Travail à distance : quels moyens pour limiter les risques de fuite de données ?

Pour beaucoup, il est devenu courant de travailler en déplacement, mais les risques que cela implique en matière de sécurité sont souvent négligés.

Dans le cadre du Régime Général de Protection des Données (RGPD), la perte d'un appareil mobile professionnel contenant des données personnelles constitue une défaillance, passible d'amendes allant jusqu'à 20 millions de dollars ou 4 % du chiffre d'affaires annuel mondial. De toute évidence, les conséquences de la perte d'un ordinateur portable ou d'un téléphone par un employé n'ont jamais été aussi lourdes.

Malheureusement, il est impossible d'empêcher les employés de perdre leurs appareils mobiles à 100 %. La tentation est forte de limiter le travail sur mobile pour minimiser le risque de perte de données ou d'amende, mais cela risque d'impacter la productivité et la satisfaction des employés. La plupart des employés attendent une certaine souplesse dans leur travail, et la journée de travail de 9 h à 17 h se raréfie. Il est donc crucial que les organisations mettent en place des politiques et prennent des mesures de sécurité pour les télé-travailleurs et les travailleurs mobiles, dans l'optique de réduire le risque de perte de données.

Le travail mobile nécessite une règlementation spécifique

Les employés doivent recevoir une information claire sur les procédures et les meilleures pratiques de leur organisation en matière de télétravail et de travail mobile. La politique de sécurité et de sensibilisation doit couvrir plusieurs points essentiels, notamment :

- Les applications et actifs auxquels l'accès est autorisé à partir des appareils mobiles
- Les contrôles de sécurité minimum pour ces appareils
- Les composants fournis par l'entreprise, comme les certificats SSL pour l'authentification des appareils
- Les droits de l'entreprise à altérer l'appareil, par exemple en effaçant à distance les appareils perdus ou volés. Cela comprend la responsabilité de l'entreprise par rapport aux données personnelles d'un employé, si un appareil devait être effacé par mesure de précaution. Cela comprend aussi la responsabilité de l'employé par rapport à la fuite de données sensibles de l'entreprise en raison de sa négligence ou d'une mauvaise utilisation.
- La responsabilité de sauvegarder régulièrement les données de l'entreprise et de les stocker de façon appropriée

Protection par chiffrement

Beaucoup des mesures de sécurité de l'entreprise n'ont aucune emprise sur les données utilisées dans le cadre du BYOD, car ces données sortent de leur zone de contrôle. Les organisations doivent donc relever l'enjeu majeur du chiffrement des données sensibles au repos et en transit. Ce chiffrement a pour but de protéger la confidentialité des données numériques lors de leur stockage

sur des systèmes informatiques et lors de leur transmission sur Internet ou sur d'autres réseaux informatiques.
Les solutions de protection des données peuvent permettre de chiffrer les appareils, les e-mails et les données elles-mêmes. Dans de nombreux cas, ces fonctionnalités de chiffrement sont complétées par des outils de contrôle pour les appareils, les e-mails et les données.
Une messagerie sécurisée et chiffrée est la seule réponse conforme aux réglementations pour le personnel en télétravail, le BYOD et l'externalisation des projets.
Les solutions haut de gamme de prévention de la perte de données permettent aux employés de poursuivre leur travail et leurs échanges par e-mail pendant que le logiciel et les outils marquent, classent et chiffrent les données sensibles contenues dans les e-mails et pièces jointes de façon proactive.

Prévention de la perte de données (DLP)
Le télétravail et le travail mobile ont pratiquement rendu le périmètre réseau classique obsolète. Il n'est plus possible de construire un mur autour de l'informatique de votre organisation et de présumer que vos données sont en sécurité. Les organisations doivent reporter leur attention de la sécurisation du périmètre vers celle des données, où qu'elles se trouvent.
La DLP est en ensemble d'outils et de processus utilisés pour empêcher la perte de données, leur mauvaise utilisation ou l'accès à ces données par des utilisateurs non autorisés. Un logiciel de DLP classe les données critiques dans diverses catégories : métier, confidentielles et régulées, puis identifie les transgressions aux politiques définies par les organisations ou à un ensemble de politiques prédéfinies, généralement régi par la conformité à une réglementation, par exemple le RGPD.
Une fois ces transgressions repérées, la DLP applique une remédiation composée d'alertes, de chiffrement (comme indiqué ci-dessus), et d'autres actions protectrices pour empêcher les utilisateurs finaux de partager accidentellement ou par malveillance des données pouvant entraîner un risque pour l'organisation.
Les outils de DLP surveillent et contrôlent également les activités des terminaux, filtrent les flux de données sur les réseaux professionnels et surveillent les données dans le cloud pour protéger les données au repos, en mouvement, et en cours d'utilisation. Ces solutions mettent en évidence les tentatives de déplacement des données qui ne respectent pas les politiques de sécurité ou de confidentialité, et les bloquent. Cela peut empêcher des travailleurs mobiles d'obtenir des données jugées trop sensibles.

Apprentissage
Des sessions de formation régulières peuvent aider les employés à comprendre les risques et les conséquences potentielles de la perte d'un appareil mobile, et renforcer leur prudence. Ces sessions de formation doivent souligner l'importance de signaler rapidement la perte ou le vol des appareils.