CYBERSÉCURITÉ

ERCOM : L'ASSURANCE SÉCURITÉ DE VOS ÉCHANGES EN TOUTE SIMPLICITÉ

Yannick Dupuch

Acteur français de référence dans la cybersécurité, **Ercom** accompagne durablement la transformation de ses clients en leur fournissant des solutions sécurisées et évolutives, innovantes et robustes pour protéger leurs communications. Éclairage avec Yannick Dupuch, président de la société Ercom.

Votre société existe depuis 30 ans. Depuis quand développez-vous vos activités de cybersécurité ?

Ercom a commencé par des activités de conseil dans la cybersécurité. Au tournant des années 2000, elle a développé ses premiers produits, avec en particulier le téléphone sécurisé de l'avion présidentiel en 2002, puis les premières versions de Cryptosmart, une solution de sécurisation des terminaux et des communications mobiles déployée notamment auprès de l'Elysée, de Ministères et de clients Grands Comptes, en France et à l'Internationale.

En dix ans, votre activité s'est multipliée. Que furent vos principales innovations ?

Nous avons depuis développé Cryptobox, la solution de travail collaboratif la plus sécurisée du marché, dont nous avons lancé la commercialisation l'été dernier. Aujourd'hui, nous travaillons à rendre nos produits toujours plus intelligents grâce à l'analytique et au machine learning. Nous sommes aidés par des équipes de data scientists, mathématiciens, architectes big data..., bref par des passionnés de nouvelles technologies et de souveraineté numérique (dont quelques polytechniciens bien sûr).

Vos solutions s'intéressent aux téléphones portables. Par quelle méthode les sécurisez-vous ?

Ercom a développé des expertises sur les technologies de chiffrement de bout en bout[1] que nous avons adaptées pour sécuriser les terminaux et les communications mobiles, en particulier sur les OS Android, plus facilement accessibles qu'iOS d'Apple. Nous devons aussi notre succès à notre carte à puce (format micro-SD développée avec Oberthur) qui permet une sécurisation forte des clés de chiffrement.

Pour développer vos technologies, avez-vous noué des partenariats ?

Nous collaborons avec plusieurs partenaires, notamment avec Samsung pour intégrer nativement Cryptosmart dans leurs terminaux.

Vos agréments présentent-ils un avantage ?

Nos technologies sont régulièrement auditées par des organismes tiers indépendants, et agréés par l'ANSSI, l'OTAN et l'Union Européenne. Ce fut le cas par exemple pour Cryptosmart (agrément au niveau Diffusion Restreinte pour les experts). Ce type d'agrément est important pour nos clients et nous distingue des autres acteurs de solutions de sécurité. Il nécessite un investissement conséquent en ressources, en moyens financiers et humains : il faut environ un an si tout se passe bien pour l'obtenir.

Êtes-vous en mesure aujourd'hui de sécuriser les conversations, les SMS et les datas ?

Cryptosmart permet de sécuriser le terminal ainsi que toutes les communications (voix, data, SMS). Cette solution est déployée sur des terminaux grand public Samsung, les best-sellers actuels de la marque que sont les Galaxy A5, S7, S7 EDGE et Tab S2 VE.

Est-ce simple d'utilisation ?

Vous mettez le doigt sur un facteur de succès extrêmement important dans notre domaine : combiner sécurité et simplicité. Pour simplifier la customer experience (expérience des consommateurs), nous déployons des démarches d'analyse et d'amélioration en amont et en aval de la conception de nos produits, au travers de groupes d'utilisateurs.

Fonctionnez-vous avec tous les opérateurs et fabricants de mobiles dans le monde ?

Pour un éditeur comme nous, l'idéal est d'être compatible avec tous les réseaux mobiles, ce qui est le cas puisque nos solutions peuvent être utilisées sur tous types de réseaux : GPRS, EDGE, 3G, 4G et demain 5G, ainsi que les réseaux WiFi et satellites.

