BARILLY
DYLAN
2SIO

Authentification

L'authentification est le processus de vérification de l'identité d'un utilisateur ou d'un système, afin de garantir qu'ils sont ce qui prétendent être et éviter les usurpations d'identités et permet d'assurer la traçabilité.
L'objectif de l'authentification est de contrôler l'accès aux ressources sensibles, telles que des données confidentielles, des systèmes informatiques, des réseaux..
L'authentification est essentielle pour assurer la sécurité, elle est utilisée dans divers domaines. Il existe plusieurs types d'authentification qui utilisent chacuns ses propres méthodes et niveaux de sécurité.

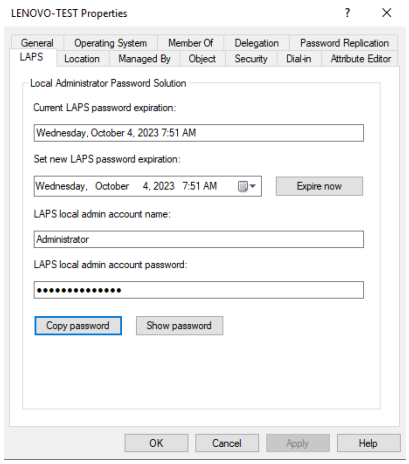
L'authentification par mot de passe, l'utilisateur doit fournir un nom d'utilisateur et son mot de passe afin d'accéder aux ressources ou à un système. Cette méthode est très courante et répandue mais ce n'est pas forcément la plus sécurisée.

L'authentification à double facteur (A2F), cette méthode ajoute une autre identification, l'utilisateur doit fournir un code généré par une application mobile, un mail ou par SMS. Cette méthode complète bien l'authentification par mot de passe.

L'authentification biométrique se base sur les caractéristiques physiologiques uniques de l'utilisateur, comme l'empreinte digitale (Touch ID) ou la reconnaissance faciale (Face ID) qui sont utilisés souvent sur les téléphones afin de vérifier l'identité de l'utilisateur qui essaye de se connecter.

Il existe d’autres types d'authentification comme celle par carte à puce, par certificat, par jeton ou bien par multi-étapes. L’authentification touche tous types de personnes dans n’importe quel domaine, mais dans une entreprise, elle est notamment plus importante surtout si on possède les droits administrateurs d’un serveur, c’est pour cela que Microsoft a créé LAPS (Local Administrator Password Solution), un outil qui permet de gérer les mots de passe des comptes administrateurs locaux sur les systèmes d’exploitations Windows.

L’objectif de LAPS est de renforcer la sécurité en garantissant que les mots de passe des comptes administrateurs locaux sont uniques et complexes, et en évitant ainsi la propagation d’identifiants d'administration par défaut ou partagés.
Avec LAPS, les mots de passe des comptes administrateur locaux sont générés de manière aléatoire, stockés de manière sécurisée directement dans l’Active Directory de l’entreprise et attribués individuellement à chaque ordinateur. Les administrateurs peuvent récupérer ces mots de passe au besoin, en utilisant simplement l’outil LAPS fourni par Microsoft. Cette utilisation permet de réduire les risques liés à l’utilisation de mots de passe par défaut ou partagés, renforçant ainsi la sécurité des systèmes Windows et des réseaux d’entreprise.



L’installation de LAPS se fait à partir d’un package à télécharger. Une fois l’installation faite, la configuration se fait sur un contrôleur de domaine via stratégie de groupe. Cette stratégie doit s’appliquer sur les utilisateurs sur lesquels vous souhaitez utiliser LAPS donc les administrateurs locaux. Il faut aussi s’assurer que les personnes ayant la stratégie de groupe LAPS aient aussi la possibilité de voir les mots de passe générés.

Cependant les utilisateurs aussi doivent avoir un bon moyen de s’authentifier tout en étant sécurisé.

En effet, pour une authentification avec mot de passe, tout dépend des droits qu’ils disposent au sein d’une entreprise, les utilisateurs avec privilèges auront d’autres spécificités de mot de passe comparé à des utilisateurs standards. Chacun a des droits différents. Dans l’Active Directory, il faut faire une GPO et se rendre dans l'éditeur de gestion de stratégie de groupe, après ceci il faudra se rendre dans la stratégie de mot

de passe afin de définir les caractéristiques des mots de passe en fonction des privilèges des utilisateurs. Des recommandations de l'ANSSI telle qu'un mot de passe utilisateur devrait faire minimum 8 caractères et qui devra être changé tous les mois. Tandis qu'un mot de passe administrateur devrait faire minimum 12 caractères et devra être changé tous les 3 mois.

Chaque problème a une solution, mais celle-ci peut être plus ou moins sécurisée en fonction de son importance et des dégâts que cela peut produire en cas d'attaque.