MobilitÃ© : La maÃ®trise des terminaux mobiles impose d'avantage.
MobilitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 25/2/2013 13:00:00

Le MDM est incontestablement un nouvel axe stratÃ©gique pour les entreprises. La mise en place dâ□□un projet de mobilitÃ© ne peut souffrir dâ□□une gestion de la sÃ©curitÃ© approximative voire absente.

Il est donc utile de bien structurer sa dÃ©marche projet et dâ□□adopter de bonnes pratiques. Nous allons aborder ces derniÃ¨res dans une sÃ©rie dâ□□articles dâ□□Opinion et dÃ©buter cette initiative avec une premiÃ¨re analyse sur lâ□□importance de la maÃ®trise des terminaux utilisÃ©s par les collaborateurs.

Dans ce contexte, il est nÃ©cessaire de suivre sept Ã©tapes pour arriver Ã bon port, afin de maÃ®triser la sÃ©curitÃ© des terminaux mobiles et dÊ¼encadrer le phÃ©nomÃ¨ne du BYOD (bring your own device).

Anayse de Risque : Planifiez le parcours, formez lÊ¼Ã©quipage

LÊ¼analyse des risques donne le cap. Elle permet de cerner le pÃ©rimÃ¨tre fonctionnel requis, de dÃ©finir les Ã©tapes et les Ã©lÃ©ments de confiance en fonction des activitÃ©s mÃ©tiers. Votre task force rÃ©unit DSI, support technique, DRH et responsable dÊ¼Ã©quipe nomade, tous parÃ©s Ã encadrer leurs collÃ¨gues aux usages conformes des terminaux mobiles.

Data leakage : DÃ©finissez une hiÃ©rarchie dâ□□accÃ¨s aux donnÃ©es

On le sait, la prÃ©occupation majeure des DSI et RSSI en matiÃ¨re de mobilitÃ© est la perte de donnÃ©es embarquÃ©es sur les terminaux. Classez vos donnÃ©es selon leur confidentialitÃ© pour lÊ¼organisation. DÃ©finissez vos rÃ¨gles dÊ¼accÃ¨s (groupes, mots de passe, authentification, chiffrement) et sÃ©lectionnez les terminaux mobiles ou systÃ¨mes (OS) Ã©ligibles dans vos cas dâ□□usage.

Support : Organisez le soutien technique.

Vos groupes dÊ¼utilisateurs mobiles, leurs terminaux et modes dÊ¼accÃ¨s une fois dÃ©finis, Ã©tablissez les procÃ©dures de support et rÃ©digez les guides de terrain adaptÃ©s Ã chaque communautÃ©.

m-UTM : Personnalisez lâ□□infrastructure mobile

Les comportements autorisÃ©s/interdits en mobilitÃ©, comme lÊ¼Ã©dition ou le tÃ©lÃ©chargement de fichiers, sont traduits en politiques de sÃ©curitÃ© m-UTM (Mobile Unified Threat Management). Ce boÃ®tier, placÃ© en DMZ dans le rÃ©seau dÊ¼entreprise, offre les fonctions de gestion (enrÃ´lement, provisioning, ..) et de MSM (mobile security management) : politiques, chiffrement, NAC, pare-feu, VPN, IPS... . Il permet la supervision et le contrÃ´le unifiÃ©s de lÊ¼infrastructure et de toute la flotte de terminaux mobiles, tablettes et smartphones compris.

Planifiez la synchronisation et la protection des donnÃ©es.

LÊ¼infrastructure de lÊ¼entreprise est le meilleur endroit pour consolider la protection et assurer la

synchronisation de contacts, donnÃ©es et dÊ¼applications embarquÃ©es sur tablettes et smartphones.

Forensic : Surveiller les flux critiques et gÃ©rer la tracabilitÃ©

LÊ¼Ã©quipement m-UTM enregistre tous les accÃ¨s au systÃ¨me dÊ¼informations. Ses rapports statistiques temps rÃ©el et sa console dÊ¼administration contribuent Ã aux activitÃ©s de forensics mais aussi Ã tracer les flux, Ã vÃ©rifier leur conformitÃ© et Ã rÃ©soudre les incidents.

Conformance : Mener un audit rÃ©gulier

Avec ces tests de conformitÃ© aux rÃ¨gles de sÃ©curitÃ©, il renforce le systÃ¨me dÊ¼information mobile.

Ces premiÃ¨res pistes sont les axes fondateurs de la dÃ©marche et permettent dâassurer Ã un projet de MDM de ne pas exposer la sociÃ©tÃ© et ses utilisateurs Ã des risques majeurs.