Pour les fabricants, au-delà de Samsung, nous aimerions pouvoir travailler avec tout le monde, et en particulier avec Apple. Mais l'Américain reste encore trop fermé à nos propositions. Si vos lecteurs travaillent chez Apple et peuvent nous y aider, nous sommes preneurs ! Pour remédier à cela, nous travaillons d'ailleurs sur une déclinaison de Cryptosmart qui sera portée sur tous types de terminaux et OS : vos lecteurs en entendront parler très vite...

Vos solutions fonctionnent-elles si l'un des interlocuteurs n'en est pas équipé ?

Il arrive que deux interlocuteurs souhaitant communiquer ne soient pas équipés tous les deux. Dans ce cas, Cryptosmart fonctionne quand même ! Elle sécurise les informations depuis le terminal équipé de la solution jusqu'à la passerelle installée dans l'entreprise cliente. La communication passe ensuite en clair jusqu'à l'interlocuteur qui n'en est pas équipé. Cela permet en particulier de sécuriser des communications passées depuis l'étranger où les risques d'écoute à des fins d'intelligence économique sont plus élevés.

Votre solution protège-t-elle aujourd'hui toutes vos données en cas de perte ou d'intrusion ?

Cryptosmart embarque une solution d'authentification forte, du même niveau qu'une carte bancaire, au travers de la carte micro-SD. En cas de perte ou de vol du terminal, notre solution permet à l'administrateur au sein de l'organisation cliente de bloquer l'accès aux informations du terminal, voire d'effacer les données qu'il contient.

Quelle solution proposez-vous pour échanger des documents et faciliter le travail collaboratif ? Propose-t-elle un chiffrement des données ?

En utilisant nos expertises sur le chiffrement de bout en bout, nous venons de lancer Cryptobox, la solution de travail collaboratif la plus sécurisée. Nous sommes partis d'un constat simple pour créer ce produit : les entreprises, pour innover ou pour accéder à de nouveaux marchés, ont besoin de collaborer, en interne ou en externe… Il leur faut donc échanger des informations sensibles, en toute confidentialité.

En stockant des données, le cloud ne présente-t-il pas un danger ?

Le cloud constitue un point névralgique, cible de nombreux hackers qui cherchent à récupérer les informations qui y sont stockées. Les attaques y sont de plus en plus nombreuses (+38 % selon PwC et tout particulièrement en France (+51 % en 2015 vs. 2014). Cryptobox répond aussi à cet enjeu : sécuriser les échanges de données sur n'importe quel cloud, sans que le fournisseur n'ait accès aux données.

Vos données sont-elles accessibles depuis votre ordinateur, votre smartphone ? Est-ce facile d'utilisation ?

Là encore, nous avons cherché à combiner sécurité et simplicité : Cryptobox est donc accessible depuis n'importe quel terminal (smartphones et tablettes Android et IoS, ou encore ordinateurs sous Windows). Elle est même la première solution à chiffrer les données depuis le navigateur installé sur votre ordinateur, sans que le client n'ait besoin d'installer une application. Là encore, l'expérience utilisateur fait l'objet de toute notre attention dans le développement du produit.

Cette solution fonctionne-t-elle sur tous les serveurs ? Sur Cloud ?

Une des spécificités de Cryptobox, c'est sa flexibilité : la solution peut être déployée de façon extrêmement simple, moins d'une journée, sur les serveurs de l'entreprise, dans un cloud, ou en mode hybride. Grâce à Cryptobox, les clients peuvent bénéficier de tous les avantages du nuage, sans les inconvénients : les informations que les clients y stockeront sont en effet totalement chiffrées, et l'hébergeur n'a pas accès aux clés de déchiffrement.

Quelles sont vos ambitions ? Quels sont vos axes de recherche ?

La sécurité de l'information est devenue un enjeu majeur pour les entreprises et les Institutions. Mais l'information, souvent qualifiée à tort ou à raison de nouveau pétrole des entreprises, doit pouvoir être exploitée. L'exploitation de la donnée chiffrée dans le cloud est donc notre prochain challenge ! ■

1. Les clés de déchiffrement sont exclusivement maîtrisées par les utilisateurs.

ERCOM

CONTACT
Raphaël BASSET • Directeur Marketing
T. +33 1 39 46 50 50 • raphael.basset@ercom.fr
www.ercom.com