Les fonctionnalités du serveur NAS

Rédigé par Halimi Yohan

05/10/2022

1 Qu'est-ce qu'un serveur NAS :

Le NAS, ou Network Attached Storage, est un appareil de stockage autonome qui peut se connecter à votre réseau privé ou professionnel via Internet. Il permet de sauvegarder, partager, sécuriser mais aussi de faciliter l'accès à vos fichiers depuis plusieurs appareils. Il est utilisé de nos jours par les professionnels comme par les particuliers.

Agissant comme un disque dur super sécurisé le serveur NAS est composé de plusieurs emplacement qu'on appelle des baies. Nous pouvons y loger des disques durs. En fonction de notre besoin d'espace disque et du niveau de sécurité souhaité les baies sont plus ou moins nombreuses.



Les différents usages que l'on peut avoir avec le serveur NAS sont :

- **Usage multimédia :**

En activant l'option « serveur multimédia » sur le NAS celui-ci permettra d'avoir accès aux données via le réseau.

- **Gestion de vidéo surveillance :**

La marque Synology propose un service de gestion de caméra IP et donc d'enregistré ou d'afficher des enregistrement vidéo en directe.

- **Sauvegarde de données :**

La fonction première d'un serveur NAS est de sauvegarder toutes les données sans pour autant avoir une limite réelle d'espace de stockage. En cela vous protégerez donc vos données en cas d'accident entrainant leurs perte.

Le chiffrement est l'un des moyens les plus efficaces pour sécuriser des données sur un serveur NAS. Meme si des personnes mal attentionnées comme des hackeurs récupèrent les données, celles-ci seront cryptés et donc seront illisible a toutes personnes n'ayant pas de clé de déchiffrement. De plus le chiffrement des données contribue à respecter les exigences réglementaires comme par exemple celles du RGPD (protection des données).

Néanmoins si le chiffrement du NAS n'est pas correctement réalisé il peut rapidement devenir dangereux pour les données sensibles. Pour éviter une violation de données il est nécessaire de :

- **Ne chiffrer que les données nécessaires :**

En cas de trop grande quantité de données celles-ci fairont ralentir le NAS voir meme rendre le cryptage des données moins efficace. Il faudra donc catégoriser les données afin de déterminer quelles données auront le plus de répercussion en cas de perte.

- **Chiffrer les données sensibles meme celle « au repos » :**

Les données dites « au repos » sont les données qui sont stockés dans le NAS contrairement aux données qui se télécharge d'un appareil a un autre. En chiffrant ses données cela évitera qu'un pirate parvienne à contourner les restrictions d'accès ou qu'un vol matériel du NAS soit fait. Il faudra tout de meme faire attention de choisir la bonne réglementation de cryptage en fonction des differentes données.

- **Utiliser des protocoles de transfert chiffrés :**

Il est important de protéger les liens sur lequel transit les données évitant les détournements de paquets TCP/IP ou encore une écoute clandestine des données.

- **Chiffrez les sessions administrateur :**

Etant donné que les administrateurs se connecte sur leurs système NAS il est dans la logique des choses de sécurisé leur session pour éviter une violation de donnée. Pour arranger ça les administrateurs se connecte via des API (L'API est un moyen puissant et polyvalent de connecter des applications et programmes divers et variés.), des lignes de commandes ou encore d'autre outils clients.

- **Utiliser un système de VPN (Virtual privat network) :**

Un VPN est un réseaux privés virtuels, il permet d'avoir une connexion internet chiffrée. Il permettra lors d'une connexion de dissimule l'identité et l'activité en ligne d'un utilisateur, il est aussi plus difficile pour les pirates de voler des données ou de compromettre des systèmes ou encore de définir leurs contenus. Cette pratique c'est beaucoup développé lors du confinement dut au COVID-19 pour le télétravail.

Il ne faut pas oublier aussi de protéger de sensibiliser les utilisateurs à la protection des données, notamment par exemple de ne pas écrire son mot de passe sur un document texte sur le bureau ou encore sur un postite. Dans ses circonstances si une personne malveillante

récupère ses informations, meme si les données sont extrêmement bien crypté l'hackeur aura juste à rentrer les identifiant et mot de passe et pourra faire se qui bon lui semble des données concernées.