Ecrit par Echo du Mardi le 4 février 2020

Vers un marché unique du numérique ?

La semaine dernière vient de se tenir à Lille le FIC (Forum International de la Cyber sécurité). Cet événement mondial de référence en matière de sécurité et de confiance numérique rassemble chaque année près de 10 000 participants. Entre- tien avec Guillaume Tissier, président de la CEIS (Compagnie européenne d'intelligence stratégique)

■ Le FIC change de dimension cette année, en passant sur trois jours au lieu de deux. Pourquoi ?

« Nous avons ressenti le besoin d'avoir une journée supplémentaire de networking dédiée aux partenaires, de plus en plus nombreux. Et comme le nombre de participants augmente d'année en année de 20% (9 700 participants en 2019, ndlr), il était important d'étaler les participations pour ne pas se sentir à l'étroit. C'est l'occasion égale- ment d'organiser davantage de 'side event' comme la Vauban Cession à la Citadelle de Lille sur le thème de la transformation numérique des opérations militaires, à laquelle nous ajoutons l'ID Forum sur les sujets de l'identité numérique, puisque le Gouvernement travaille actuellement sur une feuille de route pour lancer la future carte d'identité numérique. Ce même jour, Acteurs publics, en lien avec la Métropole européenne de Lille, animera un temps fort sur les collectivités et la responsabilité des élus en matière de cyber sécurité. »

■ Comment les maires prennent- ils conscience de cette nécessité de transformation numérique et, donc, de sécurité des données ?

« C'est plutôt inégal en fonction des communes. Les collectivités de taille importante se sont emparées du sujet depuis quelque temps déjà mais, en revanche, de nombreuses agglomérations ou communautés de communes sont encore très en retard du fait de leur transformation numérique plus récente. Et, par conséquent, la sécurité est prise en compte plus tardivement. En octobre 2019, un 'ransomware' (ndrl logiciel de rançon) a ciblé la communauté de Grand-Cognac, en Charente, qui a complétement paralysé le système informatique. Il y a un réel impact sur les administrés avec une paralysie des services puisque de nombreuses formalités administratives se font aujourd'hui sur internet. La prise de conscience des collectivités est un véritable enjeu. »

■ Prennent-elles les choses en main ?

Ecrit par Echo du Mardi le 4 février 2020

« Un certain nombre de communes se sont déjà regroupées pour monter des GIP (groupements d'intérêt public) sur les questions d'informatique et les systèmes d'information. Les collectivités possèdent des données, pour certaines, assez stratégiques. Une fuite de données des administrés peut mettre la collectivité en danger. L'impact de la trans- formation numérique est bien pris en compte mais on sent que la sécurité passe après. »

■ Pourquoi ?

« Je dirai qu'il y a les bonnes et les mauvaises raisons ! Les bonnes ? Vouloir aller vite, innover pour réduire le temps de mise sur le marché mais… cela ne milite pas vraiment pour la prise en compte de la sécurité. Et les mauvaises ? Voir la sécurité uniquement comme un coût. Bien évidemment, c'en est un mais il faut pouvoir concilier expérience utilisateur et sécurité. Le coût de la sécurité ne représente que quelques pourcents du coût global d'un projet ; le sujet le mérite bien quand on voit l'impact financier que peut avoir une fuite de données et les risques pénaux qu'il engendre. »

■ Cela passe par de la pédagogie et de la sensibilisation ?

« Chaque année, les solutions de sensibilisation et d'e-learning progressent et ce sera l'un des autres sujets du FIC : améliorer la prise de conscience de l'utilisateur, notamment sur les sujets d'ingénierie sociale. Il ne faut pas oublier non plus le côté du défenseur : effectivement, l'intelligence artificielle améliore la cyber sécurité mais il y a clairement un besoin de compétences, d'analyses et d'experts. Aujourd'hui nous sommes confrontés à un vrai problème : de nombreux postes ne sont pas pourvus, sans doute parce que nous n'avons pas assez communiqué. »

> « Une fuite de données des administrés peut mettre la collectivité en danger. »

■ Vous parliez d'utilisateur, justement, on sait aujourd'hui qu'il est le premier concerné par les sujets d'authentification.

« Le sujet de cette année porte sur la place de l'humain dans la cyber sécurité car le cyber espace est avant tout un espace humain. Le sujet de la sécurité n'est pas uniquement technique ou technologique. L'utilisateur reste, et heureusement, l'Homme. L'expérience utilisateur, en termes de sécurité, a été très longtemps négligée et on a trop pensé que la sécurité ne pouvait pas être ergonomique. Il n'est plus possible d'utiliser les anciens dispositifs. Aujourd'hui, un utilisateur possède plus d'une centaine de mots de passe. Autre aspect de ce thème : la victime, qui se fait avoir en ayant été naïve ou négligente. On voit bien que le facteur humain joue dans la plupart des cas et le courriel reste le premier vecteur d'infection.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par Echo du Mardi le 4 février 2020

Il faut encore et toujours travailler sur la sensibilisation. Un 'fishing' sur quatre est ouvert par les utilisateurs : cela veut donc dire qu'il y a encore des progrès à faire ! »

■ Quelles solutions préconisez- vous pour améliorer l'authentification ? On parle de la fin des mots de passe, est-ce réellement possible ?

