PROTÉGER LES POSTES DE TRAVAIL CONTRE LE VOL ET LA MENACE INTERNE

Un grand industriel français dans le domaine de l'automobile

Les employés de ce grand constructeur automobile manipulent régulièrement des informations sensibles : stratégies de développement, informations commerciales, recherche et développement. Le moindre poste de travail renferme un volume de données conséquent et le vol de ces informations peut avoir des conséquences graves, à court ou long terme.
De plus, les employés sont encouragés à enregistrer leurs données également sur des serveurs de fichiers (dans un dossier « Mes Documents »), dont l'infogérance est externalisée.
La direction générale veut avoir la garantie qu'un vol ou qu'une action malveillante d'un opérateur ne puisse pas avoir de conséquences et ne divulgue rien du patrimoine numérique de l'entreprise.

ZONECENTRAL

Exigences

Toutes les données produites et consommées par les utilisateurs, qu'elles soient sur le poste de travail ou sur le dossier réseau « Mes Documents » doivent être sécurisées et réservées aux ayant-droits.
Les services IT, qu'ils soient internes ou externes, doivent continuer à exercer sans contraintes leur activité, notamment la sauvegarde mais ne doivent jamais avoir accès aux données de l'utilisateur.
La solution doit être transparente pour l'utilisateur, et nécessiter le moins d'interactions possible avec celui-ci. Pour garantir un niveau de sécurité élevé, un token cryptographique doit être utilisé pour contenir la clé d'accès de l'utilisateur.

Solutions

Le client a déployé massivement la solution de chiffrement **ZoneCentral.**
Les données chiffrées sont :
+ **le profil local de l'utilisateur, qui contient notamment le bureau et les données d'application, comme les fichiers de mails,**
+ **le dossier « Mes Documents » sur le serveur de fichier (NAS). Les données système restent non chiffrées, et permettent aux services IT d'effectuer la maintenance.**

Sur les serveurs de fichiers, le chiffrement n'a aucun impact sur ses activités de l'exploitant.
Pour ne pas perturber les utilisateurs, le chiffrement initial des informations s'effectue en tâche de fond. L'utilisateur est sollicité uniquement pour saisir le code PIN du token cryptographique.

Expérience

SERVICES IT
Déploiement sur les postes de travail.

UTILISATEURS
Saisie du code PIN du token lors de l'accès aux données chiffrées.

DÉPARTEMENT SÉCURITÉ
Définition des politiques de sécurité.

Avantages

La mise en œuvre de **ZoneCentral** a permis de protéger les données de l'utilisateur sans avoir d'impact sur les processus existant de l'IT, à l'exception de quelques ajustements pour **la sauvegarde des données, qui demeurent chiffrées.**
L'impact sur les utilisateurs est minime, car les données accédées sont déchiffrées de manière **transparente** et sans baisse sensible de performance.
ZoneCentral est un produit certifié CC EAL3+, Qualifié Standard par l'ANSSI, autorisé pour NATO Restricted et EU Restricted.

Étapes suivantes

À terme, le client souhaite également utiliser le token pour l'authentification ActiveDirectory, et mettre en place du Single Sign On avec la solution **ZoneCentral** : une seule saisie de code PIN pour ouvrir la session Windows et accéder aux données chiffrées.

PRIMX
MAKE ENCRYPTION HAPPEN

business@primx.eu – Tél. : 01 77 72 64 80
Siège social : 27 rue Maurice Flandin 69003 LYON
Direction commerciale : 117 avenue Victor Hugo 92100 BOULOGNE BILLANCOURT

www.primx.eu