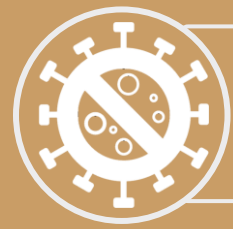
rsbp Programme régional PME Tunisie

Banque Européenne pour la Reconstruction et le Développement

Panel :

« Cyber résilience : Menaces et opportunités pour le secteur financier en Tunisie »



FORMEZ VOUS EN LIGNE EN TOUTE SECURITE!

Définitions de la cybersécurité et cyber-résilience

Australia. “The ability to prepare for, respond to and recover from a cyber attack. Cybersecurity is the praxis of protecting digital assets from connected threats. Resilience is more than just preventing or responding to an attack – it also takes into account the ability to operate during, and to adapt and recover, from such an event”.

Australie. « La capacité de se préparer, de réagir et de se remettre d'une cyberattaque. La cybersécurité est la pratique de la protection des actifs numériques contre les menaces connectées. La résilience ne se limite pas à prévenir ou à répondre à une attaque - elle prend également en compte la capacité d'opérer pendant, de s'adapter et de se remettre d'un tel événement ».

Source : FSB, “Stock take of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices”, Oct. 2017.

Cadre légal

- Circulaire aux établissements de crédit N° 2006 - 19 :(Objet: Dispositifs de control interne ‘Articles 4 et 14’)
- Circulaire de la Banque Centrale de Tunisie n° 2018 -16 du 31 décembre 2018 (Objet : Règles régissant l’activité et le fonctionnement des établissements de paiement) ;
- Circulaire de la Banque Centrale de Tunisie n°2020-11 du 11 mai 2020 (Objet : Conditions de fourniture des services de paiement mobile domestique).
- Convention d’adhésion à des plateformes ou services fournis par le régulateur (Exemple : Convention d’adhésion au système Elyssa-RTGS)

Cadre légal (suite)

- Elaboration d'une enquête relative à la cybersécurité dans le milieu financier tunisien (Novembre 2021) qui a couvert les voltes suivants:
  I. Stratégie et budget informatique
  II. Gouvernance
  III. Contrôle interne
  IV. Operations informatiques
  V. Sécurité
- Projet d'élaboration de circulaires spécifiques (actuellement en stade avancé) sur le traitement du risque cyber dans le milieu financier.

Cadre légal (suite)

Plusieurs juridictions dans le monde ont opté pour une mise en œuvre des réglementations spécifiques sur la maîtrise du risque informatique et la cybersécurité du secteur financier.

- Le **Conseil de Stabilité Financière 'CSF'** ou **Financial Stability Board 'FSB'** avait recensé que ses 25 juridictions membres avaient élaboré au moins une réglementation de ce type dans un rapport qui a été publié en Oct. 2017.

- **L'Autorité Bancaire Européenne (EBA)** a élaboré en Novembre 2019 un guide dans lequel elle définit des orientations sur le risque informatique et la cybersécurité obligeant ainsi ses états membres a révisé et adapter leurs textes par rapport à ces orientations.

- Un nouveau projet de règlement européen, appelé ***Digital Operational Resilience Act*** **(DORA),** presque validé (en Mai 2022) par le Conseil de l'Union européenne, qui va reprendre plusieurs dispositions figurant dans les orientations définies précédemment par l'EBA, tout en les complétant de dispositifs nouveaux, notamment sur la surveillance des grands prestataires informatiques, le reporting des incidents ou la pratique de tests de sécurité.

- **La Banque Mondiale BM** dispose d'un registre des différents textes relatifs à la gestion du risque informatique et de la cybersécurité du secteur financier.

Modèle d'un texte réglementaire sur le risque informatique et le risque cyber

- On remarque une certaine convergence quant à l'approche utilisée pour l'élaboration de textes de ce type, qui comporte plusieurs sections :

  - Renforcement de la gouvernance (Implication de la direction générale et les organes de gouvernance CA, définition de stratégie, …),

  - Renforcement de la gestion des risques (Définition de politique ,appétence aux risques, Implication de la 2ème et de la 3ème ligne de défense),

  - Renforcement des mesures de sécurité (Protection physique, protection logique, mesures de détection, mécanismes de réaction , et plan de rétablissement)

  - Renforcement du « 'Build' et du 'Run' Construction et Exécution » (Gestion des incidents, continuité d'activité , KPI et Reporting)

  - Obligations (Déclaration d'incidents, Planification de tests d'intrusion, Suivi des prestataires externes surtout ceux qui exercent dans le 'Cloud Computing')

Quelques Citations à la marge

- « ***Cyber Terrorism Is country's biggest threat*** » une déclaration de l'ancien Président OBAMA après l'attaque de SONY en Novembre 2014 par des hackers de la Corée du Nord 'GoP' 'Guardian of Peace' causant une perte estimée à 4 billion $.

- « ***Cyber Terrorism is the biggest threat of the country , we will soon have only two types of nation , nation with cyber offensive & defensive capabilities and those without*** » A. P. J. Abdul Kalam Marecar 11ème président de l'Inde