CONFÉRENCE PLÉNIÈRE - ÉCHANGES CROISÉS EN TABLE RONDE

Cybersécurité, cyberdéfense : sommes-nous véritablement des utilisateurs avertis ?

Cybersécurité, cyberdéfense, cybercriminalité : comment ne pas céder à la panique devant tant de messages médiatiques qui affolent ? Doit-on se désintéresser totalement de ce sujet tellement complexe ? Les plus grandes entreprises hyper protégées avec de gros moyens et aux experts de renom, se font dépouiller de nos informations stratégiques ou personnelles et sensibles. Comment est-ce possible ? Plus les moyens sont sophistiqués, plus cela coûte cher et moins nous avons l'impression de maîtriser notre sécurité, devant la confier à des tiers plus experts. Alors, on fait quoi ?

Tout d'abord, il faut « raison garder ». Les termes « cyber..... » utilisés aujourd'hui segmentent des cibles différentes : la sécurité du numérique (désormais présent partout), la sécurité des infrastructures et organismes d'importance vitale, les attaques numériques des bandits internationaux (qui risquent moins en opérant d'un PC caché dans le monde virtuel), ... La Cybersécurité ne s'adresse donc pas de la même manière aux acteurs ayant à l'évidence des caractéristiques différentes. Une démarche d'observation, de collecte d'information, d'analyse et de diagnostic s'impose au préalable. Si vous ne savez pas quelle méthode choisir pour y voir clair, vous avez des informations structurées, fiables, sur des sites officiels :

- l'ANSSI par exemple, https://www.ssi.gouv.fr/, l'Agence Nationale de la Sécurité des Systèmes d'Information,

- la CNIL, la Commission Nationale de l'Informatique et des Libertés, https://www.cnil.fr/fr

- Le CLUSIF national et les Clusir régionaux, dont le Clusir-Auvergne-Rhône-Alpes www.clusir-rha.org

- ...

Vous avez entendu parler du RGPD, du Règlement Général de Protection des Données, mis en place par l'Europe pour donner un nouvel élan à la Loi Informatique et Libertés, qui date de janvier 1978, et qui visait à protéger nos données personnelles en obligeant les acteurs de la collecte et du traitement de nos données à respecter 5 règles d'or :

- La finalité,
- La proportionnalité,
- Le droit à l'oubli,
- Le respect du droit des personnes,
- La sécurité des données.

Le RGPD complète ce dispositif en introduisant d'autres obligations. Parmi celles-ci, il oblige les acteurs de la collecte et du traitement des données à faire ce travail de diagnostic, de lister tous les traitements et toutes les données qualifiées de personnelles ou sensibles, et de décrire à quoi elles servent, à qui elles servent, de s'engager à respecter les obligations en découlant, de vous garantir une description fidèle de ce qui est collecté et traité et de s'y conformer. Il vous permet de refuser votre consentement, de récupérer vos données, ...

Le RGPD oblige aussi à prouver que l'entreprise lui est conforme et de mettre en place un processus qualité de suivi et de vérification de cette conformité. Votre rôle en tant qu'entreprise est donc de décrire, de vérifier, de trier, de s'engager à respecter les principes et règles définies dont la sécurité des données. Votre rôle en tant que citoyen est de vérifier que les acteurs avec qui vous échangez ont documenté leur organisation au regard du RGPD et vous permettent de savoir ce qu'ils font de vos données, y compris sur le plan sécuritaire. Les amendes potentielles sont désormais très dissuasives.

Pour être moins exposé devant le monde cyber qui nous entoure, commençons par prioriser nos données : 5% seulement de nos données sont stratégiques. Mettons notre attention sur celles-ci. Apprivoisons les outils qui nous sont offerts (si c'est gratuit, c'est vous le produit !), ne cliquez-pas sur « OK » sans lire, refusez d'utiliser un produit qui ne respecte pas le RGPD. Si les plus connus ne sont pas toujours conformes, leur puissance peut-elle résister à la prise de conscience collective de l'obligation de respecter ses données, surtout personnelles ?

Comme la ceinture de sécurité il y a quelque années (ou le casque à vélo), il fallait obliger à l'attacher (ou le porter). De plus en plus de personnes ne peuvent plus conduire un véhicule sans boucler leur ceinture ou faire du vélo sans casque. C'est exactement la même situation pour la sécurité dans le monde du numérique, il y a des malfaisants qui ont encore trop de chance de pouvoir voler (dupliquer, cela ne se voit même pas !!!) facilement, sans être retrouvé, sans risquer une peine dissuasive. Il ne tient donc qu'à nous tous de mettre la barre un peu plus haut, de prendre les précautions d'usage, de consacrer un petit budget pour acheter des licences ou des systèmes de sécurité. Nous ne faisons plus attention à la serrure de notre porte d'entrée 5 points, 5 étoiles, … qui n'est pas infaillible. Il faut donc s'attacher à ces quelques mesures de précautions pour commencer et nous ne serons dès lors un peu plus des utilisateurs avertis …

Pascal VINCENT,

Secrétaire Général Adjoint du Clusir RhA, co-animateur Club Intelligence Economique
Président - Manager Opérationnel ***M2GS SAS***