex Fiat Industrial	IT	6,7	7,66	8,07	▲	20%
Finmeccanica	IT	7,73	11,37	11,66	▲	51%
Hitachi Ltd	JP	900,7	831,4	794,1	▼	**-12%**
Mitsubishi Electric	JP	1446	1467,5	1518,5	▲	5%
Panasonic	JP	1427	1565,5	1557,5	▼	9%
Sony	JP	2472	3450	3555,5	▲	44%
Assa Abloy	SW	414,8	519	536	▲	29%
Axis AB	SW	199,6	339,9	339,6	▼	**70%**
Saab Group	SW	202,3	235,2	231,1	▼	14%

Nom	Pays	Cours au 31/12/14	Cours au 03/04/15	Cours au 17/04/15	▲/▼	Depuis le 01/01/15
Volvo Corp.	SW	84,7	100,9	99,85	▼	18%
Babcock Int Group	UK	1058	985,5	1043	▲	-1%
Bae Systems	UK	472	524,5	515	▼	9%
Qinetiq Group	UK	187,9	191,4	200,7	▲	7%
Ultra Electronics	UK	1800	1707	1717	▲	-5%
Boeing	US	129,98	149,28	151,97	▲	17%
Cisco Systems	US	27,81	27,13	28,6	▲	3%
Elbit Systems	US	60,73	74,22	79,12	▲	30%
General Dynamics	US	137,62	133,73	133,15	▼	-3%
Honeywell International	US	99,92	103,51	103,92	▲	4%
Kratos	US	5,02	5,58	5,89	▲	17%
L3 Communications	US	126,21	124,99	124,42	▼	-1%
LEIDOS / ex SAIC	US	43,52	42,16	42,01	▼	-3%
Lockheed Martin	US	192,57	198,72	197,12	▼	2%
Northrop Grumman	US	147,39	161,63	163,38	▲	11%
Raytheon	US	109,88	108,46	108,93	▲	-1%
Tyco International	US	43,86	43,33	43,31	▲	-1%
United Technologies	US	115	117,13	117,48	▲	2%

DE: Frankfurt, FR: Paris, IT: Milano, UK: London, SW: Stockholm, US: NYSE, JP: Tokyo

QINETIQ Group

Flottant: 595 170 000 actions soit 98,29 % du total des actions
Cours au 31/12/2014 : 187.90 GBP
Cours au 03/04/2015 : 191.40 GBP
Cours au 17/04/2015 : 200.70 GBP
Variation par rapport au 31/12/2014 : + 7 %
Dividende 2014 : 4,60 GBP soit un rendement de 2.45 %
Actualités : QinetiQ a fourni à Thales Alenia Space la technologie chargée de guider le retour vers la terre du démonstrateur de rentrée atmosphérique IXV, de l'Agence Spatiale Européenne, lancé avec succès le 11 février 2015 par un lanceur Vega. Qinetiq va fournir à la TSA américaine un système de détection des menaces, basé sur le scanner passif à ondes millimétriques, pour les centres de transport et les zones de concentration de population.

Infos utiles

➔Une publication bimensuelle
➔Rédacteur en chef : Alain Establier
➔Société Editrice : SDBR Conseil, SAS domiciliée
26 rue de la République 92150 Suresnes, France
520 236 662 RCS Nanterre
E-mail : admin@securitydefensebusinessreview.com
Web: **www.securitydefensebusinessreview.com**

➔Abonnements: +33 (0) 9 77 19 76 40
Abonnement annuel : 950 € HT (TVA 20%: 1140 € TTC)
Abonnement semestriel : 600 € HT (TVA 20% 720 € TTC)
ISSN 2107-7312

Prochain Numéro: Mardi 05 Mai 2015

4 questions à Evelyne Bourderioux

Vice-président Alliances chez Nware

➔ SDBR : Nware* est une jeune société française qui grossit vite, n'est-ce pas ?

