Fédération des Entreprises Romandes
FER Genève - FPE Bulle - UPCF Fribourg
FER Arcju - FER Neuchâtel - FER Valais

Procédure de consultation	Personnes responsables:	Date de réponse:
FER No 07-2022	M. R. Diez	18.03.2022

Modification de l'ordonnance sur les services de télécommunication (sécurité des informations et des infrastructures et services de télécommunication)

La FER salue l'approche et le travail effectué. Le contenu de cette procédure de consultation correspond à ce que l'on peut attendre du travail législatif, tant du point de vue de la gouvernance que des actions prévues, qui sont en adéquation avec la gestion du risque international dans son état actuel.

Notre fédération est alignée sur les actions techniques et organisationnelles proposées, telle la mise en place obligatoire des procédures de filtrage d'adresses IP pour les opérateurs, l'obligation de déclarer la mise en place d'un SGSI se basant sur les normes ISO, l'obligation de développer et maintenir une gestion des risques, la mise en place d'une gestion des incidents et de traçabilité des preuves, la garantie de la communication aussi bien aux instances de régulation (OFCOM, NCSC) qu'aux tiers impactés (clients) et la possibilité de déclencher des audits.

Tout cela correspond au niveau de maturité internationale, et n'attire pas de remarques détaillées de notre part. Cependant, il est nécessaire de relever l'apparition dans le texte d'approches que l'on peut considérer comme parallèles :

1) La cybermenace

Est-ce que la cybermenace est une affaire d'État? Si tel est le cas, nous pourrions parler de la protection des technologies de l'information comme faisant partie de la souveraineté, car nécessaire à la vie des entreprises et considéré dès lors comme une richesse essentielle.

Selon notre lecture, les cybermenaces doivent être placées à la croisée de la population et du territoire et par ailleurs, attendre des fournisseurs d'accès internet (FAI) qu'ils couvrent le risque «d'une manière adéquate», ne sera pas suffisant. Par exemple, les cybermenaces dont sont victimes les PME, pourraient être mieux couvertes si l'on applique aux opérateurs de VPN certaines règles appliquées aux FAI.

Le mode de fonctionnement basé sur des VPN chiffrés dont les adresses IP sources changent régulièrement amène à ce que les mécanismes prévus par les FAI ne voient pas la menace ou la détecte une fois qu'elle est dans l'espace de communication interne à la Confédération. Les solutions point à point sans traçage des sources sont un avantage pour la cybercriminalité qu'il ne faudrait pas négliger.

La FER Genève en particulier apporte depuis des décennies son accompagnement et ses compétences au sein des PME, et le fait aussi désormais au travers d'un accompagnement de maturité Cyber qu'elle met en place actuellement.

Mais au regard des 500'000 entreprises existantes au sein de la Confédération et le temps nécessaire pour les sensibiliser aux cybermenaces, il faudrait un siècle pour augmenter leur maturité, alors qu'humainement parlant, nous ne l'avons pas.

2) Les cyberrisques ont plusieurs facettes

Le rapport explicatif montre clairement le niveau de maturité atteint et attendu, les prescriptions techniques et administratives en sont la preuve. Mais les infections subies par des environnements techniques de type CPE ne peut être effectuées que par des États ou des groupes criminels organisés et sont loin des menaces qui ciblent le tissu économique des entreprises. Outre la mise en évidence de la différence, c'est la prise en charge de toutes les facettes des cyberrisques qui permettra la résilience numérique.

3) La protection de la 5G

Les FAI étant déjà considérés comme des infrastructures critiques, la protection de la 5G et des objets connectés est un vaste chantier qui reste encore à baliser et nécessitera de l'omniprésence du législateur dans la durée, les objets connectés ne font que timidement leur apparition pour le moment.

Il faut retenir que la 5G n'est que le vecteur de propagation: elle permettrait l'augmentation du vol de données et le chantage uniquement si les objets connectés sont faillibles, mal configurés, ont des failles de sécurité potentielles ou leur système de sécurité est immature au regard du risque connu.

Tout cela rend l'exercice difficile et force le législateur à communiquer sur les méthodes de communication, le type de chiffrement, la protection adéquate et le niveau de sécurité attendu.

Vaste chantier qui dépasse clairement les limites fédérales, celle des fournisseurs d'accès et d'autres intermédiaires de communication et dont le débat se déplace au niveau des fournisseurs d'objets connectés et de leur obligation, sans doute à travers des organes supra, tels l'IETF et leurs Best Current Practice, les accords de l'Organisation mondiale du commerce et de l'ENISA.

Cela étant dit, toutes considérations faites, l'adaptation de la loi, notamment à travers l'article 96, semble à propos et bienvenue.

En conclusion, notre fédération soutient cette modification d'ordonnance sur les services de télécommunication.