ROYAUME DU MAROC
Administration
de la Défense Nationale

المملكة المغربية
إدارة الدفاع الوطني

STRATEGIE NATIONALE
EN MATIERE DE CYBERSECURITE

Sommaire

Sa Majesté le ROI Mohammed VI a présidé la réunion d'adoption du plan « Maroc Numeric 2013 » avec comme fondement la confiance numérique.

Introduction

Les systèmes d'information font aujourd'hui partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises et du mode de vie des citoyens. Désormais, ils sont devenus indispensables et incontournables.

Sécuriser et contrôler l'information véhiculée par les systèmes d'information devient un enjeu de plus en plus pressant dans un monde où l'environnement lié aux technologies de l'information et de la communication est de plus en plus la cible de diverses menaces.

En effet, les attaques informatiques se multiplient sous toutes les formes contre les systèmes d'information des pays. Le nombre croissant des violations de la sécurité a déjà provoqué des dommages financiers et sécuritaires considérables et représente l'une des menaces majeures à moyen et long termes.

Dans ce contexte, et compte tenu des enjeux et risques liés à la perspective d'ouverture et de développement projeté par le plan «Maroc Numeric 2013»*, notre pays se trouve désormais, d'une part, devant l'obligation de mettre en place des mécanismes de protection et de défense des systèmes d'informations (SI) des administrations, organismes publics et infrastructures d'importance vitale et d'autre part, de sensibiliser les entreprises et les citoyens sur les enjeux et les risques liés aux menaces informatiques.

Pour ce faire, l'Etat a décidé de renforcer les capacités nationales en matière de sécurité des systèmes d'informations des administrations, organismes publics et infrastructures d'importance vitale. La création du Comité Stratégique de la Sécurité des Systèmes d'Informations (CSSSI) et de la Direction Générale de la Sécurité des Systèmes d'Informations (DGSSI), ont été les premières étapes de cet engagement.

Dans le même sillage et conformément au décret n° 2-11-508 du 22 chaonal 1432 (21 septembre 2011) portant création du CSSSI, la présente stratégie a été établie en vue d'assurer la protection des systèmes d'informations des administrations, organismes publics et infrastructures d'importance vitale.

De l'intérêt accordé à la sécurité numérique au Maroc

L'adoption des technologies du numérique, la dépendance du secteur public et privé de ces mêmes technologies et l'interdépendance des infrastructures critiques introduisent un degré de vulnérabilité* non négligeable dans le fonctionnement normal des institutions. Ceci peut mettre en péril leur pérennité ainsi que la souveraineté des Etats.

Aujourd'hui, les cyberattaques* peuvent avoir pour objectif de voler des données, d'endommager ou d'altérer le fonctionnement normale des SI et ont toutes des conséquences négatives pour les organisations ou individus qui en sont victimes.

A cet effet, le Ministère chargé des nouvelles technologies a diligenté une enquête qui a porté sur un échantillon comprenant une cinquantaine d'organismes marocains, dont principalement des acteurs du gouvernement, de la banque, de l'informatique, de l'énergie, etc. Cette enquête complétée par une démarche d'entretiens spécifiques avait mis en lumière les points suivants :

• L'intérêt porté pour le développement des technologies de l'Information au Maroc : l'Internet est utilisé par la quasi-totalité des organismes (près de 95%) et leurs sites Internet sont considérés comme ayant un impact potentiel fort sur l'image de leurs organisations ;

• Les attentes exprimées par les organismes par rapport à la future stratégie nationale : ces attentes se rapportent en premier lieu à la mise en place d'organisations autour de la sécurité des systèmes d'information. Qu'il s'agisse d'un organisme permettant d'échanger sur le sujet entre responsables informatiques ou d'autorités nationales de veille et de diffusion d'information, les résultats obtenus dépassaient tous les 80% d'opinions favorables.

A cet effet et partant d'une vision et d'ambitions claires, visant à positionner le Maroc parmi les pays émergents dynamiques dans les technologies de l'information et de la communication, le Maroc a lancé, sous la présidence effective de SA MAJESTE LE ROI en octobre 2009 la stratégie «Maroc Numeric 2013». Cette stratégie a retenue la confiance numérique* et partant la cybersécurité en tant que mesure d'accompagnement indispensable à l'ancrage du Maroc à l'économie numérique.

