Il est urgent de renforcer la cybersécurité en France

À l'heure où la sécurité des systèmes d'information fait l'objet de toute l'attention de l'exécutif en Europe comme aux États-Unis, le **Centre d'analyse stratégique** (CAS) publie sa note d'analyse sur la **cybersécurité**.

La cybersécurité est une urgence

Institution d'expertise chargée d'éclairer les orientations du gouvernement français, le CAS estime que les organisations et les particuliers sont insuffisamment protégés pour faire face à des attaques informatiques toujours plus sophistiquées : déni de service, malveillance, usurpation d'identité, attaques de couches basses des réseaux…

Qu'il s'agisse de cybercriminalité, cyberespionnage ou de militarisation du cyberespace, ces attaques se multiplient avec l'augmentation du nombre de terminaux connectés, l'engouement pour le Cloud et l'Internet des objets. Ainsi, **50 milliards d'objets** devraient être connectés à Internet en 2020.

Qu'en est-il aujourd'hui de la perception du risque ?

- Seuls **38 % des Français** seraient conscients que le téléchargement d'applications sur smartphones/tablettes est un facteur de risque ;
- Bien que **63 % des entreprises** de plus de 200 salariés en France aient une politique de sécurité de l'information, seules 14 % d'entre elles évalueraient systématiquement l'impact financier de cyberattaques ;

À l'échelle mondiale, le coût de la cybercriminalité a été estimé en 2012 par Symantec à 110 milliards de dollars (87,5 milliards d'euros), dont 2,5 milliards d'euros en France.

Dans ce contexte, observe le CAS dans son analyse, *« élever le niveau de cybersécurité est une urgence pour préserver la compétitivité économique et la souveraineté nationale »*.

Vers une extension des missions de l'ANSSI

Comment concilier sécurité, ouverture des systèmes d'information et protection des libertés individuelles ? Le Centre d'analyse stratégique formule les quatre propositions suivantes :

- **Renforcer les exigences de sécurité** imposées aux opérateurs d'importance vitale (OIV), sous le contrôle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;
- Développer et mettre à la disposition des PME des outils simples pour **gérer les risques** ;
- **Élargir les missions de l'ANSSI** pour accompagner le développement de l'offre française de solutions de cybersécurité ;
- **Revoir le cadre juridique** afin de conduire, sous le contrôle de l'ANSSI et d'un comité

d'éthique ad hoc, des expérimentations sur la sécurité des logiciels et les moyens de traiter les attaques.

Parallèlement, l'offre de formation en France devrait être étendue afin de répondre *« à la demande croissante d'experts en sécurité informatique »*. Plus largement, conclut le CAS, le déficit d'éducation à l'informatique dans le pays pourrait être comblé par *« l'enseignement de l'usage et des langages numériques dès le primaire et le secondaire »*.

Voir aussi

Dossier Silicon.fr – Internet est-il prêt pour l'Internet des Objets ?