Arrêté du ministre des technologies de la communication du 12 septembre 2023, fixant les critères techniques d'audit et les modalités de suivi de la mise en œuvre des recommandations contenues dans le rapport d'audit.

Le ministre des technologies de la communication,

Vu la Constitution,

Vu le code des télécommunications promulgué par la loi n° 2001-1 du 15 janvier 2001, ensemble les textes qui l'ont modifié ou complété, dont le dernier en date la loi n° 2013-10 du 12 avril 2013,

Vu le décret-loi n° 2023-17 du 11 mars 2023, relatif à la cybersécurité,

Vu le décret n° 2004-1248 du 25 mai 2004, fixant l'organisation administrative et financière et les modalités de fonctionnement de l'agence nationale de la sécurité informatique,

Vu le décret n° 2012-1997 du 11 septembre 2012, fixant les attributions du ministère des technologies de l'information et de la communication,

Vu le décret n° 2012-1998 du 11 septembre 2012, portant organisation du ministère des technologies de l'information et de la communication,

Vu le décret Présidentiel n° 2021-138 du 11 octobre 2021, portant nomination des membres du Gouvernement,

Vu le décret n° 2023-550 du 1er août 2023, portant nomination du Chef du Gouvernement.

Arrête :

Article premier - Les organismes cités à l'article 6 du décret-loi n° 2023-17 du 11 mars 2023, relatif à la cybersécurité, sont soumis à un système d'audit obligatoire et périodique par le biais d'une mission d'évaluation sur site de la sécurité de leurs systèmes d'information.

L'audit de sécurité des systèmes d'information doit être réalisé conformément au référentiel défini par l'Agence Nationale de la Cybersécurité qui comporte les éléments essentiels suivants :

- Evaluation des aspects structurels, organisationnels et opérationnels de la sécurité des systèmes d'information,
- Audit technique de la sécurité des composants du système d'information et test de leur immunité face aux incidents cybernétiques,
- Analyse et évaluation des risques cybernétiques et présentation d'un plan de traitement afin d'éliminer ou de réduire le dégât des incidents cybernétiques.

Art. 2 - L'expert chargé de l'audit remet à l'organisme audité un rapport portant son cachet et sa signature et élaboré conformément au modèle du rapport d'audit fourni par l'Agence. Ce rapport comporte, essentiellement, ce qui suit :

- Une description complète du système d'information avec les justifications nécessaires en cas d'exclusion de certains composants du périmètre de l'audit,
- Une vérification de l'application des recommandations et des solutions de sécurité organisationnelles et techniques proposées pour pallier aux insuffisances enregistrées lors du dernier audit,
- Une évaluation complète de la sécurité du système d'information et une analyse précise des insuffisances organisationnelles et techniques relatives aux procédures et mécanismes de sécurité adoptés ainsi qu'une évaluation des risques qui pourraient résulter de l'exploitation des failles découvertes,
- Les recommandations et les solutions de sécurité organisationnelles et techniques proposées pour pallier aux insuffisances enregistrées,
- Une copie des procès-verbaux des réunions de démarrage et de clôture de la mission d'audit.

Art. 3 - L'Agence étudie le rapport d'audit soumis et répond par acceptation ou refus et elle peut aussi demander à l'organisme audité de lui fournir des informations ou des documents supplémentaires et elle peut également procéder à un contrôle sur site.

Art. 4 - L'Agence peut rejeter le rapport d'audit dans les cas suivants :

- La non-conformité du rapport d'audit au modèle de rapport mentionné à l'article 2 du présent arrêté,
- L'évaluation de la sécurité du système d'information est non pertinente ou incomplète,
- Le rapport d'audit n'inclut pas les recommandations et les solutions qui doivent être proposées pour pallier aux insuffisances enregistrées,
- La non-réalisation de la mission d'audit selon le référentiel d'audit mentionné au niveau de l'article premier du présent arrêté.

En cas de rejet du rapport, l'organisme concerné est tenu de refaire l'audit et de communiquer le nouveau rapport à l'Agence dans un délai ne dépassant pas deux mois à compter de la date de la notification.

Art. 5 - L'expert auditeur est tenu, lors de la réalisation de la mission d'audit, d'informer immédiatement l'Agence lorsqu'il découvre des risques de sécurité graves pouvant affecter la sécurité du cyberespace et il est tenu également d'alerter l'organisme concerné pour prendre les contremesures nécessaires.

Art. 6 - Le présent arrêté sera publié au Journal officiel de la République tunisienne.

Tunis, le 12 septembre 2023.

Le ministre des technologies de la communication

Nizar Ben Neji

Vu

Le Chef du Gouvernement

Ahmed Hachani