Décret n° 2004-1250 du 25 mai 2004, fixant les systèmes informatiques et les réseaux des organismes soumis à l'audit obligatoire périodique de la sécurité informatique et les critères relatifs à la nature de l'audit et à sa périodicité et aux procédures de suivi de l'application des recommandations contenues dans le rapport d'audit.

Le Président de la République,

Sur proposition du ministre des technologies de la communication et du transport,

Vu la loi n° 2004-5 du 3 février 2004, relative à la sécurité informatique et notamment son article *5,*

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° 2004-1249 du 25 mai 2004, fixant les conditions et les procédures de certification des experts auditeurs dans le domaine de la sécurité informatique,

Vu l'avis du tribunal administratif.

Décrète :

Article premier. - Le présent décret fixe les systèmes informatiques et les réseaux des organismes soumis à l'audit obligatoire périodique de la sécurité informatique et les critères relatifs à la nature de l'audit, à sa périodicité et aux procédures de suivi de l'application des recommandations contenues dans le rapport d'audit conformément à l'article 5 de la loi susvisée n° 2004-5 du 3 février 2004.

Art. 2. - Sont soumis à l'audit obligatoire périodique conformément à l'article 5 de la loi susvisée n° 2004-5 du 3 février 2004, les systèmes informatiques et les réseaux relevants des organismes publics et les systèmes informatiques et les réseaux des organismes du secteur privé suivants :

- les opérateurs de réseaux publics de télécommunications et les fournisseurs des services de télécommunications et d'internet,

- les entreprises dont les réseaux informatiques sont interconnectés à travers des réseaux externes de télécommunications,

- les entreprises qui procèdent au traitement automatisé des données personnelles de leurs clients dans le cadre de la fourniture de leurs services à travers les réseaux de télécommunications.

Art. 3. - L'opération d'audit se déroule par le biai d'une enquête de terrain basée sur les principaux éléments suivants :

- audit des aspects organisationnels et de la structuration de la fonction sécurité, ainsi que du mode de gestion des procédures de sécurité et la disponibilité des outils de sécurisation du système informatique et de leur mode d'utilisation,

- analyse technique de la sécurité de toutes les composantes du système informatique, avec la réalisation du test de leur résistance à tous les types de dangers,

- analyse et évaluation des dangers qui pourraient résulter de l'exploitation des failles découvertes suite à l'opération d'audit.

Art. 4. - A la fin de l'opération d'audit visée à l'article 3 du présent décret, l'expert chargé de l'audit délivre à l'organisme concerné un rapport portant son cachet et sa signature.

Ce rapport renferme, essentiellement, ce qui suit :

- une description et une évaluation complète de la sécurité du système informatique, comprenant les mesures qui ont étés adoptées depuis le dernier audit réalisé et les insuffisances enregistrées dans l'application des recommandations,

- une analyse précise des insuffisances organisationnelles et techniques relatives aux procédures et outils de sécurité adoptés, comportant une évaluation des risques qui pourraient résulter de l'exploitation des failles découvertes,

- la proposition des procédures et des solutions organisationnelles et techniques de sécurité qui devront être adoptées pour dépasser les insuffisances enregistrées.

Art. 5. - Les organismes prévus à l'article *5* de la loi susvisée n° 2004-5 du 3 février 2004, devront auditer la sécurité de leurs systèmes informatiques et leurs réseaux de manière périodique une fois au moins tous les douze (12) mois.

L'agence nationale de la sécurité informatique peut proroger ce délai pour des raisons exceptionnelles et sur demande de l'organisme concerné, trois (3) mois au moins avant l'expiration du délai prévu pour effectuer l'opération d'audit.

Art. 6. - L'organisme concerné envoie à l'agence nationale de la sécurité informatique le rapport d'audit et tous les procès-verbaux des réunions de travail organisées avec l'expert auditeur, par lettre recommandée ou document électronique fiable avec accusé de réception ou par dépôt auprès de l'agence contre récépissé dans une enveloppe fermée, et ceci, dans un délai ne dépassant pas dix (10) jours à partir de la date de réception du rapport d'audit.

Art. 7. - L'agence nationale de la sécurité informatique peut, après étude du rapport, demander à l'organisme concerné de lui fournir des informations ou des documents supplémentaires et de procéder à un contrôle de terrain.

L'agence peut procéder à ce contrôle, après avoir avisé le président de l'organisme concerné par lettre recommandée ou document électronique fiable avec accusé de réception.

Art. 8. - L'agence nationale de la sécurité informatique peut rejeter le rapport d'audit dans les cas suivants :

- la non-réalisation de l'audit de terrain, selon les procédures prévues à l'article 3 du présent décret,

- si le rapport d'audit ne contient pas les éléments prévus à l'article 4 du présent décret ou si l'agence s'aperçoit que le rapport d'audit ne contenait pas des données importantes relatives aux insuffisances enregistrées.

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

A l'expiration de ce délai sans résultat, l'agence peut designer un expert qui sera chargé de l'audit susvisée aux frais de l'organisme contrevenant.

Art. 9. - Les organismes du secteur privé prévus à l'article 2 du présent décret disposent d'une période de douze (12) mois à compter de la date de publication du présent décret pour appliquer ses dispositions.

Art. 10. - Le ministre des technologies de la communication et du transport est chargé de l'exécution du présent décret qui sera publié au Journal Officiel de la République Tunisienne.

Tunis, le 25 mai 2004.

Zine El Abidine Ben Ali