بنك المغرب
BANK AL-MAGHRIB

Le Gouverneur

الوالي

D N° 3/W/16

Rabat, le 10 juin 2016

Directive fixant les règles minimales à observer par les établissements de crédit pour réaliser les tests d'intrusion des systèmes d'information

Le Wali de Bank Al-Maghrib ;

vu la loi n°103-12 relative aux établissements de crédit et organismes assimilés promulguée par le dahir n° 1-14-193 du 1er rabii I 1436 (24 Décembre 2014);

vu les dispositions de la circulaire n°4/W/2014 du 30 octobre 2014 relative au contrôle interne des établissements de crédit ;

vu les dispositions de la Directive Nationale de la Sécurité des Systèmes d'Information.

après avis du Comité des établissements de crédit émis en date du 1er juin 2016 ;

la présente directive fixe les règles minimales à observer par les établissements de crédit désignés ci-après «établissement» pour la réalisation des tests d'intrusion sur leurs systèmes d'information désignés ci-après «tests».

Article premier

L'établissement doit évaluer la sécurité de son système d'information et inscrire la conduite régulière de tests dans un cadre global d'évaluation de l'efficacité des dispositifs de sécurité, s'appuyant sur une démarche basée sur les risques.

Article 2

L'établissement élabore une cartographie des risques de ses systèmes d'information au regard des risques d'intrusion ou de cyberattaques.

Article 3

L'établissement arrête annuellement un programme de tests à mener, tenant compte de l'ensemble des exigences légales, réglementaires et contractuelles en la matière.

Le programme doit spécifier le périmètre, la nature, l'étendue et la fréquence des tests pour l'ensemble du système d'information de l'établissement, qu'il soit primaire ou de secours. Il doit être soumis pour validation au comité d'audit ou des risques de l'établissement, selon le cas.

Article 4

Les tests ont pour objet d'analyser l'état de sécurité du système d'information de l'établissement et d'évaluer sa capacité à faire face de manière adéquate à des attaques ciblant ledit système.

Article 5

Le périmètre, la nature, l'étendue et la fréquence des tests doivent être adaptés aux systèmes d'information de l'établissement notamment :

- la criticité de ces systèmes ;
- les résultats de l'analyse des risques devant être menée par l'établissement au sens de l'article 2;
- la taille et le volume d'activité.

Article 6

Les systèmes d'information ouverts sur l'extérieur doivent faire l'objet de tests infra-annuels.

Article 7

Des tests sont à effectuer à l'occasion de tout changement dans le système d'information susceptible d'impacter l'exposition globale aux risques de sécurité de l'information ou de cyberattaques.

Bank Al-Maghrib peut exiger d'un établissement de réaliser des tests ciblés, selon la fréquence et les modalités qu'elle détermine.

Article 8

Le Responsable de la Sécurité des Systèmes d'Information de l'établissement établit et pilote la réalisation du programme annuel des tests. En coordination avec le responsable de l'entité en charge du système d'information, il définit les modalités de réalisation des tests.

La fonction « Responsable de la Sécurité des Systèmes d'Information » est entendue au sens de la Directive Nationale de la Sécurité des Systèmes d'Information.

Article 9

Les tests doivent être réalisés aussi bien à partir du réseau informatique interne de l'établissement que depuis l'extérieur.

Article 10

L'établissement doit établir une démarche et méthodologie, s'appuyant sur les bonnes pratiques en la matière, pour la réalisation des tests. Il doit au moins effectuer des tests selon les approches ci-après :

- une approche qui consiste à réaliser les tests sans connaissances préalables sur le système d'information cible ;
- une approche qui consiste à réaliser les tests avec des connaissances préalables sur le système d'information cible.

Article 11

L'établissement est tenu d'établir une charte qui définit le cadre de réalisation des tests et les règles à observer par les équipes internes et externes en charge de leur réalisation.

