Devolutions

Pourquoi et comment vous devriez désactiver les liaisons non authentifiées LDAP dans Active Directory

ACTIVE DIRECTORY POSSÈDE DES FONCTIONNALITÉS HÉRITÉES ASSEZ OBSCURES

Depuis des décennies, le maître incontesté des environnements de réseau d'entreprise, c'est Windows Active Directory. Ce joueur est là pour rester, même si Azure Active Directory prend tranquillement sa place.

Par contre, comme pour la majorité des produits qui existent depuis longtemps, Active Directory possède des fonctionnalités héritées assez obscures qui ont l'air d'avoir été placées dans une capsule temporelle. Autrement dit, Active Directory est comme un vieux bâtiment désuet qui risque de prendre feu s'il n'est pas correctement rénové. Par exemple : les liaisons non authentifiées LDAP sont activées par défaut dans Windows Server 2019 et vous devriez penser à les désactiver.

(En passant, si vous ne voulez pas lire toutes les explications, vous pouvez passer directement à la fin de l'article où vous trouverez l'extrait du code PowerShell.)

LDAP dans Active Directory

Active Directory vient avec plusieurs services, dont le principal est le serveur LDAP (*Lightweight Directory Access Protocol*). Il regroupe des informations sur tout ce qui se trouve à l'intérieur du domaine (les utilisateurs, les groupes d'utilisateurs, les ordinateurs, les appareils, etc.). Au moment de la connexion à un domaine Windows, une partie du processus d'authentification implique l'envoi d'une demande de liaison LDAP au contrôleur de domaine pour valider les informations d'identification. Les applications tierces délèguent fréquemment l'authentification à Active Directory depuis LDAP.

Authentification LDAP

Les applications Windows classiques utilisent les fonctions intégrées pour valider les informations d'identification avec NTLM, Kerberos avec LDAP ou encore Secure LDAP (LDAPS) s'il a été configuré. Les applications tierces qui ont une prise en charge limitée de NTLM ou Kerberos peuvent, à la place, choisir d'envoyer les informations d'identification complètes en utilisant la liaison LDAP simple. Elle est similaire à l'authentification de base HTTP, mais demeure acceptée dans LDAPS grâce à la protection fournie par Transport Layer Security (TLS).

Anonyme ou non authentifié?

La liaison LDAP simple a plus d'un tour dans son sac : il est possible d'utiliser un nom d'utilisateur et un mot de passe vides pour « s'authentifier » en tant qu'utilisateur anonyme. N'importe qui peut récupérer les mêmes informations renvoyées par la commande Get-ADRootDSE de PowerShell à partir du serveur LDAP. L'authentification anonyme LDAP se produit quand le nom d'utilisateur et le mot de passe sont des chaînes vides. L'authentification non authentifiée LDAP se produit quant à elle quand le nom d'utilisateur est présent, mais que le mot de passe est vide. Bien que les deux cas soient souvent confondus, la spécification de LDAP rend **obligatoire l'authentification anonyme. L'authentification non authentifiée, elle, est facultative**. Et il est recommandé de la désactiver par défaut.

Conséquences inattendues

Si les deux cas semblent pratiquement identiques, pourquoi l'authentification non authentifiée est-elle si importante?

Étant donné que c'est rare et souvent mal compris, plusieurs développeurs ne s'attendent pas à ce que les requêtes de liaison LDAP aboutissent à un mot de passe vide. La plupart des applications qui délèguent l'authentification à LDAP s'attendent à ce que la liaison LDAP fonctionne seulement si le mot de passe correct est fourni, ce qui n'est évidemment pas le cas quand le mot de passe est vide. La véritable authentification anonyme utilise un nom d'utilisateur vide, qui est probablement intercepté par plusieurs vérifications initiales.

Est-ce que tous les développeurs pensent à vérifier les mots de passe vides? Absolument pas! Et c'est d'ailleurs à l'origine de nombreuses failles de sécurité dans le passé.

Prévenir le problème

Même s'il est préférable que les applications qui utilisent l'authentification LDAP vérifient les mots de passe vides, il est possible de désactiver les liaisons LDAP non authentifiées à partir de Windows Server 2019. L'extrait de code PowerShell suivant suffit pour effectuer la modification nécessaire :

```
$RootDSE = Get-ADRootDSE
$ObjectPath = 'CN=Directory Service,CN=Windows NT,CN=Services,{0}' -f $RootDSE.
ConfigurationNamingContext
Set-ADObject -Identity $ObjectPath -Add @{ 'msDS-Other-Settings' =
'DenyUnauthenticatedBind=1' }
```

Le mot de la fin

La liaison non authentifiée LDAP n'est pas un problème de sécurité en soi, mais ça reste le genre de fonctionnalité qui mène trop souvent à des conséquences inattendues. Les chercheurs en sécurité devraient toujours essayer d'utiliser des mots de passe vides dans les applications qui effectuent une authentification LDAP dans l'espoir de trouver une éventuelle vulnérabilité. C'est un parfait exemple d'un élément relativement facile à réparer, à condition de savoir que ça existe en premier lieu.