Décret n° 2-15-712 du 12 joumada II 1437 (22 mars 2016) fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale.

LE CHEF DU GOUVERNEMENT,

Vu le dahir n° 1-12-04 du 14 rabii I 1433 (7 février 2012) portant délégation de pouvoir en matière d'Administration de la défense nationale ;

Vu le décret n° 2-11-508 du 22 chaoual 1432 (21 septembre 2011) portant création du comité stratégique de la sécurité des systèmes d'information notamment son article premier ;

Vu le décret n° 2-82-673 du 28 rabii I 1403 (13 janvier 1983) relatif à l'organisation de l'Administration de la défense nationale et portant création de la Direction générale de la sécurité des systèmes d'information, tel qu'il a été complété par le décret n° 2-11-509 du 22 chaoual 1432 (21 septembre 2011), notamment son article 7 *quater* ;

Vu la circulaire du Chef du gouvernement n° 3/2014 du 8 joumada I 1435 (10 mars 2014) relative à la directive nationale de la sécurité des systèmes d'information ;

Après délibération en Conseil du gouvernement, réuni le 3 rabii II 1437 (14 janvier 2016) ;

Après délibération en Conseil des ministres, réuni le 26 rabii II 1437 (6 février 2016),

DÉCRÈTE :

ARTICLE PREMIER. – Au sens du présent décret, on entend par :

« Infrastructures d'importance vitale » : Installations, ouvrages et systèmes qui sont indispensables au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social, et dont le dommage ou l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions.

« Secteur d'activités d'importance vitale » : Constitué d'activités concourant à un même objectif. Ces activités ont trait soit à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, ou à l'exercice des prérogatives de l'Etat, ou au fonctionnement de l'économie, ou au maintien des capacités de sécurité du pays, dès lors que ces activités sont difficilement substituables ou remplaçables, ou qui peuvent présenter un danger grave pour la population.

« Information sensible » : Information dont la compromission, l'altération, le détournement ou la destruction est de nature à nuire à la continuité du fonctionnement ou mettant en danger le patrimoine informationnel de l'infrastructure d'importance vitale.

« Système d'information sensible d'une infrastructure d'importance vitale » :

Système d'information traitant des informations sur lesquelles une atteinte à la confidentialité, à l'intégrité ou à leur disponibilité porterait préjudice à la continuité de fonctionnement de l'infrastructure d'importance vitale.

« Autorité compétente » : Autorité gouvernementale chargée de l'administration de la défense nationale (Direction générale de la sécurité des systèmes d'information).

ART. 2. – Champ d'application

Le présent décret s'applique aux administrations, établissements et entreprises publics et organismes disposant d'un agrément ou d'une licence de l'Etat pour exercer une activité réglementée, considérés comme des infrastructures d'importance vitale et disposant de systèmes d'information sensibles. Ces infrastructures sont désignées ci-après sous le terme « entité ».

ART. 3. – Délimitation des secteurs d'activités et des infrastructures d'importance vitale

La liste des secteurs d'activités d'importance vitale et des autorités gouvernementales ou établissements publics ou personnes morales de droit public assurant la coordination de ces secteurs est fixée en annexe du présent décret.

Les infrastructures d'importance vitale visées à l'article 2 du présent décret sont désignées pour chaque secteur d'activités d'importance vitale par l'autorité gouvernementale ou l'établissement public ou la personne morale de droit public assurant la coordination de ce secteur.

La liste de ces infrastructures doit être tenue secrète et son contenu doit faire l'objet d'un réexamen au moins une fois par an.

ART. 4. – Identification et recensement des systèmes d'information sensibles des infrastructures d'importance vitale

Chaque entité établit, sur la base des résultats d'une analyse des risques, un répertoire contenant les listes de ses systèmes d'information sensibles tels que définis à l'article premier ci-dessus, et le communique à l'autorité compétente dans un délai maximum de 12 mois après la publication du présent décret au «Bulletin officiel».

L'autorité compétente fixe les modalités régissant la classification des systèmes d'information.

Chaque entité doit notifier à l'autorité compétente tout changement affectant la liste de ses systèmes d'information sensibles.

Les listes et les répertoires des systèmes d'information sensibles des infrastructures d'importance vitale sont tenus secrets.

Chaque entité doit désigner un responsable de la sécurité de ces systèmes qui sera le point de contact vis-à-vis de l'autorité compétente.

