«Eurosmart continuera de jouer un rôle pionnier et moteur dans les domaines de la normalisation, l'interopérabilité et le déploiement des applications numériques sécurisées en Europe»

Entretien avec Didier Sérodon, nouveau président d'Eurosmart

POSTÉ LE 12.13.16

Didier Sérodon, SVP Strategic Project / Continuous Improvement de Safran Identity & Security, vient d'être nommé président d'Eurosmart, l'association internationale à but non lucratif représentant l'industrie de la Smart Security (technologie basée sur la carte à puce et ayant migré vers les objets portables sécurisés) pour les applications multi-secteurs.

En tant que président fraîchement élu, quelle sera votre première priorité dans votre nouveau rôle de «voix de l'industrie de la Smart Security», comme est appelée Eurosmart?

D.S.: Eurosmart continuera à rester à la pointe des évolutions du marché et des défis commerciaux tels que l'Internet des Objets (IdO), etc. – en jouant un rôle pionnier et moteur dans les domaines de la normalisation, de l'interopérabilité et du déploiement d'applications numériques sécurisées dans toute l'Europe. Plusieurs réglementations européennes mises en oeuvre à grande échelle sont basées sur l'expertise d'Eurosmart. Nous devons faire en sorte qu'Eurosmart poursuive sur cette voie, mais aussi nous ouvrir à tous ces nouveaux marchés où la sécurité est essentielle, mais qui n'ont peu ou pas d'expérience dans le domaine de la gestion de la sécurité.

Je peux vous donner l'exemple des réseaux Wi-Fi qui sont compromis parce que la sécurité des ampoules connectées n'a pas été correctement appréhendée.

L'Internet des Objets illustre bien ces nouveaux marchés que vous venez de mentionner. Avec lui, ce sont de nouvelles activités et de nouvelles applications qui entrent en jeu. Quelle est l'approche d'Eurosmart?

D.S.: L'IdO est effectivement un sujet très intéressant, non seulement en raison de la taille du marché et de sa croissance, mais aussi parce que les nouveaux acteurs sont exposés à des risques de sécurité qu'ils ne savent pas comment aborder.

Il y a quelques semaines d'ici, une attaque de grande ampleur a été menée sur un site web à l'aide de caméras connectées. Les fabricants de caméras ignoraient complètement que leurs appareils pouvaient être exploités de la sorte, et n'avaient donc même pas pensé à les protéger. Chez Eurosmart, nous avons une connaissance pointue du marché de la sécurité, et nous essayons de la partager. Nous avons défini une stratégie en trois étapes.

1. Soumettre un simple questionnaire d'évaluation de la sécurité: si je ne suis pas un expert dans le domaine de la sécurité, comment est-ce que je peux comprendre les risques contre lesquels mon appareil devra

- être protégé?

2. Ensuite, proposer une gamme de solutions sécurisées en fonction des risques déterminés sur la base de la question suivante: que dois-je sécuriser, et comment?
3. Enfin, collaborer étroitement avec la Commission européenne pour mettre en oeuvre des labels de confiance faciles à comprendre pour les utilisateurs finaux.

Quels sont les autres projets de l'organisation à l'heure actuelle?

D.S.: Nous avons beaucoup de projets en tête, notamment l'organisation d'un événement au Parlement européen sur l'impact de la cybersécurité sur le confort d'utilisation. Dans le cadre de sa Stratégie pour le marché unique numérique, la Commission européenne réexaminera la directive «Vie privée et communications électroniques» de 2002 afin d'en assurer la cohérence avec le Règlement général sur la protection des données, de garantir des conditions de concurrence équitables pour tous les acteurs du marché (opérateurs de télécommunications vs opérateurs OTT) et de protéger le droit des utilisateurs à la vie privée.

Les décideurs européens devraient particulièrement s'attacher à évaluer si le niveau de sécurité actuel des services de communication électronique (notamment en ce qui concerne la protection des données personnelles stockées dans des terminaux tels que les smartphones) doit être amélioré, compte tenu de l'adoption d'une nouvelle législation imposant des exigences en matière de sécurité (Règlement général sur la protection des données, Directive sur la sécurité des réseaux et de l'information, etc.), de la publication de rapports consacrés à la surveillance de masse électronique (rapport Moraes) et des événements récents liés à l'infection de smartphones par des virus et autres programmes malveillants. L'Union européenne devra donc trouver un compromis entre différents besoins concurrents, par exemple en ce qui concerne l'impact du renforcement du niveau de sécurité sur le confort d'utilisation. Les décideurs européens restent également très attentifs à ce dilemme lorsqu'ils traitent de la cybersécurité dans d'autres politiques sectorielles de l'Union européenne, notamment en ce qui concerne la migration et les affaires intérieures (sécurité des documents d'identification), la directive sur les services de paiement (PSD2) et l'eGovernment (plan d'action relatif à l'administration en ligne 2016-2020).

Didier, pouvez-vous revenir en quelques mots sur votre expérience et votre carrière?

D.S.: Je vais tâcher d'être bref et de résumer mes 25 années d'expérience dans ce secteur en quelques lignes. J'ai suivi une formation d'ingénieur et ai décroché plus récemment un Master en Marketing international. J'ai débuté dans le secteur des cartes à puce en 1992 chez Philips Smart Cards and Systems, qui a ensuite été racheté par Oberthur. J'y ai occupé plusieurs fonctions: ingénieur préventes, commercialisation de produits, direction d'équipes de projet, développement de logiciels, responsable d'unité opérationnelle, ou encore responsable de la communication d'entreprise. J'ai ensuite travaillé dans une petite société de logiciels qui proposait des équipements de test pour les cartes à puce et des systèmes d'exploitation de cartes à puce, puis chez un grand fournisseur de terminaux PDV avant de rejoindre Safran Identity & Security.