Sélection mensuelle d'un sujet affectant la sûreté des entreprises
Mois de juillet 2014
Les cyberattaques : l'organisation des pôles défensifs et la mutualisation des savoirs.

Une tendance se dessine dans l'organisation de la protection contre les cyberattaques. Des pôles défensifs souvent spécifiques à un domaine d'activité voient le jour en partenariat entre la voie universitaire (recherche et formation), les pouvoirs publics essentiellement sur un plan régional, et les PME.

Les PME dans la cybercriminalité

Les PME sont un élément clef de cette défense. Leur insuffisance de protection en fait des cibles privilégiées alors qu'elles sont au cœur des processus industriels dans la chaîne qui les relient à leurs donneurs d'ordre.

Il importe donc pour une PME de ne pas rester isolée dans la lutte contre les cyberattaques mais de se rapprocher des conseils de région, des préfets, des universités et éventuellement, selon le domaine d'activité, de s'intégrer dans l'un des pôles de mutualisation qui se développent actuellement. Le lien avec la concurrence n'est pas à exclure dans ce type de lutte. Au contraire, confrontée aux mêmes structures d'attaque et de données à protéger, la mutualisation avec des entreprises du même secteur ou d'un secteur lié est plutôt recommandée.

De fait, en juillet 2012, un développeur, parvenu à pirater un modèle de serrure fabriqué par la société Onity, un des poids lourds du secteur, et fournisseur notamment de chaînes hôtelières, faisait part de l'opportunité pour les entreprises du secteur de faire de la sécurité informatique un axe prioritaire de la stratégie d'entreprise. Ce modèle de serrure étant en effet disposé sur des millions de portes de chambres d'hôtel à travers le monde. En juillet 2014, les constructeurs automobiles ont commencé à s'organiser. Dans la mesure où les véhicules connectés représenteront, selon une étude du cabinet Rolland Berger, 67% des ventes mondiales en 2018, certains constructeurs se sont regroupés autour d'un organisme de recherche, Batelle Cyber Innovation, pour trouver une approche globale et dynamique à la sécurité des objets connectés. L'idée d'étendre cette collaboration aux fabricants de téléphone, fait également son chemin, dans la mesure où les téléphones mobiles et GPS peuvent devenir de véritables chevaux de Troie concernant la sécurité des systèmes connectés.

La prise de conscience des pouvoirs publics

Cette tendance est la conséquence directe de la prise de conscience par les pouvoirs publics de l'ampleur de la menace concrétisée par le lancement du « Pacte Défense Cyber 2014-2016 » par le ministre de la Défense, Jean-Yves Le Drian. La cyber défense a également été érigée au rang des priorités de la loi de programmation militaire 2014-2019 face à l'explosion des attaques contre les systèmes d'information civils et militaires vitaux pour le pays.

En pratique, le pacte comprend six axes et une cinquantaine d'actions. L'axe VI notamment avec l'action 46 vise à « *contribuer à fédérer dans le cadre régional des grandes implantations de la défense tous les acteurs publics ou privées en lien avec le ministère* ». Il s'agit de « *fédérer les énergies, mutualiser les capacités et permettre une fertilisation croisée entre experts, enseignants et opérationnels, militaires comme civils, du publics comme du privé* ». Les domaines d'activités sont par ailleurs précisés dans l'action 46 notamment les zones de Toulon et Brest pour la marine, Lille pour les forces terrestres et la région Bordeaux/Toulouse pour le domaine aérospatial.

Dans ce cadre, un projet a vu le jour à Toulouse en mai 2014. Une quinzaine d'acteurs ont pris part à un programme, baptisé Albatros, dédié à la lutte contre la cybercriminalité dans le domaine de l'aéronautique. Steria, une entreprise leader des services numériques et notamment dans la protection des données techniques et commerciales y participe, de même que l'Université Toulouse Capitole et la société Airbus. L'un des axes du programme est dédié aux PME sous l'appellation Box@PME. Une centaine d'experts travaillent ainsi au service d'une quarantaine d'entreprises pour une mise en commun des savoirs faire de l'industrie, de la recherche et de la formation, dans le but de faire émerger une filière cybersécurité spécifique en Aéronautique et Spatiale. Le projet se divise ainsi en trois entités : box@PME qui réunit Airbus à quatre PMI et ETI (Entreprises de taille intermédiaire) de sa chaîne de production, une entité de veille fédérant plusieurs laboratoires de recherches, une entité travaillant à l'émergence de l'offre de formation dans ce domaine. Deux diplômes universitaires sont ainsi en train de voir le jour à Toulouse : l'un à L'IRIS pour la rentrée 2014 et l'autre au sein de Toulouse-Capitole 1 qui ouvrira en 2015.

En juin 2014, Bernard Cazeneuve, ministre de l'Intérieur, a poursuivi cette ligne directrice en confirmant la nomination d'un cyber préfet en charge des questions de sécurité informatique. Sur le terrain, une note adressée aux préfets de région dès 2013 avait rappelé l'importance de développer des liens forts avec le monde de l'entreprise. A l'instar du programme Albatros et de son leitmotiv, l'objectif est de « *coopérer pour mieux résister* ».

La CCI du Tarn a organisé en juillet 2014 dans cette même démarche des tables rondes avec la communauté d'agglomération de l'Albigeoise et la Technopole Albinnoprod afin d'accompagner les PME sur la prévention et la lutte contre les cyberattaques.

De même la région Bretagne et l'Institut national de recherche en informatique et automatique (INRIA) viennent de signer en juillet 2014 une convention pour développer la recherche et la formation dans le domaine de la cybersécurité. Cette convention vient concrétiser le développement du pôle d'excellence cyber en Bretagne, un des axes également du Pacte Cyber Défense.

.