Cybersécurité : l'UE débloque 450 M€ pour doper l'industrie européenne

L'Europe met 450 millions d'euros sur la table pour doper l'industrie de la cybersécurité européenne. Ce partenariat public-privé (PPP), qui s'inscrit dans le cadre du programme de recherche Horizon 2020, vise à stimuler la coopération entre la sphère publique et les industriels, afin de développer des solutions *« applicables à différents secteurs, tels que l'énergie, la santé, les transports et la finance »*, explique l'UE.

La Commission européenne a signé aujourd'hui ce partenariat avec les industriels européens regroupés au sein de l'ECSO (European Cyber Security Organisation), un lobby bruxellois tout juste créé qui compte parmi ses membres une autre organisation d'industriels européens de la sécurité (EOS), une association française (Alliance pour la Confiance Numérique, membre de la FIEEC et comptant dans ses rangs Orange, Airbus, Thales, Bull, Gemalto, Safran, le CEA et l'Inria), son homologue allemande, Teletrust, mais aussi la très officielle Agence nationale pour la sécurité des systèmes d'information (Anssi).

> *L'ANSSI sera l'un des membres fondateurs de l'association ?? @ecso_eu et du cPPP cyberhttps://t.co/BTGPxgHpBLhttps://t.co/krq3zWAU93*
>
> *— ANSSI (@ANSSI_FR) July 5, 2016*

La commission européenne assure que le partenariat, signé par son commissaire pour l'économie et la société numérique Günther Oettinger (à droite sur la photo ci-dessus), devrait déboucher sur des **investissements du secteur privé trois fois supérieurs à sa mise de départ**. Soit 1,8 milliard d'euros à l'horizon 2020. Les premiers appels à proposition doivent être publiés au premier trimestre 2017. La commission voit également ce PPP comme « *une plateforme hébergeant les discussions entre l'offre et la demande en matière de produits et solutions de cybersécurité* ».

Certification unique pour 27 pays

Par ailleurs, la Commission manifeste son intention de mettre en place une certification unique à l'échelle de l'Europe. En effet, pour accéder à certains marchés sensibles, les fournisseurs doivent aujourd'hui faire auditer leurs solutions par une agence gouvernementale. Un processus parfois long et coûteux, mais qui se limite pour l'essentiel à un pays. En France, par exemple, dans le cadre de la législation sur les OIV (Opérateurs d'importance vitale), l'Anssi entend qualifier prestataires et solutions. Le dispositif est aujourd'hui encore largement embryonnaire (seule une liste de prestataires d'audit dument qualifiés a été publiée), mais s'étendra demain aux sondes de détection d'intrusion et même aux Cloud.

Même si l'Anssi a précisé que certaines qualifications obtenues dans l'Hexagone seront aussi valables en Allemagne (et vice-versa), l'idée de la Commission est de travailler à un processus de certification à l'échelle de l'Europe des 27. Le futur rôle de l'Enisa (l'agence européenne chargée de la sécurité des réseaux et de l'information) ? Difficile de l'affirmer, mais la Commission indique que les missions de l'agence vont être réévaluées dans les mois qui viennent.

NIS : plus de coopération européenne

Ce plan s'inscrit évidemment dans le cadre de la stratégie pour un marché unique numérique – la Commission voyant dans les certifications effectuées pays par pays un « *risque de fragmentation* » de l'Europe -, mais également dans la perspective de la **directive NIS** (Network and Information Security). Ce projet, qui doit être **voté tout prochainement au Parlement** européen pour entrer en vigueur dès le mois d'août, imposera des règles de sécurité à des entreprises assurant des services vitaux ainsi qu'aux prestataires de services numériques. Les sociétés concernées auront aussi pour obligation de communiquer les incidents de sécurité les plus graves à des organisations spécialisées dans la réponse aux incidents, que chaque pays membre devra mettre en place. Le

projet prévoit aussi de renforcer la coopération entre états membres sur ce sujet.

En résumé, l'approche de NIS ressemble à s'y méprendre à la règlementation sur les OIV que la France met peu à peu en place. Même si Guillaume Poupard, le directeur général de l'Anssi, y voit un texte complémentaire, permettant d'élargir la mise en place de règles de sécurité à un second cercle d'entreprises, plus large que les quelque 250 OIV français.

Notons d'ailleurs que la sortie annoncée de la Grande-Bretagne pourrait faciliter les discussions entre pays membres de l'Union. La participation du GCHQ (Government Communications Headquarters) britannique à plusieurs opérations de piratage orchestrées par la NSA américaine contre des intérêts européens (citons les cas de Belgacom ou du Français Gemalto) ne facilitant guère le partage d'informations entre nations européennes sur les menaces et la sécurité de leurs infrastructures vitales. Contrairement à l'Anssi française, le GCHQ est à la fois chargé de la défense des intérêts britanniques et de missions de renseignement électronique.

A lire aussi :

La sécurité des OIV mise au pas par l'Etat… petit à petit

L'Etat français va certifier les Cloud de confiance