ART. 5. – Application de la directive nationale de la sécurité des systèmes d'information et des règles de sécurité sectoriels

Chaque entité veille à ce que ses systèmes d'information sensibles soient conformes aux règles prescrites par la directive nationale de la sécurité des systèmes d'information et les standards de sécurité édictées par l'autorité compétente et applicables aux systèmes d'information sensibles des infrastructures d'importance vitale.

L'autorité compétente peut prévoir des règles de sécurité particulières à un secteur ou type d'activité de l'entité. Cette autorité notifie aux entités les délais requis pour les appliquer.

Les règles de sécurité identifiées par l'autorité compétente peuvent être appliquées au secteur privé dans le cadre des conventions conclues avec ce secteur.

ART. 6. – Déclaration et traitement des incidents de sécurité

Chaque entité doit mettre en place les moyens nécessaires pour la supervision et la détection des Cyberattaques. Les données techniques générées par ces moyens sont exploitées par le Centre de veille, de détection et de réponse aux attaques informatiques (ma-CERT) relevant de la direction Générale de la Sécurité des Systèmes d'Information désigné ci-après par centre.

Chaque entité doit communiquer, dans les quarante-huit heures, au ma-CERT les informations relatives aux incidents majeurs affectant la sécurité ou le fonctionnement de leurs systèmes d'information sensibles. Elle doit également fournir au centre les informations complémentaires concernant l'incident, demandées par ledit centre.

L'autorité compétente précise les informations qui doivent être communiquées, les modalités de leur transmission ainsi que les types d'incidents concernés.

En cas d'incident majeur, l'autorité compétente doit transmettre, dans le mois qui suit, à l'entité concernée et à l'autorité gouvernementale ou à l'établissement public ou à la personne morale de droit public assurant la coordination du secteur d'activités d'importance vitale, une synthèse des informations recueillies et des recommandations qui en découlent.

Pour faire face aux crises majeures menaçant ou affectant la sécurité des systèmes d'information sensibles, l'autorité compétente peut fixer des mesures que les entités doivent mettre en œuvre.

L'autorité compétente préserve la confidentialité des informations qu'elle recueille auprès des entités mentionnées à l'article 2 susvisé dans le cadre de l'application des dispositions de cet article.

ART. 7. – Audit de la sécurité des systèmes d'information

Les entités mentionnées à l'article 2 susvisé soumettent, conformément au programme des missions d'audit arrêté par l'autorité compétente, leurs systèmes d'information sensibles à un audit effectué par la Direction générale de la sécurité des systèmes d'information ou par des prestataires privés homologués par l'autorité compétente.

Un arrêté du Chef du gouvernement fixe les critères d'homologation des prestataires d'audit privés ainsi que les modalités de déroulement de l'audit.

L'autorité compétente notifie à l'autorité gouvernementale, à l'établissement public et à la personne morale de droit public assurant la coordination du secteur d'activités d'importance vitale le programme des missions d'audit de sécurité des systèmes d'information. Elle précise, en fonction de la nature des opérations à mener, si cet audit sera effectué par la Direction générale de la sécurité des systèmes d'information ou par des prestataires privés homologués par l'autorité compétente.

Lorsque les audits sont effectués par les prestataires privés homologués, les coûts de ces opérations sont imputés sur le budget de l'entité concernée. Dans tous les cas, les audits sont menés sous la supervision de l'autorité compétente.

A l'issue de chaque opération d'audit, la Direction générale de la sécurité des systèmes d'information ou le prestataire privé homologué rédige un rapport exposant ses constatations et formulant ses recommandations sur le niveau de sécurité des systèmes d'information de l'entité concernée et sur le respect par cette dernière des règles et standards de sécurité prévues par le présent décret.

Lorsque l'audit est effectué par un prestataire privé homologué, les conclusions de cette opération sont communiquées par l'entité concernée à la Direction générale de la sécurité des systèmes d'information.

Les conclusions du rapport d'audit sont communiquées par la Direction générale de la sécurité des systèmes d'information à l'entité concernée et à l'autorité gouvernementale ou à l'établissement public ou à la personne morale de droit public assurant la coordination du secteur d'activités d'importance vitale.

Les entités concernées doivent mettre en place un plan d'actions pour mettre en œuvre les recommandations figurant dans les rapports d'audit. A l'effet du suivi de sa mise en œuvre, chaque entité communique son plan d'actions à la direction générale de la sécurité des systèmes d'information.

ART. 8. – Plan de continuité et de reprise d'activités

Chaque entité doit préparer un plan de continuité et de reprise d'activités intégrant l'ensemble des solutions de secours pour neutraliser les interruptions des activités, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

Chaque entité doit préparer un plan technique de continuité et de reprise d'activités intégrant l'ensemble des solutions de secours informatique. Ce plan doit être testé annuellement, afin de le mettre à jour en fonction des évolutions propres de l'infrastructure et de l'évolution des menaces.

