PRÉSIDENCE
DE LA RÉPUBLIQUE
DU SÉNÉGAL

POLITIQUE DE SÉCURITÉ LOGIQUE

DCSSI
DIRECTION GENERALE DU CHIFFRE ET DE LA SECURITE DES SYSTEMES D'INFORMATION

SECURITE DES ECHANGES

Les services de réseau comprennent la fourniture de connexion, les services de réseau privé, les réseaux à valeur ajoutée et les solutions de management de la sécurité des réseaux comme les pare-feu et les systèmes de détection d'intrusion. Ces services peuvent aller du simple octroi d'une bande passante non gérée à des offres complexes à valeur ajoutée.
Pour tous les services de réseau, il convient d'identifier les mécanismes de sécurité, les niveaux de service et les exigences de gestion, et de les intégrer dans les accords de services de réseau, que ces services soient fournis en interne ou qu'ils soient externalisés.
Il faut, par conséquent, prendre des mesures pour garantir aussi bien la sécurité des données échangées que celle des supports de transmission.

01 Il faut mettre en place une politique d'accès aux réseaux de l'entité, qui précise les exigences d’authentification des utilisateurs.

02 Il faut définir les responsabilités et les procédures de gestion des équipements réseau.

03 Les moyens de transmission de l'information doivent être conformes à la législation en vigueur.

04 Il faut mettre en place un mécanisme de surveillance et de journalisation de toutes les activités dans le réseau.

05 Les données transmises via les réseaux publics doivent être protégées selon leur niveau de classification. Il faut utiliser les réseaux de l'Etat, autant que faire se peut, pour transmettre des données hors de l'entité.

06 Les services de réseau doivent, en accord avec le fournisseur, être sécurisés par des fonctions de sécurité : l'authentification, l'intégrité, le chiffrement, la non répudiation et les contrôles de connexion réseau.

07 Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifiques. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par le HFD concerné, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter, à un périmètre déterminé, les conséquences d'une intrusion depuis la voie radio. A défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil, sur des systèmes d’information manipulant des données sensibles, est proscrit.

08 Il faut effectuer un cloisonnement, physique et/ou logique des réseaux informatiques, suivant un critère bien défini pour séparer les réseaux : par service administratif, par niveau de sécurité, etc.

09 Dans le cas d'une interconnexion avec un autre organisme ou lors de la mutualisation des moyens de traitement de l'information, il faut effectuer une analyse des risques afin de protéger les systèmes contenant des informations sensibles :

POLITIQUE DE SÉCURITÉ LOGIQUE

SECURITE DES ECHANGES (SUITE)

Sur le plan des données échangées, c'est-à-dire pendant la transmission de l 'information, des procédures doivent être mises en place pour assurer sa protection :

- Il faut choisir des algorithmes de chiffrement labellisés par la Commission nationale de cryptologie.
- Il faut sensibiliser le personnel sur les risques de divulgation des informations classifiées.
- Il faut sensibiliser le personnel sur les dangers, au plan de la sécurité, de l'utilisation des appareils indiscrets, comme le téléphone et la télécopie, pour échanger des informations sensibles. Il faut utiliser en lieu et place, des téléphones et des fax chiffrés sous réserve des dispositions de la loi no 2008-41 du 20 août 2008 sur la cryptologie.
- Les données transmises par le biais d'équipements électroniques doivent respecter la législation sur les transactions électroniques et les différents décrets d' application.
- Il faut mettre en place un système d'authentification forte et un système de chiffrement pour sécuriser la messagerie électronique de l'entité.
- Il faut assurer la disponibilité et la fiabilité de la messagerie électronique.

Sur le plan des données stockées, il faut mettre en place une politique de chiffrement de ces données pour garantir leur confidentialité, leur intégrité et leur authenticité ainsi qu'une politique de gestion des clefs de chiffrement. Ces mesures sont les suivantes :

- Chiffrer une ou plusieurs parties des disques durs des systèmes d'information contenant les informations sensibles.
- Lorsque le matériel ou le système d'information est mis hors service, en plus de l'effacement sécurisé des disques, l'intégralité de ces disques doit être chiffrée pour réduire le risque de divulgation de l'information sensible.
- Il faut utiliser les moyens d'effacement sécurisé des données contenues dans les disques durs labellisés par la Commission nationale de cryptologie.
- Il faut se conformer à la règle 19-9-1 pour le choix des algorithmes de chiffrement.
- Il faut choisir des longueurs de clefs de chiffrement conformes aux recommandations de la Commission nationale de cryptologie.
- Il faut mettre en œuvre une politique rigoureuse de gestion des clefs de chiffrement afin d'en assurer la protection, sans faille, durant tout leur cycle de vie.
- Il faut former les utilisateurs à l'emploi correct des matériels et des logiciels de chiffrement.