MANAGING THE SECURITY POLICIES OF WORKSTATIONS

A Major French Aeronautics and Defence Group

This major French Corporation is involved in highly sensitive sectors, often relating to Defence. It manages and undertakes large-scale projects for which data confidentiality is imperative. Its clients provide it with access to information that may be classified, and it must guarantee the level of protection by using security software that is qualified for this security level.

ZONECENTRAL CRYHOD

Requirements

The data stored on the workstations and on portable media (USB sticks or hard disks) must remain inaccessible to unauthorised persons. It must be impossible for users to save unprotected data on a portable device.
Furthermore, the security policies must be determined by the security managers, and must be unmodifiable by the IT teams, whatever their system and network rights.
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:
+ all the local partitions on the workstation;
+ the inserted USB sticks and hard disks: the devices must be encrypted for users to be able to save data on them.
The system data remain unencrypted, enabling the IT services to conduct maintenance. The **ZoneCentral** Security Policies are digitally signed by the security manager: the security choices made are sealed and cannot be deleted or modified by other persons, even if they have high-level system administration rights.
A disk encryption (or surface encryption) solution from a third-party publisher is also in place, and undertakes authentication in the pre-boot phase.

Experience

IT SERVICES
Deploying on the workstations.

USERS
Entering the token PIN code when accessing encrypted data; encryption prompt each time a removable device is inserted.

SECURITY DEPARTMENT
Defining and signing the security policies.

Benefits

Since **ZoneCentral** is a product certified CC EAL3+, Qualified by the French ANSSI, and allowed for NATO Restricted and EU Restricted, it meets the Security Requirements for the highly-sensitive projects that are carried out.
The impact on users is minimal, and this enables them to protect removable devices with ease when they need to move around with confidential files.
Lastly, the choice of security parameters is ring-fenced by the cryptographic signature of the Security Officers, and guarantees the global and controlled deployment of policies.

Next steps

The client would like to replace the 3rd party surface encryption solution with **Cryhod**, in order to put in place a Single Sign-On function with **ZoneCentral**. Once the cryptographic token PIN code is entered for Cryhod authentication, the authentication phases at Windows login and in ZoneCentral are automatic, with no need to re-enter the PIN.

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