METEO DU NUMERIQUE

ETUDE SUR L'ETAT DES LIEUX DE LA PROTECTION DU CYBERESPACE AFRICAIN

Pendant que des pays comme la Tunisie, la Zambie, le Rwanda, le Togo s'activent pour instaurer des institutions fortes à même d'agir efficacement et rapidement en cas de cyberattaque d'une part et protéger les citoyens et entreprises d'autre part, le dispositif de défense du cyberespace sénégalais semble être méconnu des acteurs. En effet, lorsque l'on recherche -par exemple ou par réflexe- le groupe de mots CERT Sénégal, en top du résultat des recherches, on retrouve un article d'un partenariat du Sénégal avec l'Agence Nationale des Services et Systèmes d'Information (ANSSI) de la France.
En effet, dans le cadre de ses missions d'assurer un cyberespace stable et sûr et d'accompagner les pays en voie de développement dans ce sens, l'ANSSI est elle-même membre d'AfricaCERT ; organisme à but non lucratif créé en mai 2010 à Kigali au Rwanda et dont l'objectif est d'aider les pays africains à mettre en place et à exploiter des équipes de sécurité informatique et de réponses aux incidents tout en leur fournissant de l'expertise et des conseils. Tandis que le Sénégal est en instance d'adhérer à cette vision panafriciane de bâtir une Afrique unie dans la promotion de la cybersécurité.

Certes le Sénégal a installé récemment son équipe de réponse opérationnelle aux incidents mergée au sein de l'ADIE. C'est ce qui justifierait le fait que cet organe national qui porte de lourdes responsabilités soit inconnu du public.
Pourtant il serait judiciable de mettre en exergue cette structure nationale de défense contre les cyberattaques Par exemple :

- en commençant par la rendre autonome de l'ADIE,
- en ayant un site vitrine qui présente ses missions et prérogatives (sencert.sn ?)
- en la nommant sans ambiguïté (SenCERT ne serait pas mal).

Ces recommandations s'affichent simples mais leurs mises en applications permettront de situer les acteurs et de mieux les rassurer dans leur usages quotidiens du cyberespace que ce soit dans le cadre professionnel ou personnel. Dans le document de la stratégie nationale sénégalaise de la cybersécurité (SNC 2022) mise en place en 2017, la création du CERT fait partie des objectifs clés mais 4 ans après l'instance parait faible en n'est pas placée au centre des moyens de défense du cyberespace sénégalais.

Devons-nous rappeler que les attaques au cyberespace ont valeurs égales à celles d'attaque terroristes ? Un cyberespace nu sans défense favorise l'intrusion des personnes malveillantes qui pourraient pénétrer et provoquer d'importants dégâts tels que les pertes financières (faute de disponibilité), les risques de porter atteinte à l'intégrité des citoyens et l'accès à des informations classées secret défense (faute de confidentialité). Pour la petite leçon : confidentialité, disponibilité et intégrité constituent les fondamentaux de la cybersécurité.
D'autres pays africains sont meilleurs élèves en termes de stratégie face aux enjeux de la cybersécurité.

Bien entendu malgré les efforts fournis par ces pays, il reste encore d'énormes progrès à faire notamment en ce qui concerne la formation et la sensibilisation des citoyens pourtant exposés. Nous avons réalisé une étude auprès de 27 pays africains dont l'Afrique de l'Est afin de mesurer leurs statuts en termes de stratégie de cybersécurité nationale. Les critères d'appréciation qui sont utilisés pour jauger chaque pays sont ceux qui sont recommandés au plan international pour construire un socle minimal d'un environnement de cybersécurité.

Il urge d'intégrer le fait que Internet prend un espace croissant dans notre vie quotidienne. Ceci est accompagné de nouveaux usages qui arrivent avec de nouveaux risques en face des usagers numériquement aculturés. Il y a donc urgence à mettre en place des dispositifs évolutifs à même de résister à la cybercriminalité.

Tableaux 1 et 2 : Table des légendes Critères et Statut Météo

NUMERO D'ORDRE	CORRESPONDANCE CRITERE
1	Existence d'un document de la stratégie nationale ou régionale de la cybersécurité
2	Existence d'un cadre règlementaire des communications électroniques
3	Existence de services ou organismes étatiques pour accompagner en cas d'incidents (CERT,CNIL)
4	Existence d'une agence ou institution étatique dédiée aux questions de sécurité des systèmes d'information (exemple : ANSSI)
5	Adhérence à CERT Africa
6	Existences de structures pour le développement des compétences locales en expertise cybersécurité
7	Accompagnement et sensibilisation adaptés de la population

METEO	DEFINITION
🟢	SATISFAISANT
🟡	PEUT MIEUX FAIRE
🟠	RESTE A FAIRE
🔴	RIEN N'EST FAIT

PAYS	CRITERES D'APPRECIATION						
	1	2	3	4	5	6	7
BENIN							
BURKINA FASO							
BURUNDI							
CAMEROUN							
COTE D'IVOIRE							
COMORES							
CONGO RDC							
DJIBOUTI							
ETHIOPIE							

GABON							
GHANA							
GUINEE							
KENYA							
MADAGASCAR							
MAURITANIE							
MALI							
MAROC							
NAMIBIE							
NIGER							
NIGERIA							
OUGANDA							
RWANDA							
SENEGAL							

SIERRA LEONE							
TCHAD							
TOGO							
TUNISIE							

Pour avoir des détails de recommandations pour passer au vert tous les critères par pays, prenez contact avec lameteodunumeriqueenafrique@gmail.com