Nº 00277 du 18 au 22 mai 2026

zOOm

Défis de la souveraineté numérique et technologique : quelles stratégies pour l'Afrique ?

CHEDS
Savoir - Excellence - Sécurité
Centre des Hautes Etudes de Défense et de Sécurité

Le Zoom est un document hebdomadaire qui vise à donner un aperçu sur une thématique considérée comme tendance lourde dans la période couverte.

Sénégal, le Trésor public ciblé par une attaque, la 3e institution publique visée en six mois

Le Sénégal est, cette semaine, victime d'une troisième cyberattaque sur une institution publique, en moins de 6 mois. Après le site des impôts en octobre 2025, le Département chargé de délivrer les cartes nationales d'identité en janvier 2026, c'est au tour du Trésor public d'être victime d'une cyberattaque. Une nouvelle preuve de la vulnérabilité des systèmes informatiques au Sénégal devenu, comme d'autres pays africains en plein processus de digitalisation, la cible privilégiée des hackers. Selon les experts, cette nouvelle cyberattaque rappelle surtout l'urgence pour le Sénégal de mieux se préparer et d'anticiper ce genre d'intrusions. Pour cela, « *il faut une plus grande implication de l'État et réformer rapidement l'arsenal législatif* », affirme le spécialiste en cyberdéfense, Gérard Joseph Francisco Dacosta.

(Source : https://www.rfi.fr/fr/afrique/20260514-s%C3%A9n%C3%A9gal-le-tr%C3%A9sor-public-cibl%C3%A9-par-une-cyberattaque-la-troisi%C3%A8me-institution-publique-vis%C3%A9e-en-six-mois)

Le New Deal technologique à l'épreuve des cyberattaques répétées

Au Sénégal, le discours officiel met en avant des ambitions fortes : data centers, souveraineté numérique, résilience des systèmes d'information, modernisation de l'État. Sur le papier, l'architecture est cohérente, presque rassurante. Elle dessine un État conscient des enjeux de cybersécurité, cherchant à se doter d'outils modernes pour protéger ses infrastructures critiques et encadrer les usages numériques. Mais entre la stratégie et la réalité opérationnelle, un écart se creuse, visible à chaque nouvel incident, qui oblige une administration à suspendre ses activités, puis à les relancer dans l'urgence. Ce décalage soulève une question simple, mais essentielle : à quel moment la souveraineté numérique devient-elle effective, et non plus seulement déclarative ? À force d'incidents répétés, une forme de réalisme s'impose. Le pays n'est pas dépourvu d'ambition numérique, ni même de dispositifs en construction. Mais, il se trouve dans une phase intermédiaire où les infrastructures existent, les stratégies sont formulées, mais où la résilience réelle reste encore en consolidation.

(Source : https://www.osiris.sn/le-new-deal-technologique-a-l-epreuve-des-cyberattaques-repetees.html)

Comment les hackers font trembler nos institutions stratégiques ?

Pour les spécialistes, les conséquences d'attaques répétées pourraient devenir économiques et politiques. Une administration numérique, perçue comme vulnérable, risque d'affaiblir la confiance des citoyens dans les plateformes publiques, mais aussi celle des partenaires internationaux. « Si les systèmes qui produisent les données financières ou budgétaires sont compromis, cela pose un problème de crédibilité », avertit Gallo Fall, expert en cybersécurité, basé aux États-Unis. Gérard Joseph Francisco Dacosta redoute, lui, un scénario de paralysie généralisée, comparable à celui vécu par l'Estonie en 2007, après une série de cyberattaques massives. « *On peut se réveiller un jour avec des plateformes publiques bloquées, des services interrompus et un pays paralysé numériquement* », prévient-il. Face à la montée des cybermenaces, les experts plaident enfin pour un investissement massif dans les compétences locales. Tous deux estiment que le Sénégal dispose déjà de profils qualifiés, mais peine à les retenir ou à leur offrir un cadre de travail attractif. Il estime que le Sénégal ne pourra protéger durablement ses infrastructures numériques sans construire une véritable doctrine nationale de cybersécurité, fondée sur la prévention, la souveraineté technologique et le développement d'une expertise locale forte.

(Source : https://www.osiris.sn/le-senegal-est-il-une-cible-comment-des-hackers-font-trembler-nos-institutions.html)

L'expert Malick Fall propose une feuille de route pour renforcer la résilience numérique au Sénégal

Face aux récentes cyberattaques ayant visé des infrastructures étatiques majeures, le Sénégal se trouve « *à un tournant de son histoire technologique et sécuritaire* ». C'est le diagnostic posé par Malick Fall, consultant en cybersécurité et *Chief Executive Officer (CEO)* de Polaris Secure Technologies, qui avertit « *qu'ignorer ou minimiser la gravité de ces incidents serait une faute stratégique lourde de conséquences* ». Pour y faire face, l'expert décline une stratégie globale articulée en trois temps. L'urgence absolue repose sur la sécurisation immédiate des entités non encore impactées. Malick Fall recommande de mener « *des audits de sécurité immédiats sur toutes les administrations critiques* » afin de « *faire l'état des lieux de la cybersécurité de nos joyaux* ». Sur le plan opérationnel, il préconise la « *supervision permanente des actifs critiques* » ainsi que le déploiement d'une « *cellule nationale de réponse aux incidents, opérationnelle 24h/24* ». La sécurisation technique immédiate passe aussi par la « *mise à jour systématique des systèmes d'exploitation et logiciels* », le « *backup et la restauration des systèmes* » et le « *chiffrement des données sensibles au repos et en transit* ».

(Source : https://www.osiris.sn/cybersecurite-l-expert-malick-fall-propose-une-feuille-de-route-pour-renforcer.html)

Le Libéria se dote d'un laboratoire de cybersécurité et d'investigation numérique

Le Liberia s'est doté d'un laboratoire de cybersécurité et d'investigation numérique. Le dispositif vise à renforcer les capacités du pays face à la montée des menaces cybernétiques. Selon le ministère des Postes et Télécommunications, le laboratoire est équipé d'outils de criminalistique numérique de dernière génération, de systèmes de surveillance des menaces en temps réel, de capacités avancées de réponse aux incidents, ainsi que d'équipements spécialisés de formation. « *Ce laboratoire de classe mondiale renforce considérablement la capacité du pays à enquêter sur les cybercrimes, à récupérer des preuves numériques, à analyser les menaces et à se défendre contre les risques cyberémergents* ». Les pays africains misent, de plus en plus, sur le numérique pour soutenir leur développement socio-économique. Pour y parvenir, ils doivent investir davantage dans la cybersécurité.

(Source : https://www.wearetech.africa/fr/fils/actualites/gestion-publique/le-liberia-se-dote-d-un-laboratoire-de-cybersecurite-et-d-investigation-numerique)