Toute personne en charge d'une action relevant du plan de continuité et de reprise d'activités doit connaître précisément son rôle et ce qu'elle doit faire concrètement en cas d'incident. Elle doit également comprendre la finalité recherchée, afin d'inscrire son action dans la cohérence globale de l'entité.

ART. 9. – Externalisation des systèmes d'information

En cas d'externalisation d'un système d'information sensible, le respect de la directive nationale de la sécurité des systèmes d'information et des règlements ou référentiels techniques relatifs à la sécurité des systèmes d'information des infrastructures d'importance vitale par les tiers est obligatoire.

Toute externalisation de service applicatif d'une entité doit faire l'objet d'un contrat de droit marocain. Le contrat doit intégrer impérativement des engagements de protection de l'information, d'auditabilité et de réversibilité. Les exigences de sécurité et les niveaux de service voulus doivent être inclus de façon précise dans les contrats conclus.

L'hébergement des données sensibles des entités sur le territoire national est obligatoire.

L'autorité compétente fixe le référentiel technique régissant la sécurité relative à l'externalisation des systèmes d'information.

ART. 10. – Prise en compte de la sécurité des systèmes d'information dans les achats et la maintenance

Chaque entité doit intégrer, dans les dossiers de consultation et de maintenance des systèmes d'information sensibles, des dispositions relatives aux exigences de sécurité de ces systèmes.

L'autorité compétente fixe les exigences de sécurité à respecter par les entités lors de la rédaction des plans de maintenance et des dossiers de consultation.

ART. 11. – Accompagnement et assistance des entités

La direction générale de la sécurité des systèmes d'information accompagne et assiste les entités pour appliquer les dispositions du présent décret.

ART. 12. – Le présent décret est publié au *Bulletin officiel*.

Fait à Rabat, le 12 joumada II 1437 (22 mars 2016).

ABDEL-ILAH BENKIRAN.

*

* *

ANNEXE

Liste des secteurs d'activités d'importance vitale et autorités gouvernementales ou établissements publics ou personnes morales de droit public chargés d'assurer la coordination des secteurs

SECTEURS	AUTORITES GOUVERNEMENTALES OU ETABLISSEMENTS PUBLICS OU PERSONNES MORALES DE DROIT PUBLIC CHARGES D'ASSURER LA COORDINATION DES SECTEURS
SECURITE PUBLIQUE	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INTERIEUR
JUSTICE	AUTORITE GOUVERNEMENTALE CHARGEE DE LA JUSTICE
LEGISLATION	SECRETARIAT GENERAL DU GOUVERNEMENT
SECTEUR DES FINANCES	AUTORITE GOUVERNEMENTALE CHARGEE DES FINANCES
INDUSTRIE	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INDUSTRIE
SANTE	AUTORITE GOUVERNEMENTALE CHARGEE DE LA SANTE
AUDIOVISUEL ET COMMUNICATION	AUTORITE GOUVERNEMENTALE CHARGEE DE LA COMMUNICATION
PRODUCTION ET DISTRIBUTION DE L'ENERGIE, ET MINES	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INTERIEUR AUTORITE GOUVERNEMENTALE CHARGEE DE L'ENERGIE ET DES MINES
RESEAUX DES TRANSPORTS	AUTORITE GOUVERNEMENTALE CHARGEE DES TRANSPORTS
APPROVISIONNEMENT ET DISTRIBUTION D'EAU	AUTORITE GOUVERNEMENTALE CHARGEE DE L'INTERIEUR AUTORITE GOUVERNEMENTALE CHARGEE DE L'EAU
SERVICES POSTAUX	AUTORITE GOUVERNEMENTALE CHARGEE DES POSTES
SECTEUR BANCAIRE	BANK AL-MAGHRIB
TELECOMMUNICATIONS	AGENCE NATIONALE DE REGLEMENTATION DES TELECOMMUNICATIONS
SECTEUR DES MARCHES FINANCIERS	AUTORITE MAROCAINE DU MARCHE DES CAPITAUX
SECTEUR DES ASSURANCES	AUTORITE DE CONTROLE DES ASSURANCES ET DE LA PREVOYANCE SOCIALE

Le texte en langue arabe a été publié dans l'édition générale du «Bulletin officiel» n° 6456 du 6 rejeb 1437 (14 avril 2016).