

CYBERSÉCURITÉ : QUELS DÉFIS POUR LE MAROC ?



AHMED YAACOBI (X88)
directeur Comexim NTIC

Les mesures adoptées par le Royaume chérifien pour le cyberspace ont permis de gagner 43 points et le classer 50^e à l'échelle mondiale, selon l'indice de la cybersécurité publié par l'Union internationale des télécommunications. C'est une orientation politique volontariste du Maroc, qui permet d'envisager l'avenir avec confiance.

La cybersécurité est un sujet de plus en plus important au Maroc comme dans le monde entier. De nombreuses entreprises et administrations dépendent de plus en plus de la technologie pour leur activité quotidienne. Protéger leurs données et leurs systèmes ainsi que les données personnelles et confidentielles des utilisateurs contre les cybermenaces devient crucial. En février 2022, le conflit ukrainien a ouvert la voie à un nouveau chapitre dans la guerre hybride, la cyberdéfense devient une priorité vitale.

La création d'une autorité nationale

Au Maroc, plusieurs mesures ont été prises pour renforcer la cybersécurité du pays. L'une des mesures phares est bien la création d'une agence nationale de cybersécurité : la DGSSI, la direction générale de la sécurité des systèmes d'information (autorité nationale en la matière), qui a pour mission de coordonner les efforts de lutte contre les menaces informatiques et de veiller à la protection des systèmes et des données du pays. Cette agence travaille en étroite collaboration avec les acteurs du secteur privé et les autorités compétentes pour renforcer la sécurité des réseaux et des systèmes informatiques au Maroc. La



© Who is Danny

DGSSI a pris un ensemble de mesures et mis en place des procédures à caractère stratégique, juridique, technique, opérationnel et de sensibilisation, visant à assurer un environnement numérique sûr et fiable garant de la réussite de la transition numérique au Maroc, ainsi qu'à améliorer et à consolider le niveau de confiance national et international dans les services numériques.

Un centre de veille et de coordination

Après la Directive nationale de la sécurité des systèmes d'information et la Stratégie nationale en sécurité des systèmes d'information, la DGSSI a publié ces deux dernières années une batterie de guides et référentiels et des bonnes pratiques en matière de cybersécurité, dont plusieurs restent encore à produire pour être aux standards internationaux. Le maCERT (*Moroccan Computer Emergency Response Team*) créé par la DGSSI est le centre de veille, détection et réponse aux attaques

Tremblement de terre et cybersécurité

Le dernier tremblement de terre tragique au Maroc, comme tout autre événement qui dégage une forte émotion et une avalanche en flux de communications à travers internet et les réseaux sociaux, représente une opportunité pour les cybercriminels cherchant à tirer profit de cette crise douloureuse.

Des escrocs utilisent le thème du « tremblement de terre » dans des campagnes de *phishing*, à travers le téléchargement de fichiers et de liens malveillants, afin de diffuser différents types de *malwares*, notamment des chevaux de Troie d'accès à distance et de vol d'informations.

C'est pour cela que le Royaume, fort des nouvelles structures de cyberdéfense qu'il a mises en place dernièrement, a diffusé dès les premiers jours une campagne de sensibilisation des grandes entreprises et de la population sur ce risque à travers la DGSSI créée pour cette mission. Alors, comment le Maroc est arrivé à ce niveau de cybersécurité et quelle évaluation peut-on en faire ?

informatiques. Il est chargé de la mise en œuvre, en relation avec les autres administrations, de systèmes de veille, de détection, d'alerte des événements susceptibles d'affecter la sécurité des systèmes d'information de l'État et de la coordination de la réaction à ces événements. Le maCERT est une source précieuse d'informations sur les différentes menaces qui frappent aux portes.

