Economie | Entreprises et cybersécurité : « prévenir plutôt que guérir »

Dans le courant de ce mois de mars, une PME d'Orthez a été victime d'une cyber-attaque. Ses données commerciales, financières et comptables ont été cryptées, et une rançon pour leur décryptage a été demandée. Rançon, espionnage, sabotage, le phénomène, déjà bien connu et régulièrement médiatisé en 2017 pour les grandes entreprises voire ministères et services d'Etats, frappe désormais aussi de plus en plus les petites entreprises. C'est bien dans le but de sensibiliser ces acteurs et de créer chez eux une culture commune de ce risque d'un nouveau genre, que la CCI Pau Béarn organisait ce mercredi 21 mars, en partenariat avec CCI France, les Rencontres de la Cybersécurité de Pau. 250 à 300 personnes y ont participé.

Si, comme l'a rappelé Didier Laporte, le Président de la CCI Pau Béarn, la chambre consulaire travaille depuis 3 ans déjà sur les questions de cybersécurité, à travers un service de veille, de sensibilisation, d'accompagnement et de formation des entreprises à cette question, il n'empêche que « la numérisation de l'économie, nous expose, nous entreprises, un peu plus chaque jour au revers de la médaille, que sont les dangers du numérique ». Un revers qui selon les convictions des différents intervenants n'épargne personne, ni les grosses entreprises, ni les individus ni les PME, ni la défense ou la sécurité nationale.... Nicolas Patriarche, Vice-Président de la Communauté d'Agglomération Pau Béarn Pyrénées, et maire de Lons (13000 habitants), témoignant pour sa part que sa collectivité avait déjà été attaquée 3 fois, dont une fois, la première, avait donné lieu à un versement de rançon.

"Ne pas parier sur les compétences techniques des pirates"

Une rançon que les professionnels de la sécurité présents, dont notamment, le Colonel Christophe Vercellonne, commandant du groupement de gendarmerie départementale des Pyrénées-Atlantiques, déconseille fortement : « d'une part la rançon participe à l'ambiance mafieuse du système et d'autre part, la récupération effective des données est très faible, car déchiffrer un disque dur de façon discrète est bien plus difficile que de le crypter... » En d'autres termes, « il ne faut pas parier sur les compétences techniques du pirate », synthétise également, Guillaume Poupard, Directeur général de l'Agence Nationale de la Sécurité des Système de l'Information (ANSSI) via une intervention vidéo. Sur le caractère généralisée des attaques, ou tentatives d'attaques, une étude

Microsoft, estimait que 81% des entreprises françaises ont été visées par une cyberattaque en 2015... et le phénomène ne fait que croître, n'ont cessé d'alarmer les intervenants.
Quant aux types d'attaques, outre le rançonnage « qui va continuer à se développer », selon le DG de l'ANSSI, il y a aussi l'espionnage « qui touche tout le monde », ou le sabotage, qui vise à porter atteinte au système de la gestion de la donnée, et qui, là encore, « par rebond peut toucher beaucoup de monde », indique-t-il, fournissant l'exemple, peu rassurant, d'un système de transport qui pourrait être retourné contre son utilisateur... A ceux-là le colonel de gendarmerie ajoute aussi le « défaçage » visant à nuire à l'image ou à la réputation d'une entreprise par la modification non sollicitée de la présentation d'un site web.

32% d'augmentation de dépôt de plainte

Selon le Colonel Christophe Vercellone, « ce sont 5300 plaintes liées à la cybercriminalité qui sont déposées chaque mois sur le territoire, en zone gendarmerie . C'est une augmentation de 32% par rapport à 2016, mais cela représente sans doute très peu par rapport à la réalité de faits », nuance-t-il. Car un autre des messages importants, et répétés, de la matinée a été d'encourager au signalement et au dépôt de plainte. « Dans ce domaine, ce n'est pas toujours le cas, car pas mal d'entreprises ne sont pas fières de s'être faites « pigeonner ». Pour autant, cela permet aux différents services de croiser les données et d'avoir une meilleure connaissance de cette cyber criminalité », encourage notamment Michel Gouriou, le Directeur de Cabinet du Préfet.
Car en effet, la cybercriminalité est n'est pas l'apanage de quelques « geeks » isolés, confirme le colonel de gendarmerie. « Il y a désormais une véritable structuration du « darknet », avec des groupes spécialisés dans le cryptage de données, d'autres dans l'effraction des systèmes d'information... A cela s'ajoute une démocratisation des pratiques, mais aussi une professionnalisation, avec de véritables « "prestataires" se proposant d'entrer dans un système d'information pour vous. Au regard des prix proposés, l'attaque peut ainsi venir d'une petite structure, comme un concurrent ou un ancien employé mécontent... » Pas de quoi rassurer le public présent dans la salle....

"Se protéger n'est pas si compliqué"

Si le discours anxiogène des intervenants a sans doute marqué les esprits, celui-ci s'est aussi voulu positif. « Les risques sont majeurs, mais se protéger n'est pas si compliqué », a en effet contre-balancé Guillaume Poupard. Et, pour cause, la plus grosse faille de sécurité, se trouve dans l'interface clavier-chaise : c'est l'utilisateur », s'est amusé Christophe Vercellone. « Il faut sensibiliser les personnels, identifier les données sensibles, fixer des règles d'utilisation du Système d'information, apprendre à repérer les anomalies de fonctionnement... et bien sûr aussi sécuriser son système d'information, avoir un plan de sauvegarde, éventuellement un plan de communication de crise, etc. »
Une sensibilisation aux risques qui est une des vocations du site cybermalveillance.gouv.fr présenté par son Directeur général, Jérôme Notin, comme « un dispositif d'assistance aux victimes de cyberattaque », à l'initiative de l'Etat. Car, au-delà de la prévention, l'outil lancé en avril dernier offre une aide aux victimes, à travers la réalisation d'un certain nombre de « fiches réflexes sur quoi faire en cas d'attaque », ou encore de mise en contact possible avec des prestataires de proximité pour tenter de remédier aux conséquences de cette attaque. Par ailleurs un kit de sensibilisation s'apprête à être édité à partir de logiciels libres afin d'être disponible auprès du plus grand nombre. Pour l'heure, « nous manquons encore de relais pour une diffusion de ce kit auprès des petites structures, regrette-t-il ». Mais nul doute qu'une journée comme celle-ci, permettra d'améliorer le score, au moins dans le département.

Solène Méric

Crédit Photo : Aqui.fr
Publié sur aqui.fr le 21/03/2018
Url de cet article