EB : En effet, Nware a été créée en 2008, sur la base de l'expertise en infrastructure des systèmes d'information et sur la virtualisation, et compte aujourd'hui 72 collaborateurs. Deux rachats d'activités ont permis à Nware d'agréger des compétences, en particulier celui de NGM Security qui était spécialisée dans les problématiques de sécurité des entreprises dans le Cloud et faisait des audits, en partenariat avec Trend Micro dont les produits sont labellisés par l'Anssi. Ce rachat partait du principe qu'on ne peut sécuriser que les infrastructures que l'on connait bien, après les avoir auditées et en avoir tiré une stratégie de cyberdéfense. Nware n'a pas vocation à couvrir tous les aspects de la cybersécurité mais peut protéger le périmètre d'une manière efficace grâce aux outils que nous connaissons bien. Créée autour de l'idée forte «make IT simple», Nware est donc un intégrateur a valeur ajoutée des technologies de l'infrastructure, de l'intégration à la sécurisation, et un intégrateur des produits du groupement Hexatrust. Nware compte aujourd'hui plus de 200 clients ETI et Grands Comptes, dans des secteurs divers: Banque, Assurance, Industrie, Santé, Distribution. Présente à Paris, Lille et dans la région centre, Nware ouvrira en 2015 une agence à Lyon.

➔ Vous êtes en charge du concept de cyberdéfense propre à Nware. Comment se traduit-il ?

Tout d'abord par une importante veille technique et stratégique, autour des problématiques de sécurité, couplée à nos certifications pointues sur les dernières nouveautés en matière d'infrastructure: SDDC** (Software defined Storage, Software defined Network, etc.), hyperconvergence, gestion de la mobilité sécurisée. Cette approche se traduit aussi par un dialogue continu avec nos clients, pour cerner au plus près leurs besoins, complété par la consultation d'organismes comme le Cigref, l'Ordre des médecins ou l'Anssi, afin de s'inscrire dans un grand mouvement citoyen et fédérateur, et d'en intégrer toutes les connaissances. A partir de là, nous créons des solutions immédiatement opérationnelles, simples, efficaces et certifiées Anssi pour protéger les entreprises des menaces les plus fréquentes et les plus dangereuses. Notre objectif est d'implémenter le plus simplement possible les 40 principes d'hygiène informatique édictés par l'Anssi.

➔ Quels enseignements en matière de sécurité tirez-vous de vos observations ?

Il convient de couvrir les vecteurs d'attaques les plus fréquents et, malheureusement, ces vecteurs sont souvent des employés, d'anciens employés, des sous-traitants, des cocontractants ou des fournisseurs. C'est ce qui nous a amené à produire l'offre «NSecure 360» pour protéger les points les plus faibles de l'entreprise (l'administration, le web et la supervision), au premier rang desquels se trouvent les comptes à privilège. NSecure 360 comprend la solution AdminBastion de Wallix, pour tracer et contrôler les actions des administrateurs et des utilisateurs privilégiés, la solution rWeb de DenyAll, qui filtre les requêtes http/https et permet d'éviter les attaques de type injection SQL / injections de commande / cross-site scripting ou autres, et la solution Pom monitoring (Exosec) qui permet aux équipes d'exploitation du SI d'accélérer le diagnostic et de hiérarchiser les interventions, en fonction de la criticité du composant ou de l'application attaquée. Comme Nware, ces éditeurs sont français et présentent des solutions de confiance certifiées Anssi pour tous les aspects sécurité. Il faut souligner que NSecure 360 a été la première solution qui intègre et fédère des solutions produites par des membres du groupement Hexatrust pour couvrir un besoin métier spécifique.

➔ NSecure 360 est-elle la seule offre de Nware ?

Non bien sûr. Nous avons réfléchi à la manière de mettre l'hyperconvergence au service des besoins métiers des clients, en proposant des solutions qui intègrent les meilleurs produits du marché : DCIAM (Datacenter in a minute), un Datacenter à la demande et sécurisé, VDIAM (VDI in a minute) pour le passage progressif et sans risque à une infrastructure de bureau virtuel. Nous venons de finaliser une solution pour sécuriser les terminaux point de vente (péages, hôtels, restaurants, magasins), en partenariat avec Trend micro, pour contrecarrer les attaques qui se sont multipliées en 2014 (Target, Home Depot, UPS, Staples, HSBC Turquie, piratage des banques russes par Anunak) en détournant des TPV américains et européens. Enfin, nous sommes en préparation d'une offre sur les SCADA. De plus en plus, nous créerons des offres qui fédèrent les solutions Hexatrust.

Interview réalisée par Alain Establier

**Nware : www.nware.fr*
*** SDDC: Software Defined Data Center*