

Le NAS en entreprise : bien plus qu'un disque partagé

Serveur de fichiers, cible de sauvegarde, instantanés anti-ransomware : exploiter (et sécuriser) le couteau suisse du stockage PME.

8 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/nas-entreprise

Le NAS (Network Attached Storage) est le petit serveur de stockage des PME : fichiers partagés, sauvegardes, parfois bien plus. Bien choisi et bien réglé, c'est un excellent investissement ; laissé en configuration d'usine, c'est une cible favorite des ransomwares — les campagnes visant spécifiquement les NAS exposés sur Internet se succèdent. Le guide pour en tirer le meilleur sans en faire votre talon d'Achille.

1. Ce qu'un NAS fait bien

- Le partage de fichiers local : rapide, maîtrisé, avec des droits par dossier (bien organisés) — complément ou alternative au cloud selon les volumes
- La cible de sauvegarde centrale : postes et serveurs s'y sauvegardent, lui-même se répliquant vers le cloud (le montage 3-2-1 type)
- Les instantanés (snapshots) : la machine à remonter le temps — précieuse contre l'erreur ET le chiffrement (si l'attaquant ne peut pas les purger)
- Les extras utiles : hébergement de la vidéosurveillance, synchronisation de sites, accès distant maîtrisé — chaque service activé étant aussi une surface d'attaque à peser

2. Choisir : les critères PME

- La gamme « entreprise » des constructeurs établis (Synology, QNAP...) : baies 2 à 4 disques minimum, RAID, et un suivi de mises à jour sérieux
- Les disques en RAID (miroir a minima) : la panne d'UN disque ne coûte rien — mais le RAID n'est pas une sauvegarde
- Dimensionner large (les données doublent vite) et vérifier les fonctions qui comptent : snapshots, chiffrement, réplication cloud, journalisation
- L'onduleur associé d'office (coupures) : les NAS détestent les arrêts brutaux

3. Sécuriser : la liste non négociable

- JAMAIS exposé directement sur Internet : pas de redirection de ports vers le NAS, pas de QuickConnect/ relais constructeur pour les données sensibles — l'accès distant passe par le VPN
- Compte admin d'usine désactivé, mots de passe forts, MFA activée (les NAS modernes la proposent), comptes nominatifs
- Mises à jour du système ET des applications du NAS appliquées vite : les campagnes d'attaques suivent les failles publiées à quelques jours

- Les services inutilisés désactivés (UPnP, SSH, multimédia...) : chaque service off est une porte en moins
- Snapshots protégés en purge + réplication vers un stockage immuable/hors site : le ransomware qui prend l'admin du NAS ne doit PAS pouvoir tout effacer
- Journaux et alertes activés vers la supervision : disque malade, connexions étranges, RAID dégradé

ATTENTION

Le scénario des campagnes anti-NAS : scan d'Internet !' NAS exposé repéré !' faille connue ou mot de passe faible !' chiffrement du NAS ET de ses instantanés, demande de rançon sur l'écran de connexion. Tout, dans la liste ci-dessus, existe parce que ce scénario tourne en boucle depuis des années. Un NAS derrière VPN, à jour, avec réplication hors site, en est tout simplement sorti.

4. NAS et cloud : le bon partage des rôles

- Le duo type PME : le cloud pour la collaboration et la mobilité (la suite), le NAS pour les gros volumes locaux (production, photos/vidéos, archives) et comme maillon de sauvegarde
- Le NAS qui sauvegarde le cloud, le cloud qui sauvegarde le NAS : chacun est le hors-site de l'autre — architecture simple et très robuste
- Éviter le double emploi flou : si tout vit déjà très bien dans la suite, le NAS « parce qu'il faut un NAS » ajoute de la surface d'attaque sans valeur

L'essentiel à retenir

- 01 Interdire toute exposition directe du NAS sur Internet
 - 02 Activer MFA, comptes nominatifs, et désactiver l'admin d'usine
 - 03 Appliquer les mises à jour système et applications rapidement
 - 04 Configurer snapshots protégés + réplication hors site
 - 05 Brancher le NAS sur onduleur et supervision
 - 06 Clarifier le partage des rôles NAS/cloud
-

Questions fréquentes

Le NAS peut-il remplacer un « vrai » serveur ?

Pour le fichier, la sauvegarde et quelques services légers : oui, c'est même sa vocation en TPE/PME. Pour les applications métier lourdes (bases de données actives, ERP), le NAS dépanne mais le serveur dédié ou le cloud restent plus sains. La frontière : dès qu'une application critique tourne SUR le NAS, il en hérite les exigences (redondance, PRA, supervision renforcée).

Accès aux fichiers en déplacement : comment faire sans exposer le NAS ?

Par le VPN de l'entreprise (l'accès redevient « comme au bureau »), ou en synchronisant les dossiers nomades vers la suite cloud — beaucoup de NAS le font nativement. Les portails « pratiques » des constructeurs exposés au monde sont précisément ce que les campagnes d'attaques moissonnent : la commodité directe se paie trop cher.

Que faire d'un vieux NAS qui ne reçoit plus de mises à jour ?

Le sortir du chemin critique : plus de données de production dessus, et s'il sert encore (archives froides), l'isoler du réseau principal, hors Internet absolument. Puis planifier son remplacement — et l'effacement sérieux des disques avant toute sortie : un NAS réformé concentre des années de données de l'entreprise.

Pour aller plus loin

Cybermalveillance.gouv.fr — sécuriser ses équipements — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-objets-connectes

Cyberionis — notre service cloud & infrastructure — cyberionis.fr/#cloud-infrastructure

Un projet cloud ou d'infrastructure ?

Choix, migration, sécurisation, supervision : Cyberionis conçoit des infrastructures sobres et qui durent.
contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr