USE CASE

ZONECENTRAL

MANAGING ACCESS TO INFORMATION

Case of the Investments entity of a merchant bank, which is expanding internationally

REQUIREMENTS

All the structure's data is centralised on **the same file server**, which is replicated to ensure efficient resource management. **Each user has a folder on the file server** on which they work and save data daily. **Each service also has a reserved folder**, which until now had only been partitioned off with Microsoft rights.

It is however vital to ensure that this bank's data - currently accessible to the IT team - is **exclusively intelligible to authorised personnel**. Yet, at the same time, the solution **must not affect the tasks of the IT team**.

SOLUTION

The **ZONECENTRAL** solution was chosen for the project, since it enables encryption of:

- all Y: network drives leading to the personal folders of users on the file server;
- the "Desktop", "My Documents" and TEMP folders of users;
- the different folders of each department on the file server.

EXPERIENCE

ORGANISATION

In order to ensure the success of this security ramp-up, the structure has organised itself internally so as to fully separate the roles of the Information Systems Department (ISD) from those of the Information Systems Security (ISS) team. Several procedures have been put in place between the ISD and ISS teams to ensure that neither of them has full authority over the encrypted data.

This therefore concerns two teams:

- Team 1, dependent on the ISD, assigns and withdraws read and write permissions for the other team, before and after their interventions.
- Team 2, of the ISS, determines the zones to be encrypted or left unencrypted and also has the right to add and remove cryptographic accesses in the encrypted zones.

IT DEPARTMENT

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.

SSI DEPARTMENT

When a change is required in the encryption management of **ZONECENTRAL** (addition/removal of accesses, creation of unencrypted zones, etc.), an e-mail request must be sent to the ISS department. Following this exchange, the ISS team will ask IT to grant it modification rights to the desired location in order to carry out the intervention.

USERS

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

BENEFITS

The encryption established with **ZONECENTRAL** is **transparent to users**: their daily working habits are unaffected. Furthermore, the solution enables **the total partitioning-off of the roles** of each team, thereby protecting sensitive data, both internally and externally. Lastly, the security policies put in place are designed to complement Microsoft NTFS rights.

2023.06

PRIMX
MAKE ENCRYPTION HAPPEN
business@primx.eu - Tel: +33 (0)1 40 95 24 80
Head Office : 18 Rue du Général Mouton-Duvernet, 69003 Lyon / Sales Department : 21 Rue Camille Desmoulins, 92130 Issy-les-Moulineaux
www.primx.eu