

# LA PROTECTION LA PLUS SOPHISTIQUÉE CONTRE LA CYBER-MENACE



François Lavaste

Toutes les organisations sont confrontées aujourd'hui aux cyber-attaques, qui sont de plus de plus sophistiquées, notamment avec l'arrivée des APT (Advanced Persistent Threat). Il s'agit d'attaques de haut niveau conçues à des fins d'espionnage et de sabotage. Pour les contrer, **Airbus Defence and Space** mise sur des investissements majeurs en R&D et l'émergence de solutions uniques et innovantes. Rencontre avec François Lavaste, dirigeant de l'entité CyberSecurity d'Airbus Defence and Space.

## Pouvez-vous nous présenter l'entité CyberSecurity ?

C'est au sein de l'entité CyberSecurity que Airbus Defence and Space a concentré l'ensemble de ses expertises en cybersécurité. Notre mission consiste à fournir des produits et des services professionnels de haut niveau dans le but de sécuriser les systèmes d'information des gouvernements, des entreprises, des infrastructures critiques ou encore des opérateurs d'importance vitale.

Notre objectif est d'offrir à nos clients une offre de bout en bout ciblée sur la lutte contre les APT, combinant protection périmétrique et cyber défense temps réel. Nous sommes d'ailleurs les seuls en Europe à proposer une offre discriminante, qui repose sur l'anticipation et sur la vitesse de réaction face aux ennemis. Avec 20 % de notre chiffre d'affaires annuel consacré à la recherche et au développement, nous proposons des solutions innovantes et adaptées aux évolutions les plus récentes du marché.

Aujourd'hui, nous comptons plus de 600 jeunes collaborateurs (nos experts ont entre 30 et 35 ans) répartis en France, Allemagne et Grande-Bretagne. Nous sommes également implantés au Moyen Orient depuis 2011.

## Qu'en est-il de l'évolution du marché mondial de la cybersécurité ?

Le marché mondial de la cybersécurité pèsera



86 milliards de dollars en 2016\*. Affichant une grande dynamique, ce marché a un taux de croissance compris entre 8 et 10 % avec des sous-segments qui évoluent à une vitesse supérieure à celle du marché lui-même (au-delà de 20 %).

## En tant que fournisseur de solutions et de produits de cybersécurité, qu'attendez-vous des décrets d'application de la Loi de Programmation Militaire (LPM) ?

Face à la sophistication grandissante de la menace, la LPM joue un rôle majeur de sensibilisation des décideurs à la cyber menace. En outre, le deuxième volet de cette loi oblige

aujourd'hui les opérateurs d'importance vitale à améliorer la sécurité de leur système d'information et à se doter de moyens de détection de cyber-attaques à partir de solutions et logiciels que l'ANSSI aura labellisée.

## Faut-il s'arrêter aux OIV ou étendre cette réglementation au reste des entreprises ?

Les grandes entreprises, même si elles ne sont pas toutes des opérateurs d'importance vitale, peuvent être vulnérables et faire l'objet d'une cyber-attaque visant à dérober des données stratégiques ou à paralyser leur outils de production ce qui pourrait avoir un impact écono-

## EN DÉPIT DE SA FORTE CROISSANCE, LE MARCHÉ DE LA CYBERSÉCURITÉ SOUFFRE D'UN MANQUE CRIANT DE RESSOURCES.

mique non-négligeable. Protéger ces entreprises est donc une nécessité.

Néanmoins une question demeure : est-ce à l'Etat de légiférer et étendre la réglementation aux grandes entreprises ou est-ce une prérogative du marché lui-même ?

A mon avis, la cybersécurité est un sujet sur lequel les organes de gouvernance des entreprises doivent se concentrer davantage. Traiter ce risque, au niveau des entreprises me semble, en effet, plus judicieux.

Cela dit, bien que la LPM ne concerne aujourd'hui que les opérateurs d'importance vitale, elle peut influencer les dirigeants des grandes entreprises à prendre les mesures nécessaires pour protéger leurs systèmes et leurs infrastructures.

### L'ANSSI veut favoriser le développement de technologies souveraines pour protéger les OIV (opérateurs d'importance vitale). Les technologies tricolores sont-elles au meilleur niveau mondial ?

Les technologies souveraines sont vérifiées, soumises à des tests de sécurité et validées par les autorités nationales (l'ANSSI). Elles correspondent aux critères de résilience et peuvent être déclarées produits de confiance.

Airbus Defence and Space propose la gamme de produits Stormshield développés par notre filiale Arkoon Netasq, permettant la sécurisation des réseaux informatiques (**Stormshield Network Security**), des postes de travail (**Stormshield Endpoint Security**) et des données (**Stormshield Data Security**).

Par ailleurs, il y a quelques mois, nous avons introduit une solution très novatrice conçue par les experts d'Airbus Defence and Space pour détecter des menaces avancées (APT), appelée **Keelback Net**. Il s'agit d'une sonde qui permet de collecter de façon continue et d'analyser rapidement les traces et comportements suspects présents sur le réseau d'une entreprise, en particulier des « signaux faibles », furtifs donc impossibles à repérer par les moyens de détection classiques. Unique en Europe, ce produit

répond à un très haut niveau de performance. Les cybercriminels ne cessent de diversifier leurs techniques et aujourd'hui, nous constatons qu'ils ont tendance à installer leur protocole d'attaque étape par étape. Il était, donc, nécessaire de développer un outil capable de contrer ce nouveau type de cyber-attaque.

### Pour conclure, un petit mot pour les étudiants de Polytechnique ?

La cybersécurité est une filière d'excellence française. Il s'agit encore d'un domaine très neuf, en cours de structuration. En dépit de sa forte croissance, le marché de la cybersécurité souffre d'un manque criant de ressources.

Je saisis, donc, cette occasion pour appeler les étudiants à s'intéresser davantage à ce domaine, qui en plus d'être à forte technicité, répond à un objectif majeur : la protection des biens communs et de la nation. ■



Keelback Net.



SN910, dernier de la gamme Stormshield Network Security.

\*Source Gartner Mai 2014.

### BIO EXPRESS

**François Lavaste** est diplômé de l'ESCP-Europe, une école de commerce européenne, et titulaire d'un MBA de la Harvard Business School. Il a débuté sa carrière dans l'informatique en 1992 en co-fondant Eneide, éditeur de logiciel de gestion de la relation client (racheté par Coheris en 2000).

Entre 1996 et 2006, François Lavaste s'établit dans la Silicon Valley où il rejoint Intuit, leader mondial des outils de gestion financière, Brightmail, pionnier de la sécurité de la messagerie (racheté en 2004 par Symantec), et enfin Mindjet, éditeur d'applications de mind mapping et d'innovation participative. En 2006, il prend la direction générale de la zone Europe, Moyen-Orient et Afrique de Tricipher, spécialiste de la sécurité des accès et de la gestion de l'authentification forte (racheté par VMWare).

Début 2007, il rejoint Netasq pour en prendre la direction. Après l'acquisition par Airbus Defence and Space de Netasq en 2012 puis de Arkoon en 2013, il devient Directeur de Arkoon Netasq. Il est depuis 2015 secrétaire général de l'Alliance pour la Confiance Numérique (ACN), et passionné d'entrepreneuriat, de technologie et d'innovation.

Il dirige, depuis août 2015, l'activité CyberSecurity à Airbus Defence and Space, entité 100 % dédiée aux problématiques de cybersécurité.