Arrêté du Chef du gouvernement fixant les critères d'homologation des prestataires d'audit privés des systèmes d'information sensibles des infrastructures d'importance vitale ainsi que les modalités de déroulement de l'audit

Arrêté du Chef du gouvernement n° 3-44-18 du 21 safar 1440 (31 octobre 2018) fixant les critères d'homologation des prestataires d'audit privés des systèmes d'information sensibles des infrastructures d'importance vitale ainsi que les modalités de déroulement de l'audit[1].

LE CHEF DU GOUVERNEMENT,

Vu le dahir n° 1-17-08 du 21 rejeb 1438 (19 avril 2017) portant délégation de pouvoir en matière d'administration de la défense nationale;

Vu le décret n° 2-82-673 du 28 rabii I 1403 (13 janvier 1983), tel qu'il a été modifié et complété notamment par le décret n° 2-11-509 du 22 chaoual 1432 (21 septembre 2011) 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 ;

Vu le 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 et notamment son article 7,

Arrête

Chapitre premier : Dispositions générales

Article premier

Conformément aux dispositions de l'article 7 du décret n° 2-15-712 cité ci-dessus, cet arrêté fixe les critères d'homologation des prestataires

[1] - Bulletin Officiel n° 6732 du 28 rabii I 1440 (6-12- 2018), p 1913.

- Le texte en langue arabe a été publié dans l'édition générale du " Bulletin officiel " n° 6727 du 11 rabii I 1440 (19 novembre 2018).

d'audit privés des systèmes d'information sensibles des infrastructures d'importance vitale ainsi que les modalités de déroulement de l'audit.

Article 2

Au sens du présent arrêté, on entend par :

Autorité compétente : autorité gouvernementale chargée de l'Administration de la défense nationale (direction générale de la sécurité des systèmes d'information) ;

Prestataire d'audit : société établie selon le droit marocain, délivrant une ou toutes les prestations d'audit des systèmes d'informations. Cet audit peut selon le cas être : un audit organisationnel et physique, un audit d'architecture, un audit de configuration, un audit de code source, tests d'intrusion, ou un audit des systèmes industriels ;

Audit organisationnel et physique : consiste à s'assurer que les politiques et procédures de sécurité définies et mises en place par l'entité auditée sont conformes aux directives nationales de la sécurité des systèmes d'information et aux normes et standards en la matière ;

Audit d'architecture : consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information, aux pratiques en vigueur, aux exigences et aux règles internes de l'entité auditée ;

Audit de configuration : permet de vérifier la mise en oeuvre de pratiques de sécurité conformes aux pratiques en vigueur et aux exigences de sécurité et règles internes de l'entité auditée en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information ;

Audit de code source : consiste en l'analyse de tout ou partie du code source ou des conditions de compilation d'une solution logicielle dans le but de s'assurer du respect des règles précises du codage ou d'analyser les vulnérabilités liées au développement ;

Test d'intrusion : permet d'évaluer la sécurité d'un système d'information ou d'un réseau en simulant les conditions réelles d'une attaque sur le système d'information. Ce test permet de découvrir des vulnérabilités sur le système d'information d'une entité auditée et de vérifier leur exploitabilité et leur impact sur l'entité ;

Audit des systèmes industriels : consiste en l'évaluation du niveau de sécurité d'un système industriel et des dispositifs de contrôle associés. Il se compose d'un audit d'architecture, d'un audit de la configuration des éléments composant l'architecture ainsi que d'un audit organisationnel et physique ;

Commanditaire d'audit : entité faisant appel au service d'audit de la sécurité des systèmes d'information ;

Entité auditée : organisme(s) responsable(s) de tout ou partie du système d'information de l'entité auditée. Le commanditaire peut être l'entité auditée ;

Auditeur : personne menant une mission d'audit pour le compte d'un prestataire d'audit.

Chapitre II : Procédure d'homologation des prestataires d'audit

Article 3

La demande d'homologation est déposée par le prestataire d'audit auprès de l'autorité compétente contre récépissé revêtu du numéro d'enregistrement ou adressée à ladite autorité gouvernementale par lettre recommandée avec accusé de réception.

Cette demande est accompagnée par le dossier contenant les documents suivants :

- copie du statut de la société demandant l'homologation ;

- attestation d'inscription de la société au registre de commerce ;

- copies des pièces d'identité des dirigeants de la société et des experts auditeurs proposés dans le cadre de l'homologation ;

- note indiquant les moyens humains et techniques de la société demandant l'homologation ;

- curriculums vitae, et si nécessaire, les copies des certificats de formation des auditeurs proposés dans le cadre de l'homologation ;

- copies des contrats de travail conclus avec les auditeurs ;

- copies certifiées conformes délivrées par les maîtres d'ouvrages publics ou privés sous la direction desquels les prestations d'audit ont été exécutées. Chaque attestation précise notamment la nature des prestations et l'année de réalisation ainsi que le nom et la qualité du signataire et son appréciation ;

- document de présentation de la méthodologie qui sera appliquée pour la conduite de la prestation d'audit objet de la demande d'homologation.

Le dossier de demande d'homologation est réputé complet, si le prestataire d'audit n'a pas été invité à fournir des pièces ou renseignements complémentaires dans un délai de soixante (60) jours à compter de la date de réception de la demande.

