Sécurité des réseaux

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences de la norme ISO 27001 : 2022**

**5. Déroulement**

**5.1 Sécurité des réseaux**

**5.2 Sécurité des services réseau**

**5.3 Cloisonnement des réseaux**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité :

* de protéger l’information dans les réseaux et dans les installations de traitement de l'information de support contre toute dégradation via le réseau
* d’assurer la sécurité dans l’utilisation des services réseaux
* de cloisonner le réseau en limites de sécurité et contrôler le trafic entre eux en fonction des besoins de l'entreprise

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Sécurité des réseaux » s’applique aux personnes responsables de la gestion des réseaux et des applications dans notre organisation.

**1.3 Glossaire**

SI – sécurité de l’information

TIC – technologie de l’information et de la communication

RSI – responsable sécurité de l’information

SDN – *software-defined networking* - réseau défini par logiciel

SD-WAN – *software-defined wide area networking* - réseau étendu défini par logiciel

VPN – *virual private network* - réseau privé virtuel

**2. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Le RSI est garant de son application. Il reçoit l’appui du directeur.

**3. Documents**

Utilisation de la cryptographie

Transfert de l’information

Protection de la vie privée

Activités de surveillance

Journalisation

Contrôle d’accès

**4. Exigences de la norme ISO 27001 : 2022**

A.8.20 Sécurité des réseaux

Les réseaux et les terminaux doivent être sécurisés, gérés et contrôlés pour protéger l’information des systèmes et des applications.

A.8.21 Sécurité des services réseaux

Les mécanismes de sécurité, les niveaux de service et les exigences des services réseaux doivent être identifiés, mis en œuvre et surveillés.

A.8.22 Cloisonnement des réseaux

Les groupes de services d’information, d’utilisateurs et de systèmes d’information doivent être cloisonnés dans les réseaux de l’organisation.

**5 Déroulement**

**5.1 Sécurité des réseaux**

Des contrôles sont appliqués pour assurer la sécurité de l’information dans les réseaux et pour protéger les services connectés contre tout accès non autorisé. La sécurité des réseaux prend en compte les éléments suivants :

* le type et le niveau de classification de l’information que le réseau peut prendre en charge
* établir les responsabilités et les activités pour la gestion des équipements et des dispositifs de mise en réseau
* maintenir à jour la documentation, y compris les schémas de réseau et les fichiers de configuration des appareils (routeurs, commutateurs)
* séparer la responsabilité opérationnelle des réseaux de l'exploitation des systèmes TIC
* établir des mesures pour sauvegarder la confidentialité, la disponibilité et l'intégrité des données transitant sur des réseaux publics, des réseaux tiers ou sur des réseaux sans fil et pour protéger les systèmes et applications connectés, cf. les procédures Utilisation de la cryptographie, Transfert de l’information et Protection de la vie privée
* une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection d'actions susceptibles d'affecter la sécurité de l'information ou pertinentes pour celle-ci, cf. la procédure Activités de surveillance et la politique Journalisation
* coordonner étroitement les activités de gestion du réseau à la fois pour optimiser le service à l'organisation et pour garantir que les contrôles soient appliqués de manière cohérente dans l'ensemble de l'infrastructure de traitement de l'information
* authentifier les systèmes sur le réseau
* restreindre et filtrer la connexion des systèmes au réseau (pare-feu)
* détecter, restreindre et authentifier la connexion des équipements et dispositifs au réseau
* durcir les dispositifs réseau
* séparer les canaux d'administration du réseau des autres trafics du réseau
* isoler temporairement les sous-réseaux critiques si le réseau est attaqué
* désactiver les protocoles réseau vulnérables

L'organisation s'assure que des contrôles de sécurité appropriés sont appliqués à l'utilisation des réseaux virtualisés. Les réseaux virtualisés couvrent également les réseaux définis par logiciel (SDN, SD-WAN). Les réseaux virtualisés peuvent être souhaitables du point de vue de la sécurité, car ils peuvent permettre une séparation logique des communications se déroulant sur des réseaux physiques, en particulier pour les systèmes et les applications qui sont mis en œuvre à l'aide de l'informatique distribuée.