Pour instaurer cette confiance, il est nécessaire d'apporter une réponse adéquate aux dimensions humaine, juridique, économique et technologique des besoins de sécurité des infrastructures numériques et des utilisateurs. Cette confiance pourrait s'instaurer et générer un développement économique profitable à tous les acteurs de la société.

Vers une stratégie de la sécurité des systèmes d'information au Maroc

1.1 FONDEMENTS STRATEGIQUES

Pour mettre en place une démarche de cybersécurité conformément aux orientations de l'Union Internationale des Télécommunications, il est important de pouvoir identifier correctement les valeurs et les biens à protéger afin de circonscrire le périmètre de sécurité à mettre en place. Ceci implique une approche globale, pluridisciplinaire et systémique de la sécurité.

La cybersécurité doit s'appréhender d'une manière globale car il ne suffit pas de protéger les informations lors de leur transfert mais aussi lorsqu'elles sont traitées et stockées. Des solutions de sécurité d'ordre uniquement technologique ne peuvent pas suppléer à un manque de gestion cohérente et rigoureuse des besoins, mesures, procédures et outils de la sécurité.

La définition d'une stratégie de sécurité des systèmes d'information passe par :

• La prise en compte de l'analyse des risques* liés au cyberespace* selon un processus dynamique et continu pour guider la démarche de sécurité préconisée ;

• La définition d'une Politique de Sécurité des Systèmes d'Information (PSSI)* permettant de traduire la compréhension des risques encourus et de leurs impacts en des mesures de sécurité à implémenter ;

• Le déploiement de solutions à même de sécuriser les systèmes informatiques et les infrastructures de télécommunications ;

• La mise en place d'une démarche de détection et de réaction aux menaces.

• La mise en place d'un cadre légal approprié ;

• L'encouragement de la recherche et le développement dans le domaine de la sécurité des SI ainsi que l'obligation du respect d'un minimum de normes* ;

• La sensibilisation de l'ensemble des acteurs afin de promouvoir une culture de la cybersécurité.

1.2 PRIORITES STRATEGIQUES

La cybersécurité comporte de nombreuses dimensions. Les diverses façons d'appréhender la sécurité des SI donnent lieu à de nouvelles orientations en matière de formation, de pratiques opérationnelles, de contrôle et de législation.

Dans ce contexte et en réponse à la nécessité pressante d'une stratégie claire de cybersécurité, quatre axes stratégiques ont été retenues, à savoir :

• L'évaluation des risques pesant sur les systèmes d'information au sein des administrations, organismes publics et infrastructures d'importance vitale ;

La protection et la défense des systèmes d'information des administrations, organismes publics et infrastructures d'importance vitale ;

Le renforcement des fondements de la sécurité : Cadre juridique, Sensibilisation, Formation et Recherche & Développement ;

La promotion et le développement de la coopération nationale et internationale.

1.2.1 L'évaluation des risques pesant sur les systèmes d'information au sein des administrations, organismes publics et infrastructures d'importance vitale

Avant la mise en place de mesures préventives de sécurité, il faut procéder à une analyse des risques pour pouvoir estimer les pertes potentielles liées à une défaillance de la disponibilité, de l'intégrité ou encore de la confidentialité des données sans pour autant perdre de vue que l'impact majeur est souvent la perte de renommée et de la confiance en l'entité concernée.

La mise en œuvre cohérente et efficace de systèmes sécurisés au sein de l'Etat exige l'adoption de méthodes d'analyse de risques, de politiques et de standards de sécurité cohérents et adaptés aux contextes. Les mesures de sécurité organisationnelles et techniques décrites dans ces politiques et standards doivent être appliquées par les différentes administrations, organismes publics et infrastructures d'importance vitale.

L'évaluation des risques est un préalable à l'élaboration des directives et à la définition des axes d'efforts permettant d'aider les responsables à tous les niveaux à protéger leurs systèmes d'information.

