PROTECTING WORKSTATIONS AGAINST THEFT AND INTERNAL THREATS

A Major French Car Manufacturer

The employees of this major car manufacturer regularly handle sensitive data: development strategies; commercial, research and development information. Any workstation might contain a significant volume of data, and the theft of this information may have serious short or long-term consequences.
In addition, the employees are encouraged also to save their data on file servers (in a «My Documents» folder), the management of which is outsourced. Executive management wants to obtain the guarantee that any theft or malicious action on the part of an operator cannot have any consequences and will not entail the disclosure of any of the company's digital assets.

ZONECENTRAL

Requirements

All the data produced and consumed by the users, whether on the workstation or in the *«My Documents»* network folder, must be secured and reserved for those entitled to access them. The IT services, whether internal or external, must be able to continue exercising their activity, in particular backups, without constraints, but must never have access to the user data.
The solution must be transparent for the users, and necessitate as little interaction as possible with them.
To guarantee a high security level, a cryptographic token must be used for containing the user access key.

Solution

The client deployed the **ZoneCentral** encryption solution.
The encrypted data are:
+ **the local profile of the user, containing in particular the desktop and the application data, such as email files;**
+ **the «My Documents» folder, on the file server (NAS).**

The system data remain unencrypted, enabling the IT services to conduct maintenance. On the file servers, the encryption has no impact on the activities of the facilities manager.
In order not to disturb the users, the initial encryption of the information takes place as a background task. Users are simply called upon to enter the PIN code of the cryptographic token.

Experience

IT SERVICES
Deploying on the workstations.

USERS
Entering the token PIN code when accessing encrypted data.

SECURITY DEPARTMENT
Defining the security policies.

Benefits

The implementation of **ZoneCentral** has made it possible to protect user data without having an impact on the existing IT processes, except for a few adjustments for **backing up the data, which themselves remain encrypted.**
The impact on users is minimal, since the accessed data are decrypted **transparently** and with no tangible loss of performance.
ZoneCentral is a product certified CC EAL3+, Qualified by the French ANSSI, and allowed for NATO Restricted and EU Restricted.

Next steps

Ultimately, the client would also like to use the token for Active Directory authentication, and implement Single Sign-On with the **ZoneCentral** solution: one-time entry of the PIN code for opening the Windows session and accessing the encrypted data.

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu – Tel.: 01 77 72 64 80
Head Office: 27 rue Maurice Flandin 69003 LYON
Sales Department: 117 avenue Victor Hugo 92100 BOULOGNE BILLANCOURT

www.primx.eu