**5.2 Sécurité des services réseau**

Les mesures de sécurité nécessaires pour des services particuliers, telles que les fonctionnalités de sécurité, les niveaux de service et les exigences de service, sont identifiées et appliquées (par des fournisseurs de services réseau internes ou externes).

La capacité du fournisseur de service réseau à gérer les services convenus de manière sécurisée est déterminée et contrôlée régulièrement. Le droit d'audit est convenu entre l'organisation et le fournisseur. L'organisation tient compte des attestations de tiers fournies par les fournisseurs de services pour démontrer qu'ils maintiennent des mesures de sécurité appropriées.

Des règles d'utilisation des réseaux et des services de réseau sont formulées et appliquées afin de couvrir :

* les réseaux et les services de réseau dont l'accès est autorisé
* les exigences d'authentification pour accéder à divers services de réseau
* les procédures d'autorisation pour déterminer qui est autorisé à accéder à quels réseaux et services en réseau
* la gestion du réseau et les mesures et procédures technologiques pour protéger l'accès aux connexions réseau et aux services réseau
* les moyens utilisés pour accéder aux réseaux et aux services de réseau (utilisation d'un réseau privé virtuel (VPN) ou d'un réseau sans fil)
* l’heure, le lieu et autres attributs de l'utilisateur au moment de l'accès
* la surveillance de l'utilisation des services de réseau

Les fonctionnalités de sécurité suivantes des services réseau sont prises en compte :

* la technologie appliquée à la sécurité des services de réseau :
  + authentification
  + cryptage
  + mesures de connexion au réseau
* les paramètres techniques requis pour une connexion sécurisée avec les services du réseau conformément aux règles de sécurité et de connexion au réseau
* la mise en cache (réseau de diffusion de contenu) et ses paramètres qui permettent aux utilisateurs de choisir l'utilisation de la mise en cache conformément aux exigences de performance, de disponibilité et de confidentialité
* les procédures d'utilisation du service réseau pour restreindre l'accès aux services ou applications réseau

Les services de réseau comprennent la fourniture de connexions, de services de réseau privé et de solutions de sécurité de réseau gérées (pare-feu et systèmes de détection d'intrusion).

**5.3 Cloisonnement des réseaux**

L'organisation gère la sécurité des grands réseaux en les cloisonnant en domaines de réseau distincts et en les séparant du réseau public (Internet).

Les domaines peuvent être choisis en fonction :

* du niveau de confiance
* de la criticité
* de la sensibilité (domaine d'accès public, domaine de bureau, domaine de serveur, systèmes à faible et à haut risque)
* des unités organisationnelles (ressources du personnel, finances, marketing)
* d’une combinaison (domaine de serveur se connectant à plusieurs unités organisationnelles)

La séparation peut être effectuée en utilisant des réseaux physiquement différents ou en utilisant des réseaux logiques différents.

Le périmètre de chaque domaine est bien défini. Si l'accès entre les domaines du réseau est autorisé, il est contrôlé au niveau du périmètre à l'aide d'une passerelle (pare-feu, routeur filtrant).

Les critères du cloisonnement des réseaux en domaines et l'accès autorisé via les passerelles sont basés sur une évaluation des exigences de sécurité de chaque domaine.

L'évaluation respecte la politique Contrôle d’accès, les exigences d'accès, la valeur et la classification des informations traitées et tient compte de l'impact relatif sur les coûts et les performances de l'intégration d'une technologie de passerelle appropriée.

Les réseaux sans fil nécessitent un traitement spécial en raison du périmètre réseau mal défini. L'ajustement de la couverture radio est réalisé pour le cloisonnement des réseaux sans fil. Pour les environnements sensibles, tous les accès sans fil sont traités comme des connexions externes et sont séparés des réseaux internes jusqu'à ce que l'accès ait traversé une passerelle conformément aux mesures du réseau avant d'accorder l'accès aux systèmes internes.

Le réseau d'accès sans fil pour les invités est séparé de ceux du personnel. Le Wi-Fi pour les invités a au moins les mêmes restrictions que le Wi-Fi pour le personnel.