Toute modification de l'un des éléments sur la base desquels la demande d'homologation a été effectuée doit être communiquée à l'autorité compétente pendant la phase de traitement de cette demande.

Article 4

Lorsqu'elle s'assure que le dossier de la demande est complet, l'autorité compétente évalue ou invite éventuellement le prestataire d'audit demandeur de l'homologation à faire évaluer ses services auprès d'organismes mandatés à cet effet par elle-même. Le demandeur d'homologation prend en charge tous les frais de cette opération.

L'évaluation précitée se fait au regard du référentiel d'exigences élaboré par l'autorité compétente, et mis à la disposition du public sur le site web de la direction générale de la sécurité des systèmes d'information (www.dgssi.gov.ma).

Article 5

Au vu des résultats du rapport d'évaluation, visé à l'article ci-dessus, l'autorité compétente décide d'homologuer ou non le demandeur d'homologation, et ce dans un délai qui ne dépasse pas quatre-vingt-dix (90) jours depuis la date de la réception du dossier complet de la demande.

La décision d'homologation indique le nom et l'adresse du prestataire d'audit concerné, le numéro de ladite homologation, les dates de sa délivrance et de son expiration.

L'homologation est valable pour une durée maximale de trois (3) ans et peut être renouvelée dans les mêmes conditions que celles de sa délivrance initiale. Dans ce cas, la demande de renouvellement de l'homologation doit être déposée auprès de l'autorité compétente soixante (60) jours au moins avant la date d'expiration de l'homologation.

Le prestataire d'audit est tenu d'informer, sans délai, l'autorité compétente de toute modification des circonstances dans lesquelles il a été homologué.

En cas de refus de l'homologation, le demandeur doit être avisé, par l'autorité compétente des motifs de ce refus.

Article 6

L'homologation est délivrée aux prestataires d'audit pour l'un ou plusieurs des domaines d'audit suivants :

- audit organisationnel et physique ;

- audit d'architecture ;

- audit de configuration ;

- audit de code source ;

- test d'intrusion ;

- audit des systèmes industriels.

Article 7

Lorsque, à la suite des vérifications effectuées par l'autorité compétente, celle-ci constate que le prestataire d'audit homologué ne répond plus au référentiel d'exigences visé à l'article 4 ci-dessus, ladite autorité invite le prestataire concerné à se conformer à ces exigences dans le délai qu'elle détermine.

Si le prestataire d'audit concerné ne s'y est pas conformé, l'autorité compétente décide :

- la suspension de l'homologation en mettant le prestataire d'audit concerné en demeure de se conformer aux prescriptions indiquées dans la décision de suspension dans un délai maximum de trois (3) mois ;

- le retrait de l'homologation, lorsque, à l'issue du délai fixé dans la décision de suspension, il ne s'est pas conformé aux prescriptions indiquées dans la décision de suspension.

Article 8

La liste des prestataires d'audit homologués est publiée annuellement au " Bulletin officiel ".

Chapitre III : Modalités de déroulement de l'audit

Article 9

L'audit fait l'objet d'une convention entre le commanditaire d'audit et le prestataire d'audit. Cette convention doit, principalement comprendre:

- l'objet de l'audit ;

- le périmètre de l'audit et ses modalités ;

- les principales normes sur lesquelles se base l'audit ;

- les dates et les lieux de l'audit ;

- les canaux de communication sécurisés entre l'auditeur et l'entité auditée ;

- les moyens et la logistique nécessaires à l'exécution de l'audit ;

- les clauses de confidentialité concernant l'audit ;

- éventuellement, le suivi de la mise en oeuvre des recommandations issues de cet audit par le prestataire de l'audit.

Article 10

Le prestataire d'audit peut, dans un cadre contractuel et après accord formel du commanditaire, sous-traiter une partie des activités d'audit à un autre prestataire d'audit homologué par l'autorité compétente.

Il peut aussi, dans un cadre contractuel et après accord formel du commanditaire, faire intervenir un expert sur une partie des activités d'audit.

Article 11

La mission d'audit est achevée à la suite de la réalisation de l'ensemble des actions définies dans la convention d'audit et de la communication du rapport final d'audit au commanditaire de l'audit.

A la fin de la mission d'audit, le prestataire d'audit doit communiquer au commanditaire tous les documents et supports résultant de l'audit et ne doit garder aucune copie.

Article 12

L'entité auditée doit garder les rapports d'audit et documents associés, notamment :

- les procès-verbaux des réunions ;

- les grilles d'évaluation des niveaux de maturité par rapport aux objectifs de sécurité initialement définis ;

- les relevés et résultats des tests techniques comportant les preuves de l'audit.

Les rapports d'audit et documents associés doivent rester confidentiels et protégés durant la période de conservation par l'entité auditée.

Les conclusions des rapports d'audit et les plans d'action de mise en œuvre des recommandations figurant dans ces rapports doivent être

communiqués par l'entité auditée à l'autorité compétente à la fin de la mission d'audit.

Article 13

Le présent arrêté est publié au Bulletin officiel.

Rabat, le 21 safar 1440 (31 octobre 2018).

SAAD DINE EL OTMANI.