RAPPORT D'ACTIVITÉ

Mise en œuvre d'une campagne de sensibilisation à la cybersécurité via les stratégies de groupe (GPO)

TABLE DES MATIÈRES

CONTEXTE PROFESSIONNEL

La mission s'inscrit au sein de la Mairie de Castelginest gérant quotidiennement des flux de données sensibles relatifs à l'état civil, l'urbanisme et aux finances publiques. Dans un environnement technologique basé sur une infrastructure Active Directory sous Windows Server, le parc informatique est composé de nombreux postes clients répartis dans différents services administratifs. Le constat de départ est simple : malgré les protections techniques en place (antivirus, pare-feu), les agents municipaux présentent une faible acculturation aux risques cyber. Dans ce contexte, ma mission consiste à transformer l'ouverture de session, geste quotidien et automatique, en un levier de sensibilisation permanent pour renforcer la sécurité globale de la structure face aux menaces telles que le phishing ou l'ingénierie sociale.

LA SITUATION

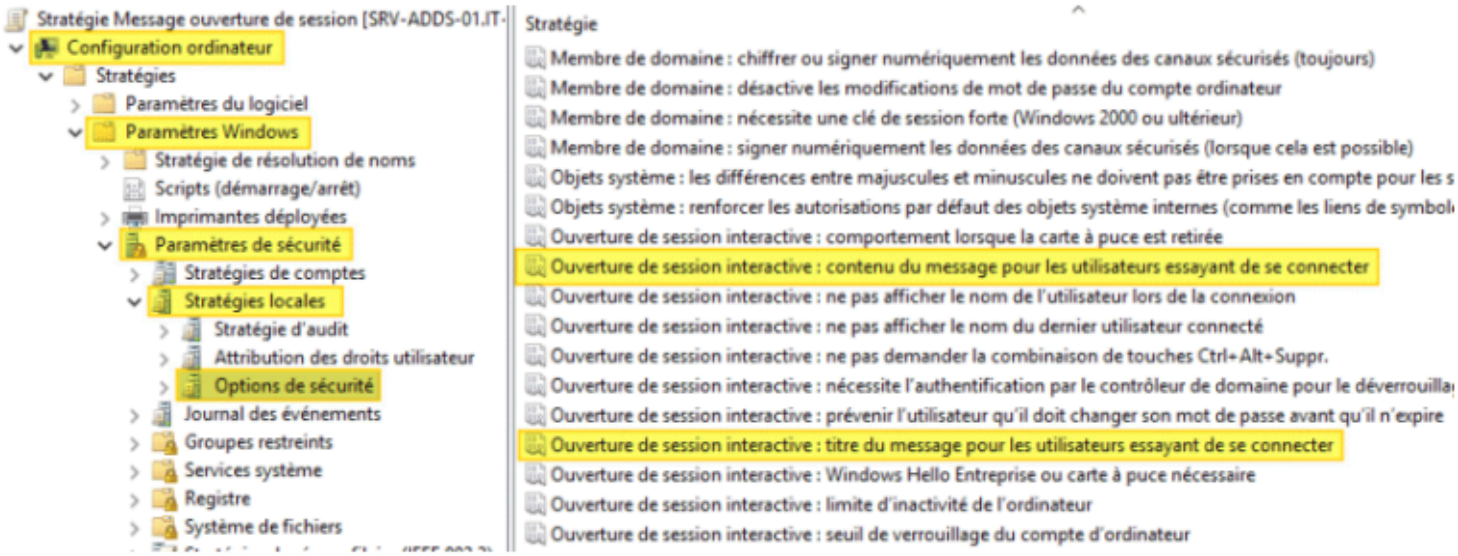
Le projet porte sur le déploiement d'une solution de communication directe sur les postes de travail sans installation de logiciel tiers. L'objectif principal est d'imposer la lecture de consignes de sécurité critiques avant même que l'utilisateur n'accède à son environnement de travail. Pour ce faire, j'ai adopté une démarche structurée : j'ai d'abord synthétisé les bonnes pratiques informatiques en messages courts et percutants, couvrant des thématiques variées comme la complexité des mots de passe, la vigilance sur les périphériques USB et la sécurisation du télétravail. Techniquement, j'ai utilisé l'outil Gestion des stratégies de groupe (GPO) pour configurer deux paramètres spécifiques dans les options de sécurité des stratégies locales. Cette GPO, nommée "Message ouverture de session", a été liée à l'Unité d'Organisation (OU) regroupant les ordinateurs de la mairie, garantissant ainsi une application uniforme de la politique de sécurité.

