PROTÉGER LES SECRETS DE CONCEPTION ET COMMERCIAUX EN MOBILITÉ

Un grand constructeur aéronautique veut éviter l'espionnage industriel et commercial

Ce constructeur aéronautique a identifié deux corps de métiers amenés à se déplacer régulièrement dans le monde entier avec des données confidentielles telles que des données de conception ou des informations commerciales sensibles : les techniciens de maintenance et les ingénieurs commerciaux.

ZONECENTRAL CRYHOD

Exigences

La sécurité des données présentes sur le poste de travail doit être assurée en cas de vol ou de copies de disque dur réalisées à l'insu de l'utilisateur (exemple : ordinateur déposé au coffre d'un hôtel).
Les postes de travail sont hétérogènes : PC portables haut de gamme, tablette 2 en 1 de type Surface Pro, tablettes tactiles durcies pour un environnement d'atelier.
L'accès par VPN aux partages réseau doit assurer que l'utilisateur possède, en plus des droits d'accès Windows, le **droit d'en connaître**.
L'équipe sécurité impose impérativement que tout poste qui sort de la société soit **intégralement chiffré**.
Pour garantir un niveau de sécurité élevé, un token cryptographique (carte à puce ou équivalent USB) doit être utilisé pour contenir la clé d'accès de l'utilisateur. Ce token était déjà utilisé au sein de l'entreprise pour l'identification Windows.

Solutions

Le client a déployé Cryhod et ZoneCentral sur les tablettes durcies des opérateurs et les PC portables haut de gamme de la flotte commerciale. Les produits Prim'X permettent de s'interfacer avec tout type de tokens, et un certificat dédié aux opérations de chiffrement a été ajouté au token déjà utilisé au sein de l'entreprise pour l'identification Windows.
Un technicien de l'équipe sécurité prépare le poste et le chiffre avec **Cryhod**. Il ajoute ensuite l'accès cryptographique de l'utilisateur final avant de remettre le poste intégralement chiffré en main propre.
Les données chiffrées sont :
+ les partitions du poste de travail,
+ et les partages réseau accédés via le VPN.
Pour améliorer l'expérience utilisateur, le contexte cryptographique est partagé entre **Cryhod** et **ZoneCentral** ce qui évite des saisies de PIN redondantes. L'utilisateur saisit une seul fois son PIN de token au démarrage de la machine pour travailler sur ses données sensibles chiffrées.

Expérience

SERVICES IT
Déploiement télédistribué sur les postes de travail de **Cryhod** et **ZoneCentral**.

UTILISATEURS
Saisie unique du code PIN du token au démarrage du poste.

DÉPARTEMENT SÉCURITÉ
Génération d'un certificat de chiffrement par utilisateur.

Avantages

Cryhod et **ZoneCentral** partagent le contexte cryptographique et facilitent l'expérience de l'utilisateur aussi bien pour l'utilisation de tous les jours que pour les opérations de renouvellement d'accès cryptographique.

Étapes suivantes

Le client souhaite étendre la solution **Cryhod** aux opérateurs IT d'astreinte en leur distribuant des clés Windows To Go chiffrées avec **Cryhod To Go**. Le but est de remplacer les PC portables de prêts par des clés USB bootables chiffrées dont le coût est plus faible.

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