

Philippe Duluc, Bull : « Un intérêt marqué pour le smartphone sécurisé... merci Snowden »

Croisé dans les allées du FIC 2014 (Forum International de la Cybercriminalité, qui se tenait les 21 et 22 janvier à Lille), **Philippe Duluc**, directeur de la division sécurité de Bull, donne des détails sur l'accueil que reçoit le **Hoox m2**, le smartphone sécurisé de la société.



Basé sur un système Android révisé par les équipes de Bull Cybersécurité, la solution intègre une puce de chiffrement certifiée EAL4+, un capteur biométrique, un coffre-fort électronique et un système anti intrusion pour ces ports d'extension. Hoox embarque la technologie Cryptosmart d'Ercom pour le chiffrement de la voix et des messages. Le smartphone est annoncé au tarif de **2 000 euros pièce**.

Où en êtes-vous de la commercialisation de votre smartphone sécurisé Hoox, annoncé en octobre dernier ?

Philippe Duluc : La livraison des premiers équipements aura lieu à partir de février. Mais cette annonce en amont nous a amené de nombreux contacts. Les révélations d'Edward Snowden ont aussi évidemment renforcé notre stratégie. Depuis l'annonce en octobre, nous avons eu plusieurs centaines de discussions avec des prospects autour de Hoox. Et déjà vendu quelques versions de test. Si nous ne parvenions pas à signer plusieurs dizaines de contrats, y compris pour des tests, au cours du premier semestre, je serais déçu.

Nous pensions à l'origine que les premiers prospects pour le Hoox proviendraient du secteur public, mais, aujourd'hui, ce sont plutôt les acteurs du secteur privé qui manifestent l'intérêt le plus grand pour cette technologie, notamment les banques. Il s'agit souvent d'équiper des populations restreintes – des membres du comex, des commerciaux à l'export, des postes exposés lors de leurs déplacements. On parle de quelques dizaines de terminaux par organisation, distribués de façon permanente ou ponctuellement, en fonction de projets ou d'activités précises.

Quelles garanties offrez-vous en matière de sécurité ?

Le Hoox se situe clairement entre des applications de sécurisation des téléphones du commerce, en pratique assez limitées, et des solutions développées par l'Etat pour le secret-défense et le confidentiel-défense (référence au Theorem de Thales, NDLR). Notre objectif était d'assurer une

sécurité native. Pour ce faire, nous avons étudié et redesigné une souche d'Android, sur la base d'une méthode d'analyse de risques. Tous les aspects ont été étudiés : interceptions, piégeage du terminal, écoutes radio ou via les apps. Nous avons ensuite modifié les couches hautes et basses de l'OS pour réduire ces risques. La solution comprend des éléments de sécurisation sur le terminal ainsi qu'une passerelle de cryptographie implantée dans le SI des clients. Notre objectif est désormais d'obtenir l'agrément de l'ANSSI pour l'utilisation en diffusion restreinte (le niveau en-dessous du confidentiel-défense, NDLR).

Comment assurez-vous la sécurité au niveau matériel ?

Nous travaillons avec des sous-traitants produisant des sous-ensembles électroniques que nous intégrons. Mais ces entreprises nous fournissent un matériel nu ; nous assurons nous-mêmes l'implémentation du logiciel. Bien sûr, ce serait insuffisant pour du secret-défense où il faut maîtriser toute la chaîne, mais Hoox est le fruit d'un compromis entre les exigences de sécurité maximale et le prix. Par ailleurs, aucun de nos pentesters (personne chargée des tests d'intrusion, NDLR) n'a pour l'instant réussi à prendre en défaut la solution.

Bull vient de présenter son plan stratégique pour la période 2015-2017. Quelle place y occupe la sécurité ?

La cybersécurité est confirmée comme étant une priorité du groupe. La division en charge de ces sujets propose tant des services que des produits, comme le Hoox évidemment, mais également un périphérique de stockage sécurisé (le Globull, agréé confidentiel-défense) et des appliances de chiffrement. Nous sommes le seul fournisseur français sur ce créneau.

A la lumière des révélations d'Edward Snowden, être un fournisseur national peut être un atout pour les marchés hexagonaux. Mais également un frein à l'export. Le Forum économique mondial a fait état de ses craintes de voir l'Internet se balkaniser. Qu'en pensez-vous ?

Je suis d'accord pour dire que nous allons assister à une certaine forme de balkanisation. Mais, à l'intérieur de l'Europe, nous avons un destin commun qui éloigne ce spectre. C'est particulièrement vrai entre l'Allemagne et la France.

En complément : nos autres articles sur le FIC 2014

- [De l'Anssi à la DGSE : Patrick Pailloux, de la lumière à l'ombre](#)
- [La France met 1 milliard d'euros de mieux sur l'arme cyberdéfense](#)
- [Forum International de la Cybersécurité : la sécu au temps de Snowden](#)
- [Luc-François Salvador, Pdg de Sogeti : « la cybersécurité, une activité qui croît de 30 % par an »](#)