« On l'annonce depuis long- temps ! C'est un vrai sujet, en effet. Aujourd'hui, il existe des technologies de biométrie et de biométrie comportementale qui peuvent permettre d'apporter des solutions en termes d'authentification. Les authentifications à deux facteurs (de type 3D Secure qui envoient un message lors d'un paiement, ndlr) sont perçues comme lourdes et contraignantes par les utilisateurs. Toute la question est de trouver comment simplifier ces démarches. Pourquoi ne pas imaginer un dispositif tel que France Connect (qui permet d'accéder plus facilement aux services publics via un compte unique) ? Cela suppose de créer des écosystèmes acceptant les mêmes identifiants et identités. Mais je suis convaincu qu'adopter cette logique d'éco- système et avoir un dispositif d'authentification dont la gestion permet de se connecter à différents services est, pour l'utilisateur, une bonne solution. »

■ Peut-on s'inspirer d'autres pays sur ces sujets ?

« L'Estonie est souvent citée en exemple sur l'identité ; il y a aussi des expériences intéressantes en Belgique. En France, nous sommes malheureusement un peu en retard et c'est assez paradoxal car sur ces sujets d'identité, et notamment sur la partie du support physique de l'identité, notamment avec les cartes à puce, nous étions à la pointe il y a quelques années. Pour des tas de raisons nous avons pris du retard. Nous sommes en train de le combler. En matière de cyber sécurité, l'éco-système français est très innovant, avec de nombreuses PME qui développent des solutions localisées selon les besoins. La difficulté à laquelle nous faisons face c'est l'accélération de ces entreprises. Faute d'avoir, sur le territoire, de grands groupes ou de gros éditeurs généra- listes spécialisés dans la sécurité qui constituent des pôles d'agrégation, les PME ne grossissent pas assez vite et se vendent trop tôt à des entre- prises étrangères. »

> « Il y a clairement un besoin de compétences, d'analyses et d'experts. »

■ Quelle est la politique actuelle du Gouvernement en matière de sécurité numérique ?

« Il y a des actions sur les différents volets : d'abord avec la montée en puissance des moyens dédiés à

Ecrit par Echo du Mardi le 4 février 2020

l'ANSII (Agence nationale de la sécurité des systèmes d'informartion) sur la prise en compte de la sécurité non seulement des administrations mais aussi des services vitaux. Ensuite, sur la partie militaire et ses capacités de lutte informatique défensive mais aussi offensive, où une vraie doctrine de lutte offensive a été lancée. Le ministère des Armées cherche aujourd'hui à être autonome dans sa défense sur terre en s'appuyant sur des technologies et des moyens souverains. Dans ce cadre, le ministère a lancé plusieurs projets, notamment celui de 'Cyberdéfense factory' à Rennes en octobre 2019, ouvert à tous les acteurs du domaine cyber pour faire émerger de nouvelles technologies. Au niveau interministériel, la question réside plutôt dans la nécessité de créer un lieu – à la fois lieu de formation, de business et d'accueil des start-ups – sur le modèle du campus israélien, qui a inspiré Emmanuel Macron lors d'un voyage présidentiel. C'est un projet que nous soutenons et qui est porté par Orange Cyber défense. »

■ En 2018, la mise en place du RGPD (Règlement européen pour la protection des données) a bousculé l'ensemble du tissu économique et social. Vers quelles perspectives se tourne le marché de la cyber sécurité pour les années à venir ?

« Le débat est avant tout européen, pour avoir un marché unique du numérique. Certes, nous avons déjà fait un pas important avec le RGPD. Mais d'un point de vue du business, les marchés sont encore très cloisonnés. Une start-up ou une entreprise française de cyber sécurité se tourne d'abord vers le marché américain plutôt que vers les marchés européens. Ces sujets sont souverains mais pas unique- ment, il est possible de collaborer entre acteurs européens et sur ce point, le FIC s'est donné pour objectif de participer à ce décloisonnement international. »

Propos recueillis par Amandine Pinot La Gazette Nord-Pas de Calais pour Réso Hebdo Éco reso-hebdo-eco.com

Quelques chiffres

• Marché mondial de la cyber sécurité en 2019 : 150 milliards de dollars

• Marché français : entre 4 et 6 milliards d'euros

• Premier marché européen : la Grande-Bretagne

• Au premier semestre 2019, la CNIL a enregistré en moyenne 5,7 violations par jour

Les secteurs les plus touchés : l'hébergement et la restauration (188 violations), le commerce (177), la finance (137), les sciences et techniques (132) et l'Administration publique (92)

Causes principales : malveillance (54%), cause accidentelle (26%), violations ou fuites d'origine autre ou

Ecrit par Echo du Mardi le 4 février 2020

inconnue (20%).

Observatoire Data Breach