Mise en place d’une solution de type Network Attached Storage

Politique de sécurité du NAS ASSURMER

CHAMMAH GUILLAUME
DRIF WASSIM
LEGROS KYLIAN

05.03.2025

BTS SIO SISR 2B DSI

Sommaire

POLITIQUE DE SÉCURITÉ DU SERVEUR NAS

1. Application

Cette politique de sécurité vise à assurer l'intégrité, la confidentialité et la disponibilité des informations stockées sur le serveur NAS. Elle s'applique à l'ensemble des employés, prestataires et professionnels ayant accès à ces données.

2. Contrôle d’accès et authentification

- L'accès au serveur NAS est strictement réservé aux utilisateurs autorisés.
- Une authentification forte est obligatoire (mot de passe complexe et authentification à deux facteurs).
- Les droits d'accès sont attribués selon le principe du moindre privilège.
- Une journalisation des accès est mise en place pour assurer un suivi des connexions.

3. Sauvegarde et réplication des données

- Une stratégie de sauvegarde 3-2-1 est appliquée :
    - 3 copies des données (originale + 2 sauvegardes).
    - 2 supports de stockage différents.
    - 1 sauvegarde hors site.
- Des sauvegardes automatiques sont planifiées quotidiennement.
- Un test régulier de restauration est effectué pour garantir l’efficacité du dispositif.

4. Protection contre les cybermenaces

- Le firmware et les logiciels du NAS sont mis à jour régulièrement.
- Un pare-feu et un antivirus sont activés et maintenus à jour.

- La détection des comportements suspects est mise en place via des systèmes de surveillance.

5. Chiffrement des données

- Toutes les données sensibles sont chiffrées au repos et en transit.
- Les connexions distantes sont sécurisées par SSL/TLS.
- Les supports de sauvegarde externes sont chiffrés.

6. Gestion des incidents et continuité d'activité

- Un plan de reprise d'activité (PRA) est défini et testé périodiquement.
- Toute anomalie ou incident de sécurité doit être signalé immédiatement au service informatique.
- Un audit de sécurité est réalisé annuellement.

7. Sensibilisation et formation

- Une formation régulière est dispensée aux employés sur les bonnes pratiques de sécurité.
- Des campagnes de sensibilisation sont organisées pour rappeler les risques et les mesures de prévention.

8. Conclusion Cette politique doit être respectée par l'ensemble du personnel. Toute violation peut entraîner des sanctions disciplinaires. La politique est mise à jour régulièrement pour s'adapter aux nouvelles menaces et technologies.