



L'Administration de la défense nationale annonce deux lois respectivement sur la cybersécurité et les services de confiance

e-administration : Opération «commando» de l'armée

Mohamed Badrane
mbadrane@aujourd'hui.ma

Des protocoles stricts et obligatoires à destination des administrations publiques traitant des flux d'informations et de données à caractère sensible ou bien personnel pour les usagers seront mis en place.

Face à la montée des risques sur la Toile, les FAR (Forces armées royales) lancent l'offensive. En effet, le ministre délégué chargé de l'Administration de la défense nationale, Abdellatif Louidji, vient d'annoncer l'élaboration de deux textes de lois très importants. Et pour cause. Les projets sont appelés à combler un vide dans des domaines cruciaux, à savoir la cyber-sécurité et la dématérialisation des services. Dans le détail, le responsable a dévoilé la préparation d'un projet de loi relatif à

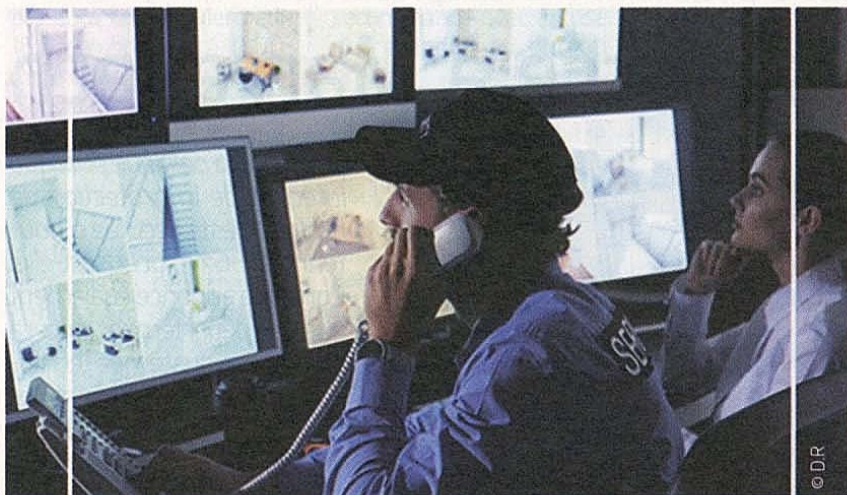
la cybersécurité qui va offrir un cadre légal pour l'optimisation de la défense et la sécurisation des systèmes d'information des administrations publiques ainsi que des sites stratégiques. Concrètement, l'Administration de la défense nationale va mettre en place par le biais dudit projet des protocoles stricts et obligatoires à destination des administrations publiques traitant des flux d'informations et de données à caractère sensible ou bien personnel pour les usagers. La sécurisation doit

également toucher les sites vitaux et les infrastructures stratégiques du pays. Il est vrai que la Défense nationale à travers la DGSSI (Direction générale de la sécurité des systèmes d'information) sécurise déjà les systèmes d'information publics mais les deux textes de loi vont offrir un cadre légal et réglementaire plus adapté aux contraintes et défis actuels. Il sera question avec l'entrée en vigueur de la loi de la mise en place au niveau des administrations concernées de dispositifs et services chargés notamment de la gestion, la prévention ainsi que la détection des risques dans le monde cybernétique sans oublier la confrontation et la gestion des situations de crise. En plus de ce premier texte, la Défense nationale a préparé un deuxième projet de loi relatif cette fois-ci aux services de confiance appliqués aux opérations dématérialisées. Ainsi, le texte selon le ministre délégué chargé de l'Administration de la défense nationale, va définir le système utilisé pour l'échange de données par voie électronique, la conformité avec les documents rédigés sur un support papier en plus des documents réalisés sur un support électronique. Le texte de loi couvre également les services de confiance qui concernent plusieurs prestations, notamment la réalisation, la vérification et l'authentification des signatures électroniques. Parmi les prestations citées, il y a également la vérification et le contrôle des cachets électroniques et l'horodatage électronique sans oublier la conservation de signatures et de cachets électroniques ainsi que la vérification et la validation

de certificats pour l'authentification de site internet. Aussi, le projet de loi va encadrer l'action des prestataires de services de confiance opérant sur le marché marocain à travers une série de règles obligatoires à respecter à la fois par les prestataires et les clients de services de confiance. A noter enfin que le ministre délégué chargé de l'Administration de la défense nationale annonce également l'organisation prochainement de la 7e édition du colloque annuel de la sécurité des systèmes d'information placée cette année sous le signe «Le support extérieur des systèmes d'information et les défis de la cybersécurité».

Le 2^{ème} projet de loi va définir le système utilisé pour l'échange de données par voie électronique, la conformité avec les documents rédigés sur un support papier en plus des documents réalisés sur un support électronique.

DGSSI



La Direction générale de la sécurité des systèmes d'information (DGSSI) avait été créée par décret N° 2-11-509. Elle est rattachée à l'Administration de la défense nationale. La DGSSI est notamment chargée de coordonner les travaux interministériels relatifs à l'élaboration et la mise en œuvre de la stratégie de l'Etat en matière de sécurité des systèmes d'information. Elle a, en outre, pour mission de veiller à l'application des directives et orientations du comité stratégique de la sécurité des

systèmes d'information ainsi que de certifier les dispositifs de création et de vérification de signature électronique et agréer les prestataires de service pour la certification électronique. Parmi ses missions également, mettre en place, en relation avec les départements ministériels, un système de veille, de détection, d'alerte des événements affectant ou susceptibles d'affecter la sécurité des systèmes d'information de l'Etat et coordonner les mesures devant être prises à cet effet.

Menaces cybernétiques sur le Maroc

Le géant russe de la cybersécurité Kaspersky a détecté au moins 4 cyberattaques ou tentatives d'attaques sur le Maroc durant les 24 derniers mois. Il s'agit d'APT (Advanced Persistent Threats) ou bien attaques informatiques prolongées.

Même si l'origine de ces attaques n'est pas connue les APT sont le plus souvent menées par des groupes bien structurés avec l'objectif de compromettre des systèmes d'information d'un pays

cible ou obtenir des informations confidentielles dans le cadre d'opération d'espionnage. En plus des risques visant des institutions publiques, les particuliers peuvent également être la cible de hackers dans le cadre d'opération de chantage ou carrément de vol d'argent via les applications électroniques. Le hic, c'est qu'un bon nombre de citoyens marocains demeure encore peu sensible aux risques encourus sur la Toile ainsi qu'aux règles de sécurité à observer.

