L'INFORMATICIEN
Pays : France
Périodicité : Mensuel

Date : FEV 17
Page de l'article : p.42

SÉCURITÉ

L'EUROPE SUR LE CHEMIN DE L'HARMONISATION

La sécurité tient une place fondamentale dans la notion de souveraineté. Et, à ce niveau, les initiatives se multiplient, notamment au plan européen. Actuellement, l'absence de référentiel commun et uniforme est pourtant criant, malgré quelques initiatives. À la mi-décembre 2016, l'Anssi (Agence nationale de la sécurité des systèmes d'information) dévoilait toutefois son label SecNumCloud, grand frère de Secure Cloud qui avait vu le jour en 2014. Il s'inspire largement de la norme ISO 27001 en y ajoutant des spécificités techniques.

Parallèlement, de l'autre côté du Rhin, l'Office fédéral de la sécurité des technologies de l'information (BSI) a fait de même en présentant son catalogue « C5 », pour *Cloud Computing Compliance Controls Catalog*. Enfin, quelques jours à peine après la présentation de ces référentiels, les deux pays annonçaient l'European Secure Cloud (ESCloud), un référentiel à vocation européenne cette fois-ci. En décembre, le directeur de l'Anssi Guillaume Poupard nous expliquait alors que les Allemands ont eu la même démarche que la nôtre, *« mais pas dans la forme »*, glissait-il. Si bien qu'il faut comprendre que, si un prestataire est labélisé SecNumCloud ou C5, il le sera également automatiquement sur ESCloud. Pas franchement d'une grande clarté…

Ce qui est intéressant ici est plutôt dans l'analyse de l'approche sécuritaire menée par le couple franco-allemand, et sa capacité à devenir un moteur. Guillaume Poupard l'assume d'ailleurs et ne s'en cache pas. *« C'est une main tendue vers l'Europe »*, assure-t-il. Effectivement, les autres pays sont ainsi encouragés à créer leurs propres référentiels et/ou de se conformer directement à ESCloud. En revanche, certains s'agacent de la prolifération de nouvelles normes. *« Bien entendu il faut une norme pour protéger ne serait-ce que les données personnelles. Personne ne souhaite que les données d'une mairie avec des informations, comme celles des enfants, fuitent. Le véritable enjeu c'est arriver à un niveau de sécurité avec du bon sens »*, commente Jules-Henri Gavetti, PDG d'Ikoula. *« Il faut arrêter avec le lobbysme des grands donneurs d'ordre, Atos, Capgemini et consorts. Ce n'est pas vivable pour un grand nombre de start-up, ni même d'administrations. On met des normes partout, qui peuvent être autant de freins là où les Américains ou les Chinois s'en passent allégrement »*, poursuit-il.

L'axe Paris-Berlin

Outre l'Anssi et le BSI, qui marchent presque main dans la main, le couple franco-allemand prend de plus en plus de mesures communes au sujet du numérique dans son ensemble. À la mi-décembre 2016, François Hollande et Angela Merkel annonçaient la création d'un fonds doté de 1 milliard d'euros destiné au financement des start-up et à l'élaboration de standards communs. La chancelière a insisté sur la nécessité de s'armer de manière commune contre la cybercriminalité, alors que le président français rappelait le partenariat entre le moteur de recherche tricolore Qwant et le fournisseur de messagerie allemand Open-Xchange.

Tanker.io : la protection par le chiffrement des apps

Encore très discrète, la start-up française Tanker.io vient se mêler au débat autour des questions de souveraineté avec une approche intéressante : peu importe où se trouve la donnée, l'aspect fondamental étant de (re)donner la maîtrise de l'information aux entreprises. Et ce, grâce au chiffrement ! Pour le moment, la solution fonctionne uniquement avec Dropbox et OneDrive de Microsoft. Le constat étant que ces solutions sont largement installées et très utilisées, et qu'il est donc très difficile de faire changer les utilisateurs. Peu importe ! La solution est une couche de chiffrement sur les applications et sur tout le trafic avant qu'il ne soit envoyé vers les serveurs distants des éditeurs. Pour les utilisateurs finaux rien ne change. Quant aux administrateurs, ils peuvent contrôler eux-mêmes les clés en interne. *« Les équipes peuvent désormais travailler avec leurs solutions favorites les plus productives, aussi bien en interne qu'avec leurs interlocuteurs externes, sans compromettre la sécurité des données de leurs entreprises »*, souligne pour Guillaume Pontallier, co-fondateur de Tanker.io. Quant au chiffrement en lui-même, il s'effectue en local, en AES 256 bits, et de bout en bout grâce aux API fournies par les éditeurs concernés. Ce faisant, ni l'hébergeur ni Tanker n'a de possibilité d'accès à la donnée. La start-up se veut donc comme une alternative à l'idée même de souveraineté, et sa solution est actuellement en cours de certification et qualification par l'Anssi.