Les Security Days au à Dakar du 15 au 16 mars 2016

" *les gens disent toujours : n'aie pas peur de ce que tu ignores mais ils ont tort, ce que tu ignores aujourd'hui, demain te tueras* "[1]

Le 15 et le 16 mars 2016 se sont tenus à Dakar les Security Days (Secdays - https://www.securitydaysn.com/). Un événement qui, selon le programme prévisionnel, était sensé se focaliser sur le Sénégal, mais qui s'est finalement transformé en une rencontre Ouest-africaine sur la CyberSécurité. Le Bénin, la Côte-d'Ivoire, le Ghana, la Guinée, le Niger, le Burkina, la France, les Pays-Bas étaient représentés à cette rencontre.

L'objectif principal des Secdays est de promouvoir une vision et une réponse commune face aux menaces en constante évolution que sont les cybermenaces. Pour cela, les organisateurs ont réuni un public constitué d'experts, d'étudiants, d'entreprises et d'institutions confrontées aux cybermenaces pour, pendant 02 jours, faire le point des actions méthodes et solutions disponibles actuellement en Afrique.

Au cours de ces deux journées, les expériences et initiatives du Sénégal (pays hôte), de la Côte d'ivoire, de la France ont été présentées. Chacun de ces pays s'est doté d'un arsenal juridique et de solutions organisationnelles lui permettant de disposer d'outils nécessaires aux actions de lutte contre la cybercriminalité. Au nombre de ces outils, on peut citer : la mise en place de centre national de cybersécurité, de CERT[2], de point d'échange, le recensement des cyber-cafés. En Côte-d'ivoire, l'incidence financière de la cybercriminalité est évaluée à 4 milliards de XOF (selon les autorités ivoiriennes).

En dehors des plénières qui portaient sur des aspects génériques (*la sécurisation de la monnaie électronique dans l'espace UEMOA*[3]*, la sécurité des infrastructures critique des nations, les mécanismes de financement des projets cybers, Lutte contre la cyber criminalité en Côte-d'Ivoire, Faire de la lutte pour la cybersécurité, une grande cause francophone, retour d'expérience sur la coordination de la cybersécurité en Afrique*), des ateliers thématiques ont été proposés portant entre autres *sur la démarche pour la sécurisation des SI, les nouveaux métiers issus de l' émergence des cybermenaces, Identification électronique dans la transformation numérique)*.

Quatre points me paraissent importants à retenir :

1. Au plus haut niveau, la nature transfrontalière des cybermenaces impose une approche et une coordination au minimum sous régionale du problème. Aucun État ne dispose tout seul des moyens et des ressources nécessaires à sa résolution. L'attaquant d'un pays A, pouvant se rendre dans un pays B pour se connecter à un ordinateur situé dans un pays C pour attaquer un pays F en faisant transiter les communications par les pays D et E. Cette nécessité imposent en parallèle qu'au niveau des États, des outils et moyens soient organisés pour apporter une réponse efficace. Ce qui nous amène au point suivant ..
2. Au niveau national et des organisations, les politiques sécuritaires ne peut plus être conçue sans prise en compte des aspects cybersécurité. La législation doit être amendée pour permettre la prise en compte de la spécificité cyber. Les services de sécurité de l'état et des institutions (entreprises, etc) doivent être organisés pour pouvoir agir face aux cybermenaces. Ceci implique la formation, la constitution d'unités spécifiques et d'outils

1 Psy 4 De La rime, VOICI

2 Les CERT (Computer Emergency Response Team) sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous. (Source https://fr.wikipedia.org/wiki/Computer_Emergency_Response_Team)

3 L'Union économique et monétaire ouest-africaine (UEMOA) est une organisation ouest-africaine qui a comme mission la réalisation de l'intégration économique des États membres,

spécifiques comme les centres nationaux de cybersécurité, les CERT, les points d'échange etc, mais ainsi la *sensibilisation* et l'*éducation* des masses aux règles d'hygiène numérique.

3. Il n'est pas nécessaire de réinventer la roue. L'expertise et les retours d'expérience existant déjà, il appartient aux institutions de les rechercher et de les mettre à contribution. Nous pouvons citer ici l'exemple de l'ANSSI[4] qui assiste déjà le Sénégal sur les questions de Cybersécurité[5]. Ensuite les chancelleries et représentations diplomatiques des États du nord intègrent déjà dans leur plan d'action, une assistance en matière de cybersécurité (exemple du travail fait par la coopération militaire française[6] en Afrique de l'ouest).
4. Enfin, et **peut-être le point le plus important**, il est nécessaire de repenser les dispositifs de classiques formation, afin d'intégrer la sécurité et la cybersécurité comme éléments de base des réflexions, et ce dans tous les corps de métier. En effet, les systèmes d'information sont la base de l'économie moderne, dans tous les secteurs d'activité, de l'agronomie à l'armement en passant par la santé et les finances. L'information c'est le pouvoir. Les futurs managers, décideurs, ingénieurs, techniciens doivent être formés pour prendre en compte les cyberrisques dans leurs politiques, leurs actions, leurs décisions.

Maintenant, que faudrait-t'il faire pour nous au Bénin. Je voudrais ici proposer 3 pistes qui pourraient rapidement nous permettre d'avancer :

1. Organiser nos Journées Nationales de la Cybersécurité (JNC) où tous les acteurs (forces de l'ordre, forces de défense, agences gouvernementales, entreprises, FAI, chercheurs, magistrats et juges, politiques, agence de coopération et chancelleries, etc.) seraient fortement conviés par la plus haute autorité politico-administrative : Le Président de la République. Objectif principal : Où en est-on au Bénin sur cette question ? Il s'agira de faire un état des lieux succinct, de tout ce qui a été fait, ou est fait par les acteurs dans ce domaine.
2. Au sortir des JNC, monter un groupe restreint chargé de poursuivre les discussions et de proposer sous trois (03) mois, un agenda clair (sur 02 ans) des différentes actions à prendre pour mettre le Bénin au moins au niveau des pays les plus avancés de la sous-région (Sénégal, Côte d'Ivoire, Nigéria) et planifier les prochains JNC. Il appartiendra également à ce groupe d'identifier les grand événements où il faudra absolument que le Bénin soit présent et de le rappeler aux structures concernées.
3. En prélude et suite aux JNC, monter un groupe restreint chargé de finaliser le CERT Bénin et des groupes sectoriels chargés des CERTs sectoriels. En effet, il est illusoire d'attendre par exemple du Ministère de la défense, l'ouverture des rapports d'incidents à des personnes ne disposant pas du niveau d'accréditation nécessaire.

Voilà, ce que je retiens globalement des SecDays et de leur intérêt pour nous. Après, qui est prêt à prendre son bâton de pèlerin pour aller expliquer tout cela à ceux qui doivent prendre les décisions .. ? La question reste ouverte ...

---

4 ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. http://www.ssi.gouv.fr/

5 L'ADIE et l'ANSSI ont signé en marge des cette édition des SecurityDays, un programme de coopération bilatérale qui vise à « *partager les expériences et à mutualiser les connaissances des approches, des savoir-faire et des bonnes pratiques en matière de sécurité des systèmes* d'information » (source : http://www.ssi.gouv.fr/actualite/ladie-et-lanssi-signent-un-protocole-de-cooperation-bilaterale/ vu le 16 mars 2016)

6 C'est le cas spécifique des éléments français au Sénégal (EFS) qui assistent les armées Ouest-Africaines dans la prise en compte des cybermanaces (formation, atelier spécialisé pour l'armée, la police et la gendarmerie, etc.).