Article 12

Pour la réalisation des tests nécessitant de disposer d'informations explicites et confidentielles sur les systèmes ciblés, la banque privilégie le recours à ses équipes internes.

Article 13

Les équipes internes de l'établissement, qui effectuent des tests, doivent disposer de l'expertise et des certifications nécessaires. Ces équipes doivent être indépendantes et dotées de moyens suffisants.

Article 14

L'exécution des tests par un prestataire externe doit se faire dans le cadre d'une convention qui définit notamment le périmètre d'intervention, les modalités d'exécution et la responsabilité du prestataire.

Article 15

L'établissement doit s'assurer que le choix du prestataire et la réalisation des tests tiennent compte, notamment, des éléments suivants :

- le prestataire doit disposer des compétences et de l'expertise nécessaires dans les domaines de conduite des tests et d'audit de sécurité des systèmes d'information notamment bancaires;
- le prestataire et ses équipes doivent se conformer à un engagement strict de confidentialité au sujet des caractéristiques des systèmes testés, des résultats des tests et des données utilisées ou visualisées ;
- les prestations doivent être réalisées avec loyauté et intégrité;
- le prestataire s'oblige en fin de mission à procéder, dans un délai maximum de deux mois, à la destruction des enregistrements qu'il a relevés dans le cadre de sa mission ainsi que ceux fournis par l'établissement. Le prestataire s'oblige à fournir un document formel matérialisant la destruction desdits enregistrements;
- l'exploitation des vulnérabilités identifiées, pour des besoins de preuve, est obligatoirement soumise à l'accord préalable et explicite de l'établissement et

ne doit pas porter atteinte au système d'information cible, notamment, sa disponibilité, sa confidentialité et son intégrité ;
- le prestataire est tenu de respecter la législation et la réglementation en vigueur au Maroc, notamment en matière de confidentialité et de sécurité des données et des systèmes d'information.

Article 16

L'établissement veille à ce que les tests ne présentent pas des risques de perturbation opérationnelle et ne mettent pas en cause la continuité du service du système d'information. Il arrête, à cet effet, les délais et les horaires d'intervention.

Il s'assure également que son plan de continuité d'activité prévoit des mesures adéquates à entreprendre, en cas de perturbation du fonctionnement, de la performance ou la disponibilité du système d'information dus à des tests ou à des cyberattaques.

Article 17

Les résultats des tests doivent être portés à la connaissance de l'organe de direction et au comité d'audit ou des risques, selon le cas. Ces résultats doivent retracer au minimum :

- la description de la démarche et le périmètre des tests ainsi que les risques couverts ;
- la définition et la qualification des différents tests effectués et des moyens employés ;
- les vulnérabilités détectées et leurs impacts sur la sécurité du système d'information de l'établissement ;
- l'appréciation du niveau de sécurité du système d'information ayant fait l'objet des tests par rapport aux standards reconnus en la matière,
- les actions préventives et correctives nécessaires.

Article 18

L'établissement s'assure, dans le cas d'un système d'information externalisé auprès d'un prestataire, que l'ensemble des dispositions de la présente directive soit observé et pris en compte dans le contrat les liant.

Article 19

L'établissement établit un plan d'actions à l'effet de corriger les vulnérabilités et faiblesses constatées à travers les tests.

L'organe de direction veille à la réalisation dudit plan et en informe le comité d'audit ou des risques, selon le cas.

Article 20

L'établissement adresse à Bank Al-Maghrib, au plus tard le 31 mars, un rapport annuel sur les tests retraçant :

- la cartographie des risques citée à l'article 2;
- le programme des tests réalisés ;
- le bilan des tests réalisés et résultats y afférents ;
- le bilan des plans d'actions correctifs ;
- le programme de tests de l'année à venir.

Article 21

Les dispositions de la présente directive prennent effet à compter de la date de sa signature.

Signé :

Abdellatif JOUAHRI