CONFIGURATION DE LA GPO

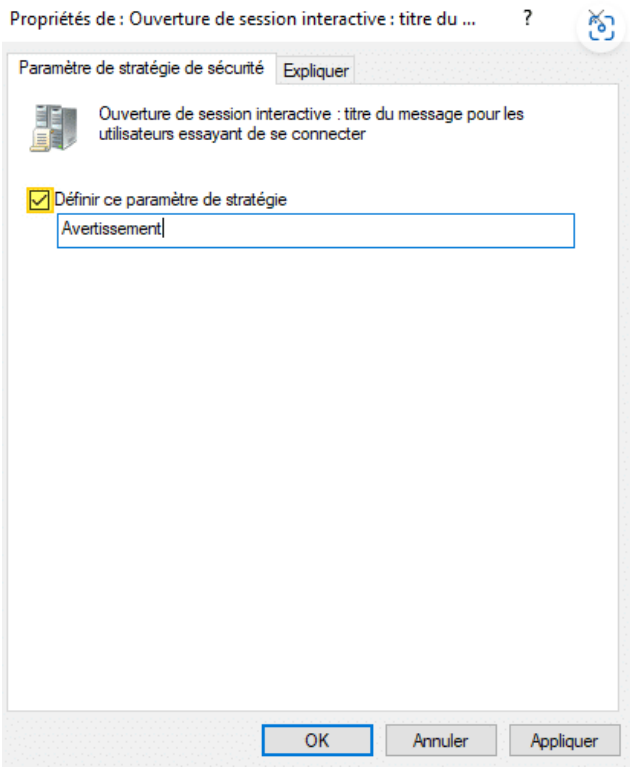
La mise en place de ces messages de sensibilisation avant la connexion de l'utilisateur implique la modification de deux paramètres, l'un pour définir le titre de message, et l'autre pour définir le contenu du message. Pour cela, créez une nouvelle GPO qui doit s'appliquer sur des objets "ordinateurs". Pour ma part, ce sera la GPO "Message ouverture de session" et elle sera liée à l'OU PC de l'annuaire Active Directory.

Ensuite, parcourez les paramètres de cette façon : « Configuration ordinateur », « Paramètres Windows », « Paramètres de sécurité », « Stratégies locales » et « Options de sécurité ». A cet emplacement, il y a deux paramètres intéressants :

- Ouverture de session interactive : titre du message pour les utilisateurs essayant de se connecter.
- Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter.