Cet axe sera mis en œuvre selon deux programmes :

i. Élaborer des plans d'évaluation des risques et menaces

• Définir une grille d'évaluation du degré de criticité des SI des administrations, organismes publics et infrastructures d'importance vitale ;

• Recenser, identifier et classifier les SI des administrations, organismes publics et infrastructures d'importance vitale ;

• Évaluer périodiquement le niveau du risque pesant sur les SI des administrations, organismes publics et infrastructures d'importance vitale ;

• Evaluer les plans de gestion du risque adoptés par les administrations, organismes publics et infrastructures d'importance vitale ;

• Identifier les SI des administrations et des organismes publics devant être supervisés par le maCERT*.

ii. Mettre en place des outils d'aide à la prise de décision

• Mener des enquêtes pour collecter des données d'ordres juridiques, techniques et procédurales ayant trait à la sécurité des SI ;

• Produire des données statistiques et des indicateurs de suivi ;

• Assurer la veille technologique, juridique et réglementaire.

1.2.2 La protection et la défense des systèmes d'information des administrations, organismes publics et infrastructures d'importance vitale.

Les SI exigent une protection matérielle et immatérielle contre tous types de menaces. Toutefois, il faut partir du constat qu'aucun système d'information, quelque soit son niveau de protection, n'est parfaitement sécurisé. Dès lors, il est nécessaire de se doter de capacités suffisantes pour détecter les intrusions et pour réagir en cas de détection d'incident, de le traiter de manière efficace et de rétablir rapidement l'opérabilité

des systèmes affectés.

Cet axe sera mis en œuvre selon trois programmes :

i. Élaboration de référentiels et de normes nationaux

• Identifier les normes et les meilleures pratiques de sécurité des technologies de l'information ;

• Définir la Politique de la Sécurité des Systèmes d'Information (PSSI) nationale au profit des administrations, organismes publics et infrastructures d'importance vitale ;

• Élaborer des guides et des référentiels pour implémenter des politiques de sécurité des systèmes d'information spécifiques.

ii. Renforcer la sécurité des SI des administrations, organismes publics et infrastructures d'importance vitale

• Veiller à la mise en œuvre de la PSSI ;

• Etudier la faisabilité et initier la mise en place progressive d'un réseau de transmission interministériel sécurisé ;

• Impliquer les opérateurs et les fournisseurs de services Internet dans la sécurité des SI ;

• Amener les administrations, les organismes publics et les infrastructures d'importance vitale à se faire auditer en vue d'être certifié ISO27001 ou équivalent.

iii. Renforcer les structures de veille, de détection et de réponse aux incidents informatiques

• Renforcer les capacités du maCERT pour offrir les principaux services et intégrer le maximum de parties prenantes, conformément aux standards internationaux ;

• Inciter les administrations, les organismes publics les infrastructures d'importance vitale en fonction de l'envergure de leurs SI à avoir des points focaux ou à mettre en place des Centres Opérationnels de Sécurité

(SOC)* des Systèmes d'Information ;

• Formaliser et mettre en œuvre les mécanismes d'échange d'informations relatifs aux traitements des alertes et des incidents entre le maCERT et les parties prenantes.

1.2.3 Le renforcement des fondements de la sécurité : Cadre juridique, Sensibilisation, Formation, et Recherche & Développement

L'évolution rapide des technologies, des infrastructures et des systèmes de communication et de traitement de l'information génère de nouvelles menaces. Il est dès lors primordial de vérifier régulièrement si les bases légales en vigueur sont toujours adaptées.

La nécessité d'une veille juridique découle, par ailleurs, du caractère transfrontalier des actes criminels qui remet en cause, dans une certaine mesure, le principe de l'application territoriale des règles légales.

Il est important d'élaborer aussi des programmes d'éducation et de formation spécifiques à la sécurité des SI. Les responsables devraient pouvoir acquérir les compétences nécessaires pour participer activement à la compréhension et à la résolution des cyber-menaces.

La recherche et développement doit assurer une autonomie acceptable et contribuer à une sécurité en profondeur des SI. Dans ce sillage, les technologies de tout premier plan et dont la maîtrise est cruciale reste celles des systèmes d'exploitation et la cryptographie.

