République tunisienne

-------§-------

Ministère des Technologies de la Communication

et de l'Economie Numérique

------§------

الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

2ème Workshop

Sur la Protection des Infrastructures d'Information Critiques

Rapport de synthèse

Contexte

Le 2ème workshop sur la protection des infrastructures d'information critiques s'inscrit en continuité avec le 1er workshop organisé par l'ANSI en collaboration avec l'instrument de la commission européenne TAIEX, et ce dans le cadre de la préparation à la mise en œuvre de la stratégie nationale de cyber-sécurité et du plan d'action pour assurer la résilience des infrastructure d'information critiques. Le workshop a eu lieu Jeudi 05 décembre 2019 à l'hôtel Africa.

Le nombre de participants s'élève à 50 RSSI et responsables informatiques issus d'organismes publics et privés des secteurs Energie, Industrie, Finance, Télécom, Santé, Transport, Agriculture, Commerce et Education.

Déroulement du workshop et principaux sujets soulevés

Les travaux du workshop ont commencé par rappeler le contexte du projet de protection des infrastructures d'information critiques, les recommandations qui ont débouché du 1er workshop. Ensuite, l'équipe chargée de l'élaboration du code numérique auprès du Ministère des Technologies de la Communication et de l'Economie Numérique a présenté en diagonal le projet de code numérique et a mis l'accent sur la section liée à la confiance numérique, en particulier à la protection des infrastructures d'information critiques, à la gestion de crise suite à des risques cybernétiques et aux prérogatives de l'ANSI. Par la suite, l'ANSI a présenté sa vision, ses objectifs et son plan d'action et a mis l'accent sur les instruments organisationnels et opérationnels mis en œuvre et projetés à court et à moyen terme pour le partage et l'échange d'information sur les risques des infrastructures d'information critiques.

Les présentations ont été suivies par des exercices sous forme d'ateliers sectoriels, les exercices ont portés sur l'état des lieux et les recommandations des participants notamment par rapport à :
- L'identification des services critiques et l'identification des risques qui leur sont liés
- L'intégration du volet sécurité du système d'information dans les projets métier
- La mise en œuvre de systèmes de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information critiques
- Développement des compétences
- La gestion des crises
- La conformité

Recommandations

Les participants ont apprécié les étapes franchies dans le projet de protection des infrastructures d'information critiques notamment par rapport à l'approbation de la stratégie nationale de cyber-sécurité, le projet de code numérique et les concertations menées par l'ANSI avec les responsables des services critiques pour mettre en place les bases organisationnelles et opérationnelles nécessaires.

Toutefois, les participants ont proposé un ensemble de recommandations déclinées en trois axes:

→ Recommandations d'ordre organisationnel

Dans le cadre de la revue du cadre de gouvernance de la cyber-sécurité en général et des infrastructures d'information critiques en particulier, il a été proposé de :

- Définir des critères de criticité à l'échelle nationale pour l'identification des services critiques pour la résilience de l'état, les responsables métier au niveau des infrastructures d'information critiques doivent participer activement à la définition de ces critères.

- Renforcer les mécanismes de suivi de l'état de sécurité des infrastructures d'information critiques

- Renforcer la fonction sécurité au niveau de l'organisation des infrastructures d'information critiques

- Ouvrer à suivre les indicateurs de sécurité des systèmes d'infrastructures d'information critiques périodiquement au niveau du conseil d'administration ou de l'entreprise.

→ Recommandations liées au développement des compétences

- Sensibiliser les décideurs et les responsables directs sur la production

- Encourager l'instauration de cycles de formation professionnelle spécialisée

- Encourager la création d'un noyau de professionnels du secteur privé spécialistes dans les systèmes spécifiques (Industrie, finance, etc)

- Maintenir un réseau d'échange et de partage avec les RSSIs des infrastructures d'information critiques

→ Recommandations d'ordre opérationnel

- Dresser et maintenir la cartographie des services critiques (sur la base des critères de criticité) et les dépendances entre les infrastructures d'information

- Mettre en œuvre au sein des infrastructures d'information critiques un système de veille sur les risques cybernétiques (SIEM, etc), et vérification des procédures et mécanismes lors de l'audit

- Encourager les infrastructures d'information critiques à mettre en place des SOCs et partager les informations sur les risques avec les IIC interdépendants (exemple SOC maritime)

- Mettre en place un service de déclaration et de suivi des incidents en ligne

- Instaurer des standards sectoriels qui définissent les exigences minimales de sécurité et mettre en place des mécanismes de suivi efficients.

Débouchés du workshop

A l'issue du workshop, il a été convenu de constituer des taskforces sectoriels pour la définition de :

- critères d'identification des infrastructures critiques

- cartographie des risques sur le métier

- exigences de sécurité orientées risques métier