Sécurisez vos serveurs NAS Synology exposés sur Internet

Nous avons traité plusieurs incidents impliquant des serveurs NAS de la marque Synology, des équipements largement utilisés dans les petites et moyennes entreprises. Dans la majorité des cas, les attaques se sont produites à distance, en exploitant la fonctionnalité QuickConnect et via des tentatives de connexion par force brute. Ces situations sont toutefois évitables grâce à une configuration adaptée et quelques bonnes pratiques simples. Nous vous partageons ci-dessous nos recommandations pour sécuriser vos équipements et réduire les risques à l'avenir :

Désactivation du compte admin par défaut
Le compte admin par défaut est souvent une cible privilégiée. En le désactivant et en créant un nouvel administrateur avec un nom d'utilisateur unique, vous évitez les attaques opportunistes sur ce compte.

Activation de l'authentification multi-facteur (MFA)
L'authentification multi-facteur permet de renforcer la sécurité des accès des équipements exposés sur Internet. En exigeant une deuxième forme de vérification, vous réduisez considérablement le risque d'accès non autorisé pour un compte dont les identifiants auraient été compromis.

Protection contre les attaques par force brute
Les attaques par force brute tentent de deviner les mots de passe par essais successifs. En configurant des protections telles que la limitation du nombre de tentatives de connexion, vous pouvez contrer efficacement ces menaces.

Mise à jour régulière de l'équipement
Les mises à jour régulières du firmware et des applications sont essentielles pour corriger les vulnérabilités. Dans certains cas, les attaquants sont susceptibles d'exploiter des vulnérabilités de l'OS de Synology.

Configuration du pare-feu
Activez le pare-feu de votre NAS et appliquez une règle restrictive par défaut : tout est bloqué sauf ce que vous autorisez. N'ouvrez que les ports strictement nécessaires au fonctionnement et, pour l'administration à distance, limitez l'accès uniquement aux adresses IP de confiance.

Audit de configuration sécurité avec le Conseiller de Sécurité
Utilisez l'utilitaire « Conseiller de Sécurité » fourni par Synology pour effectuer un audit complet de votre configuration. Cet outil identifie les configurations dangereuses du point de vue de la sécurité et vous propose des recommandations pour améliorer la sécurité globale de votre NAS.

En suivant ces recommandations, vous protégez vos données sensibles tout en continuant à exposer votre équipement sur Internet de manière sécurisée.