Cet axe sera mis en œuvre selon quatre programmes :

i. Renforcer le cadre juridique pour instaurer la confiance numérique

• Mettre à niveau le cadre légal et réglementaire pour prendre en compte les exigences spécifiques de la sécurité des SI notamment ceux relatifs aux prestations de certification électronique* et à la cryptographie;

• Examiner les recommandations des institutions régionales et internationales pour une éventuelle application dans la réglementation nationale.

ii. Identifier et organiser des programmes de formation aux questions techniques et juridiques que pose la cybersécurité

• Définir les profils de compétence adéquats dans le domaine de la cybersécurité ;

• Arrêter les programmes de formation en cybersécurité et veiller à leur application ;

• Promouvoir le développement et la distribution des supports éducatifs.

iii. Sensibiliser sur la cyber-éthique et les menaces et risques liés à la sécurité des SI

• Mettre en œuvre des programmes de sensibilisation à la sécurité des systèmes d'information ;

• Sensibiliser la population notamment les enfants et les utilisateurs individuels sur la cyber-éthique et les menaces et risques liés à la sécurité des SI.

iv. Soutenir la recherche et le développement de produits de la sécurité des SI nationaux pour garantir l'autonomie scientifique et technique

• Encourager le développement de solutions nationales dans le domaine de la sécurité informatique ;

• Recenser les travaux de recherche universitaires dans le domaine de la sécurité des S***I*** et suivre de près leur évolution ;

• Identifier les experts nationaux et internationaux qui pourraient apporter une assistance pour résoudre les problèmes de cybersécurité.

1.2.4 La promotion et le développement de la coopération nationale et internationale

La nécessité d'une coopération que ce soit sur le plan national ou international découle du caractère par essence mondial des réseaux de communication.

Sur le plan national, une coopération et une interaction effectives entre tous les acteurs concernés est nécessaire pour disposer d'une stratégie cohérente.

Sur le plan international, le dialogue sur la cybersécurité devrait promouvoir l'échange d'expérience, l'identification et l'application de règles et normes compatibles.

Cet axe sera exécuté selon deux programmes :

i. Identifier les thématiques et mécanismes de coopération

• Identifier les programmes et les thématiques de coopération

• Explorer les possibilités offertes en matière de coopération avec les milieux universitaires, organismes de régulation, secteurs privés, etc. ;

• Identifier et établir les mécanismes et les modalités de la coopération.

ii. Conclure des partenariats et les mettre en œuvre

• Nouer des partenariats avec les acteurs identifiés dans le domaine de la sécurité des SI ;

• Mettre en œuvre et évaluer les programmes de coopération.

Conclusion

En conclusion, la présente stratégie définit les grandes lignes des programmes et chantiers qui devront être lancés. Elle sera déclinée en plans d'actions opérationnels. Ces plans devront pour chaque programme décrire les mesures concrètes à mettre en œuvre suivant un calendrier déterminé tout en précisant les acteurs appelés à contribuer à leur accomplissement selon des objectifs quantifiés.

Afin de créer les conditions favorables à l'exécution des plans d'action opérationnels, les acteurs impliqués dans l'élaboration de la stratégie nationale de cybersécurité seront associés à la définition de ces plans tout en accordant une attention particulière à leurs besoins, priorités et contraintes.

Cette stratégie sera périodiquement révisée afin d'être adaptée, en cas de besoin, aux nouvelles réalités et exigences.

Glossaire

Analyse des risques

Ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque afin d'améliorer la sécurisation des SI, de justifier le budget alloué à la sécurisation du SI et prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Cyberdéfense

Ensemble des mesures techniques et non-techniques permettant à un État de contrer les cyberattaques.

Cybersécurité

Situation recherchée pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises.

Cybercriminalité

Toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau.

Cyberattaques

Actes malveillants envers un dispositif informatique, généralement via un réseau de télécommunications.

Confiance Numérique

Permet de mesurer à quel point les internautes se fient à la vie numérique.

Cyberespace

Ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.

Certificat électronique

Est un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire.

Centre Opérationnel de Sécurité (SOC)

Une plateforme dont la fonction est de fournir des services de détection des incidents de sécurité et de fournir des services pour y répondre.

Politique de Sécurité des Systèmes d'Information

Ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.

Normes

Document de référence contenant des spécifications techniques précises destiné à être utilisé comme règles ou lignes directrices.

maCERT

Center Emergency Response Team ou Centre de Veille, de Détection et de Réaction aux Attaques Informatiques au Maroc.

Maroc Numeric 2013

Stratégie Nationale pour la Société de l'Information et de l'Économie Numérique au Maroc d'ici 2013.

Système d'information (SI)

Est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné.

Vulnérabilité

Faille de sécurité dans un programme ou sur un système informatique.