

MAÎTRISER L'ACCÈS À L'INFORMATION

Cas de l'entité Investissements d'une banque d'affaires, en pleine expansion à l'international

EXIGENCES

Toutes les données de la structure sont centralisées sur **un même serveur de fichiers**, qui est répliqué pour gérer efficacement les ressources. **Chaque utilisateur possède un dossier sur le serveur de fichiers** dans lequel il travaille et sauvegarde des données quotidiennement. **Chaque service possède également un dossier réservé**, jusqu'alors uniquement cloisonné avec les droits Microsoft.

L'assurance que les données de cette banque - actuellement accessibles pour l'équipe IT - soient **uniquement intelligibles par les personnes habilitées** est indispensable. La solution ne doit **pas pour autant impacter les tâches de l'équipe IT**.

SOLUTION

La solution **ZONECENTRAL** a été retenue pour ce projet, permettant en effet de chiffrer :

- + Tous les lecteurs réseau Y: menant aux dossiers personnels des utilisateurs sur le serveur de fichiers ;
- + Les dossiers « Bureau », « Mes Documents » et TEMP des utilisateurs ;
- + Les différents dossiers de chaque service sur le serveur de fichiers.

EXPÉRIENCE

ORGANISATION

Afin d'assurer la réussite de cette élévation dans la sécurité, la structure a mis en place une organisation interne visant à séparer intégralement les rôles de la Direction des Systèmes d'Information et ceux de l'équipe Sécurité des Systèmes d'Information. Plusieurs procédures ont été mises en place entre les équipes DSI et SSI afin de s'assurer qu'aucune d'elles n'aient les pleins pouvoirs sur les données chiffrées.

Deux équipes sont ainsi concernées :

- + L'équipe 1, dépendante de la DSI, affecte et retire des droits de modification et de lecture à l'autre équipe, avant et après leurs interventions ;

- + L'équipe 2 du SSI, détermine les zones à chiffrer ou à laisser en clair et dispose également le droit d'ajouter et de retirer des accès cryptographiques dans les zones chiffrées.

SERVICE IT

Le service IT a assuré le déploiement du produit et des politiques de sécurité via GPO. Il assure la gestion des fichiers (sauvegarde et restauration) ainsi que la gestion des droits Microsoft des utilisateurs et des membres de l'équipe SSI.

SERVICE SSI

Lorsque qu'une modification dans la gestion du chiffrement de **ZONECENTRAL** (ajout/suppression d'accès, création de zone en clair...) est nécessaire, une demande par e-mail adressée au service SSI est obligatoire. Suite à cet échange, l'équipe SSI demande à l'IT de lui octroyer des droits de modifications à l'emplacement souhaité, pour effectuer l'intervention.

UTILISATEURS

Les utilisateurs sont sollicités uniquement pour la saisie du code PIN de leur SmartCard à l'ouverture de session.

AVANTAGES

Le chiffrement mis en place avec **ZONECENTRAL est transparent pour les utilisateurs** : leurs habitudes de travail au quotidien ne sont pas impactées. De plus, la solution permet **le cloisonnement technique total des rôles** de chaque équipe et permet ainsi la protection des données sensibles, en interne comme en externe. Enfin, les politiques de sécurité mises en place sont complémentaires aux droits NTFS Microsoft.



ZONCENTRAL