Des initiatives publiques et privées

En 2021, la loi n° 05-20 sur la cybersécurité a été adoptée pour renforcer les exigences et installer des normes pour les grandes entreprises publiques et privées, vitales pour l'économie et la souveraineté nationale. Toutefois au niveau PME un grand retard reste à combler. Déjà, bien avant, le Maroc avait adopté plusieurs lois et règlements pour protéger les données personnelles et la vie privée des citoyens, notamment la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette loi vise à assurer une protection efficace des particuliers contre les abus d'utilisation des données, de nature à porter atteinte à leur vie privée, et à harmoniser le système marocain de protection des données personnelles avec ceux de ses partenaires notamment européens. En outre, la loi institue une Commission nationale de contrôle de la protection des données personnelles. En plus des efforts gouvernementaux, de nombreuses entreprises au Maroc prennent des mesures de sécurité prioritaires pour protéger leurs données et leurs systèmes. D'ailleurs, plusieurs ont déjà mis en œuvre des certifications comme l'ISO 27001. À titre de performance exemplaire, notons IMDAE, la plateforme *cloud* de Barid Media, filiale de Poste Maroc, qui est la seule plateforme de signature électronique au monde à assurer la confidentialité totale de ses données (fichiers signés sans *upload*).

Une coopération interétatique et industrielle

Cette volonté du Maroc de faire de la cybersécurité une priorité attire les pays alliés pour une coopération plus étroite dans ce domaine. C'est ainsi que la cyberdiplomatie au Maroc est devenue un axe politique très animé ces dernières années. 2022 a connu la signature de plusieurs partenariats stratégiques en plus de celui avec le Royaume-Uni : avec Tel-Aviv par exemple, et la signature du 2^e protocole additionnel à la Convention de Budapest. Plus tôt cette année, un « Centre d'excellence en cybersécurité pour l'Afrique » a été lancé dans le cadre d'un projet conjoint entre le Royaume-Uni et le Maroc. De même l'implantation de géants mondiaux, tels que Thales, Orange cyberdefense ou Atos, a vocation à

favoriser la mise en place d'un *hub* de cybersécurité pour servir leurs clients aussi bien régionaux en Afrique et Moyen-Orient que plus largement au niveau européen et mondial. À titre d'exemple Thales vient d'ouvrir un nouveau centre opérationnel de cybersécurité (SOC) au Maroc. Sixième au sein de son réseau international, après ceux du Canada, de France, de Hong Kong, des Pays-Bas, du Royaume-Uni, ce centre permet de bénéficier d'une protection en temps réel contre les cyberattaques.

Relever les défis contemporains

Toutefois, de nombreux défis en matière de cybersécurité restent à relever, dans une industrie et une technologie qui évoluent constamment, pour faire face aux menaces en ligne croissantes en matière d'attaque et de défense. Voici des exemples de nouvelles tendances et développements dans le domaine de la cybersécurité. L'IA et l'apprentissage automatique sont de plus en plus utilisés pour attaquer comme pour détecter et prévenir les cyberattaques, en analysant les données en temps réel et en identifiant les anomalies. La cybersécurité de l'IoT (internet des objets) est devenue un risque de plus en plus important, car de nombreux appareils connectés sont vulnérables aux attaques en ligne. Le développement du télétravail et les réponses aux risques et soucis sécuritaires sont en constante mutation. Les attaques de *ransomware* ont augmenté en fréquence et en sophistication, ce qui a conduit à la création de nouvelles technologies pour protéger les données et les systèmes. Le *phishing* reste l'une des principales méthodes utilisées par les cybercriminels pour accéder aux informations sensibles des utilisateurs. De nouvelles solutions de protection contre le *phishing* sont requises. L'évolution de la gestion des identités et des accès (*Identity and Access Management*, IAM) est devenue un enjeu important pour gérer et protéger les accès aux données et aux systèmes. Il est donc primordial pour le Maroc de rester à jour des dernières tendances et développements en matière de cybersécurité et de faire preuve d'agilité pour prendre les mesures de sécurité nécessaires et adéquates. Cette agilité et cette réactivité nécessaires pour relever les défis futurs restent le plus grand souci des acteurs marocains, qui ont réussi jusqu'à présent avec un peu de baraka à déjouer des attaques graves qui sont dignes de films hollywoodiens et qui sont restées discrètes et confidentielles. La cybersécurité est un secteur d'innovation en constante évolution ; la coconstruction d'un écosystème par des programmes appuyés par l'État, le privé et les partenariats internationaux peut faire émerger un savoir-faire technologique capable d'affronter les menaces futures. X

*“Un
savoir-faire
technologique
capable
d'affronter
les menaces
futures.”*