Vaissiere Dylan

# Compte rendu Y Days 18/11/20

Veille Technologique :

Veille Technologique sur les différentes cyberattaques, notamment les ransomwares et comment s’en protéger en entreprise.

Les ransomware sont des logiciels malveillants qui infectent votre ordinateur et affichent des messages demandant de verser une certaine somme afin que votre système fonctionne à nouveau. Cette catégorie de programmes malveillants est une arnaque lucrative et criminelle qui peut être installée en cliquant sur des liens trompeurs dans un e-mail, via la messagerie instantanée ou un site Internet. Les ransomware ont la capacité de verrouiller l’écran d’un ordinateur ou de chiffrer sdes fichiers importants prédéfinis avec un mot de passe.

Sécurité des droits NTFS sur active directory :

Création de fichiers sur un utilisateur pour partager des fichiers et les sécurisés. (Sécurité système)

Les permissions de partage s’appliquent uniquement pour les partages réseaux et ne s’appliquent donc pas aux utilisateurs ayant un accès local au dossier (accès à l’explorateur de fichiers sur le serveur de fichiers, par exemple lors d’un accès à un bureau à distance). On peut les définir sur trois niveaux :

Il est aussi important de comprendre la notion suivante : **Chaque niveau d’autorisation contient une partie des autorisations de son parent.**

* + - **Lecture :** voir les fichiers et les dossiers, ouvrir un fichier ou un dossier, exécuter un programme.
    - **Modification :** en plus des droits de lecture, ce droit donne également la possibilité d’ajouter des fichiers, créer des dossiers, modifier les fichiers et de supprimer les fichiers et les dossiers.
    - **Contrôle total :** les droits de modification et de lecture avec en plus la possibilité de modifier les permissions NTFS sur les dossiers et les fichiers.

Pour faire court, la permission de partage est celle qui affecte le “browsing” de la ressource (\\LeNomDuServeur\LeNomDuPartage), j’ai pour habitude de mettre les partages en “modifications”, sauf dans des cas bien précis ou un applicatif aurait besoin du contrôle total, mais ceci reste rarissime.

Les permissions NTFS définissent les droits de l’utilisateur sur l’objet lui-même, que celui-ci soit accédé par le réseau (\\NomDeServeur) ou localement (C:\MaRessource). On peut les définir sur l’objet (droit **explicite**) ou bien **par héritage** de l’objet parent (schématiquement, on prend une pyramide, et les droits s’appliquent, de la pointe, vers la base) et lui attribuer une **autorisation** ou une **interdiction**, l’interdiction prévalant **toujours** sur l’autorisation et le droit explicite prévalant toujours sur le droit hérité.

Par défaut, il existe six groupes de permissions NTFS prédéfini. Ces groupes de permissions correspondent en réalité au groupement de droits spéciaux ; on les utilise pour les droits « classiques ».