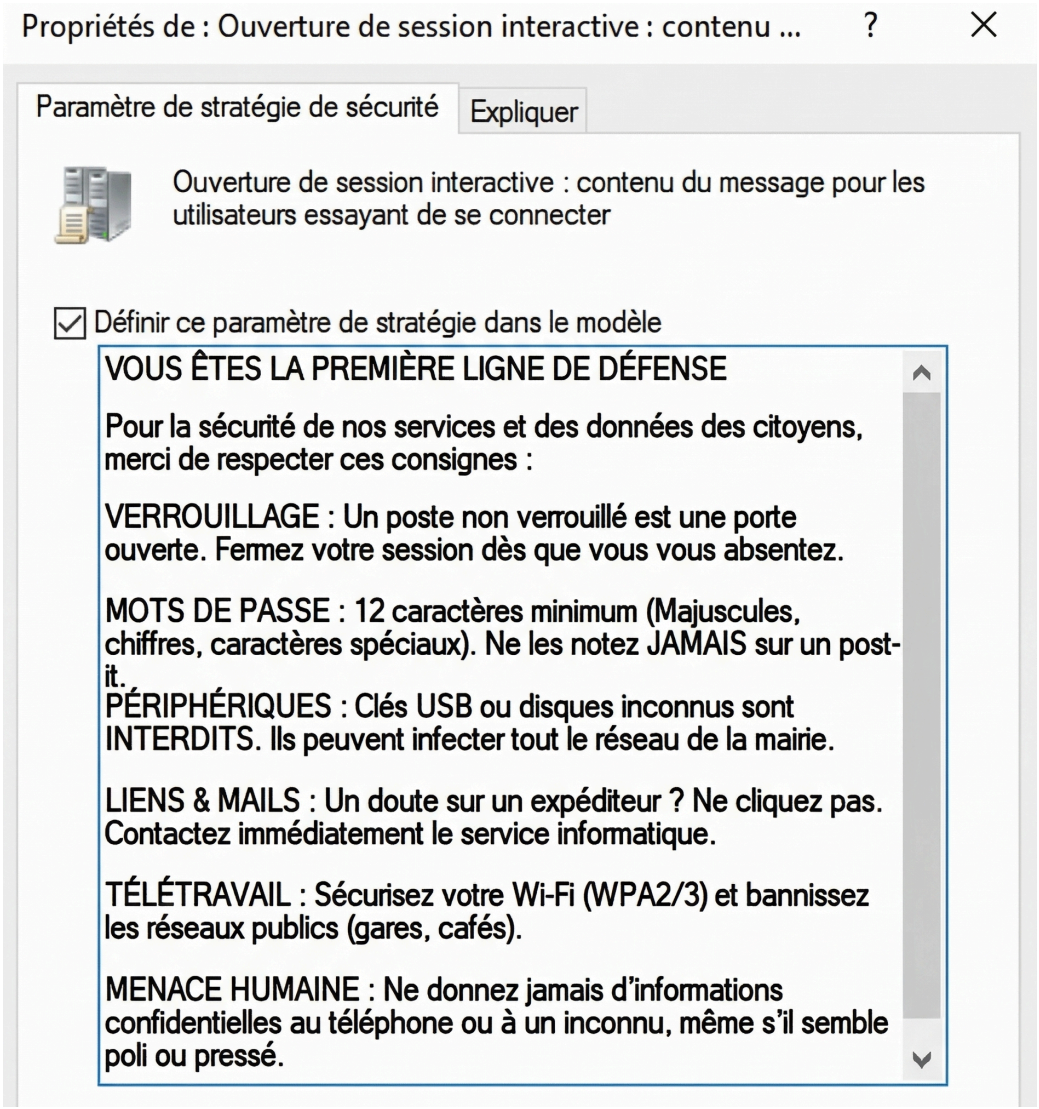


Commençons par le paramètre permettant de configurer le titre, qu'il suffit d'éditer, d'activer en cochant l'option "**Définir ce paramètre de stratégie**" et de renseigner en indiquant le titre dans la zone de saisie :



Sur exactement le même principe, le second paramètre va permettre de définir le contenu du message. Je vais indiquer les messages au préalable :

```
VOUS ÊTES LA PREMIÈRE LIGNE DE DÉFENSE

Pour la sécurité de nos services et des données des citoyens, merci de
respecter ces consignes :

VERROUILLAGE : Un poste non verrouillé est une porte ouverte. Fermez votre
session dès que vous vous absentez.

MOTS DE PASSE : 12 caractères minimum (Majuscules, chiffres, caractères
spéciaux). Ne les notez JAMAIS sur un post-it.

PÉRIPHÉRIQUES : Clés USB ou disques inconnus sont INTERDITS. Ils peuvent
infecter tout le réseau de la mairie.

LIENS & MAILS : Un doute sur un expéditeur ? Ne cliquez pas. Contactez
immédiatement le service informatique.

TÉLÉTRAVAIL : Sécurisez votre Wi-Fi (WPA2/3) et bannissez les réseaux
publics (gares, cafés).

MENACE HUMAINE : Ne donnez jamais d'informations confidentielles au
téléphone ou à un inconnu, même s'il semble poli ou pressé.
```



La GPO est prête !

L'ÉVALUATION DE LA RÉALISATION

Cette réalisation permet de valider plusieurs compétences clés. D'un point de vue technique, j'ai démontré ma capacité à administrer des systèmes informatiques en manipulant les objets de stratégie de groupe. Sur le plan de la protection des données, cette action répond aux exigences de la CNIL et du RGPD en matière d'information et de sensibilisation des personnels. Le succès de la mission est confirmé par l'apparition systématique d'une boîte de dialogue interactive lors de la connexion, obligeant l'agent à acquitter les conseils de vigilance. Cela crée une barrière psychologique préventive et valorise le rôle du service informatique comme accompagnateur du changement.

BILAN PERSONNEL

Cette expérience a été particulièrement enrichissante car elle m'a permis de comprendre que la cybersécurité ne se limite pas à des configurations matérielles complexes, mais repose en grande partie sur le facteur humain. J'ai dû faire preuve d'esprit de synthèse pour transformer des règles techniques en messages accessibles à des profils non-techniciens. La principale difficulté a été de trouver un équilibre entre la fermeté des consignes et la fluidité de l'expérience utilisateur, afin que ce message soit perçu comme une aide plutôt que comme une contrainte. Ce projet renforce ma conviction que la communication est un outil de défense au moins aussi puissant que les solutions logicielles au sein d'une administration.