

Rappel

Aperçu rapide sur nos **besoins urgents en matière de Logiciel Libre et Open-source** et sur **les pourquoi de** l'importance de l'approche Open-source (Logiciel Libre) **dans la stratégie Tunisienne, en matière de sécurité informatique:**

I- Aperçu rapide sur nos besoins urgents en matière de Logiciel Libre et Open-source et de l'importance de l'approche Open-source et Logiciel Libre dans la stratégie Tunisienne, en matière de sécurité informatique.

La stratégie Tunisienne, en matière de Sécurité Informatique dédie une importance **capitale aux opportunités offertes** par le domaine de l'open source et un besoin certain pour l'usage des outils disponibles dans le monde du Logiciel Libre.

- Besoins urgents en matière de Logiciel Libre et Open-source :

Selon nos diagnostics et entre autres, les résultats d'une enquête sur la sécurité des SI (ayant touché 70 entreprises stratégiques), réalisée par l'unité sécurité (Ex Agence Nationale de Sécurité Informatique) au cours de l'année 2003, il en ressort principalement :

-Premièrement :

Un besoin de déploiement de solutions de sécurité open-source, afin de combler les besoins quantitatifs (nombre de licences à déployer) et qualitatifs (types d'outils à déployer) :

Actuellement, un besoin logistique urgent est recensé, pour ce qui concerne :

- La disponibilité de centres de compétences privés, permettant de fournir une assistance aux usagers de produits open-source (choix, installation, formation, « maintenance »).
- Le renforcement de la formation sur les outils open-source (entre au niveau des cours académiques).
- La sensibilisation des utilisateurs sur la réalité des opportunités offertes par l'open source, ainsi que leur mise en conscience sur les éventuelles limites et les mesures d'accompagnement et enjeux à considérer.

En effet :

« La sécurité est intégrale ou elle ne l'est pas » :
L'utilisation libre d'outils du monde du Logiciel Libre permettra de réduire les besoins budgétaires énormes (licences, ..), induits par notre stratégie ambitieuse en matière de sécurisation de nos SI. Ils permettront ainsi d'assurer la complétude cardinale et qualitative des outils

de sécurité mis en œuvre. De plus, ces outils offrent, du moins pour les meilleurs, des caractéristiques rassurantes, quant à la pérennité de l'investissement car :

. Ils respectent les principaux standards (IETF).

. La documentation est assez fournie et l'assistance communautaire internationale est notable pour les meilleurs.

. Sont basés sur des étuis matures et « sécuritairement » sains (plate-forme unix, code étudié par la communauté scientifique, ...).

- Deuxièmement :

D'un autre côté complémentaire (encore plus stratégique et espérant le, qui sera INDUIT par le précédent besoin de "conseil"), il existe une urgence claire d'entamer l'éclosion d'une activité de Recherche/Développement basé(e) (primordialement) sur les outils open-source, permettant de satisfaire les besoins stratégiques d'autonomie nationale en matière d'outils de sécurité.

En effet :

- Pas de sécurité sans « confiance » dans les outils (disponibilité du code pour audit) : Pour les outils open-source, on peut vérifier tout ce que fait l'outil et comment il le fait (sans grande difficulté, la plupart du temps) et la pérennité est prouvée pour les meilleurs outils.

- Pas de sécurité sans autonomie des moyens (limitations imposées à l'export de certaines fonctions de sécurité) :
 - o On peut adapter et faire évoluer (sans grande difficulté) les outils open-source et adapter ce que fait l'outil et comment il le fait.

- o Le monde de l'open source offre des opportunités incomparables, comme moteur synergique stratégique, pour lancer une activité nationale de Recherche/Développement efficace, qui permettra de répondre à l'enjeu stratégique et urgent d'assurer l'autonomie nationale en la matière, avec des retombées bénéfiques sur l'emploi et l'export.

Source :

**National Agency for Computer Security (NACS)
Agence Nationale de la Sécurité Informatique
Ministère des Technologies de la Communication**