CLOISONNEMENT DES RÉSEAUX

1 2 3

Fiche pratique pour la mise en oeuvre de votre plan d'actions cyber dans votre collectivité.

Description rapide de l'objectif visé :

Un réseau dédié et isolé est réservé aux copieurs.
Un client VPN est configuré pour le télétravail.

Coût estimé :

100€/poste
Boitier pare-feu à partir de 1500€

Niveau de difficulté de l'action :

Complexe

Ressources nécessaires :

Ordinateur, borne Wi-FI

Niveau d'accompagnement :

Standard

Temps estimé :

2 jours

Public visé pour l'action :

Responsable informatique
Personne en charge de l'informatique

Organisation conseillée pour la mise en œuvre dans votre collectivité :

1. Qui fait quoi ? Définir les rôles et responsabilités.
Qui crée le réseau virtuel pour les copieurs et le cloisonne ?
Qui l'administre ?
Comment sont communiqués les éléments pour le prestataire en charge de l'installation et de la maintenance des copieurs ?

2. Pourquoi ?
Pour garantir la sécurité de son système d'information, l'entité doit maîtriser les équipements qui s'y connectent, chacun constituant un point d'entrée potentiellement vulnérable. Les copieurs sont devenus, de par leurs fonctionnalités, des micro-ordinateurs. Ils n'intègrent pas tous une solution de sécurité donc il est nécessaire de les mettre sur un réseau isolé.

Pour le client VPN, il est nécessaire de sécuriser les communications pour les télétravailleurs car l'accès à distance au bureau peut être la source de vulnérabilités.

3. Comment ?
Créer un réseau isolé qui est réservé aux copieurs et le paramétrer pour les échanges d'informations avec le réseau local.
Sélectionner des boitiers pare-feu qui autorisent et gèrent le client VPN.

4. Combien ?
Chaque copieur doit être sur le réseau dédié.
Chaque télétravailleur doit avoir son accès VPN.

5. Quand ?
Dès que possible.

Livrable de l'action terminée :

Les copieurs sont dans un réseau dédié tout en gardant toutes les fonctionnalités.
Les télétravailleurs se connectent au réseau de la collectivité grâce à un client VPN.

Description étape par étape pour la mise en œuvre :

S'équiper d'un boitier pare-feu qui gère un client VPN ainsi que le cloisonnement.
Réaliser le paramétrage du boitier pare-feu en filtrant les accès.

1. Gestion du VPN :

- Se connecter sur la console d'administration après l'avoir installée sur votre arrivée de FAI (fournisseur d'accès internet).
- Activer la fonctionnalité VPN puis paramétrer l'adressage.
- Créer les profils des utilisateurs télétravailleurs sur la console.
- Installer le client sur les postes des utilisateurs concernés en paramétrant les identifiants créés lors de l'étape précédente.

2. Gestion du réseau dédié aux copieurs :

- Pour le réseau dédié aux copieurs, connecter les copieurs sur un port du boitier pare-feu via un switch manageable (administrable). Connecter le reste du réseau sur un autre port du boitier pare-feu.
- Paramétrer les règles de routage entre les réseaux afin de garder les fonctionnalités des copieurs pour les utilisateurs (impression, scan to mail, scan partagé).

Attention : il est possible que les copieurs soient en IP dynamique, auquel cas, il peut être nécessaire de voir avec votre prestataire pour entrer une IP statique.

Pour aller plus loin :

ANSSI :
- Recommandations de sécurité relatives aux réseaux WI-FI
- Guide d'hygiène informatique