Trois étapes pour mieux protéger les données en mobilité

	Trois étapes pour mieux protéger les données en mobilité

Pour mieux protéger les données en mobilités, la DSI doit connaître les spécificités de chaque système d'exploitation mobile, déterminer quels terminaux accepter dans l'environnement de travail, et comprendre les capacités natives de protection des données.

Protéger les données d'entreprise contre la perte et le vol est l'une des principales priorités. Les brèches de données sont douloureuses et onéreuses. Et leurs effets peuvent être étendus, entre atteinte à la marque et sanctions réglementaires.
Heureusement, l'industrie du mobile a progressé dans la prise en compte des préoccupations des entreprises en matière de sécurité, tout particulièrement pour ce qui est de la protection des données en mobilité. Par le passé, les smartphones manquaient de capacités même basiques de chiffrement des données. Mais ils ont depuis évolué en plateformes dotées de capacités de sandboxing avancées.
Parallèlement, les suites de gestion de la mobilité d'entreprise (EMM) ont amélioré le contrôle et la surveillance via le réseau, en OTA (over-the-air), ce qui donne aux DSI une pléthore d'outils de protections des données en mobilité, qu'elles transitent sur le réseau de l'entreprise ou via un point d'accès à Internet public.

Tout part du système d'exploitation mobile
La plupart des postes de travail des entreprises fonctionnent sous Windows, voire sous OS X. Cela offre aux DSI un environnement relativement cohérent et maîtrisé. Mais les terminaux mobiles exécutent des systèmes d'exploitation plus variés et évoluant plus rapidement, susceptibles d'ailleurs de changer d'un constructeur à l'autre, sinon d'un modèle à l'autre. Lorsque les utilisateurs amènent leurs propres appareils et applications mobiles, ils accroissent encore la diversité de l'environnement, et contournent les processus de la DSI. Dès lors, celle-ci ne peut pas compter sur la standardisation et le verrouillage des terminaux et de leurs applications pour sécuriser les données en mobilité.
Sécuriser les données en mobilité nécessite de comprendre ce que chaque système d'exploitation mobile peut ou ne peut pas faire. Les administrateurs peuvent alors pleinement tirer parti des technologies, applications et réglages supportés. Par exemple, la plupart des systèmes d'exploitation mobiles actuels supportent l'isolation native des applications – ou sandboxing –, et intègrent des capacités avancées de sécurisation du noyau.
Le support du chiffrement natif à l'échelle du terminal et de l'effacement à distance, varie toutefois. Pour cela, il est fréquent que les DSI choisissent une approche de sécurisation des données en mobilité en deux temps : elles commencent par établir et faire respecter des critères d'acceptation minimum, puis comblent les limitations des plateformes avec des outils tiers.

Déterminer quels terminaux accepter
Pour établir les critères d'acceptation des terminaux, il convient d'examiner l'architecture de sécurité de chaque plateforme pour étudier à quel point les applications utilisateur, opérateur et constructeur sont isolées les unes des autres, et du noyau du système d'exploitation.

Il convient également de savoir si les applications peuvent lire ou modifier les données d'autres applications et services en dehors du bac à sable – des fichiers partagés ou des messages, par exemple. L'examen doit également couvrir les permissions qui sont accordées – par défaut ou explicitement – aux applications, ainsi que le degré de contrôle que la DSI peut exercer pour détecter et bloquer des applications potentiellement dangereuses.
Comme leurs homologues pour le poste de travail, les systèmes d'exploitation mobiles souffrent de vulnérabilités susceptibles de mettre en danger les données. La question des mises à jour des applications et du système d'exploitation, leur délai de mise à disposition, s'avère particulièrement problématique dans un écosystème fragmenté.
La même considération s'applique à la provenance des applications mobiles. Le contrôle exercé par Apple s'avère efficace pour limiter la diffusion de logiciels malveillants pour iOS – sans toutefois l'empêcher complètement. C'est un facteur à prendre en compte dans l'établissement des critères d'acceptabilité. Par exemple, certaines entreprises interdisent les terminaux Android, ou n'en autorisent que certaines versions.
Pour beaucoup, les critères de base non négociables touchent à une version d'OS mobile minimum, le support matériel du chiffrement complet du terminal, des interfaces d'administration OTA, la possibilité d'imposer l'utilisation d'un mot de passe robuste, celle d'effacer le terminal à distance, d'enregistrer les activités, de détecter les opérations de jailbreak ou de rootage, voire de gérer dans une certaine mesure les applications installées. Les terminaux ne répondant pas à ces critères de base sont susceptibles d'être interdits d'accès aux réseaux et services de l'entreprise, ou bien autorisés dans une mesure limitée qui ne mette pas en danger les données.

Protection native des données : une base
Les smartphones et les tablettes sont appelés à être perdus, avec les données métiers qu'ils transportent. Le chiffrement complet du terminal peut souvent empêcher un appareil perdu d'être à l'origine d'une brèche de données.
Mais un tel chiffrement peut s'avérer d'une portée limitée sur certaines plateformes. Par exemple, l'effacement à distance est supporté par tous, mais son efficacité varie. Sur les appareils Apple et BlackBerry, les clés de chiffrement sont supprimées, ce qui rend les données chiffrées irrécupérables. Sur les anciens appareils Android sans chiffrement matériel, l'effacement n'est qu'une réinitialisation en conditions de sortie d'usine. Ce qui est susceptible de laisser les données exposées en cas de perte, de vol ou de revente du terminal.
De la même manière, un système de fichiers chiffré ne peut pas pleinement sécuriser les données sur un terminal compromis. Il ne peut pas non plus empêcher les utilisateurs de déplacer des données sur des emplacements non chiffrés. Lorsque des applications professionnelles et personnelles coexistent sur un même appareil, il y a plus de chances pour qu'une application malicieuse ou trop curieuse compromette des données d'entreprise présente sur le même système de fichiers. A moins que la DSI ne prenne des mesures préventives, un employé autorisé à accéder à un terminal chiffré peut aisément laisser fuir des données par e-mail ou transfert vers un service de stockage en mode Cloud.
La protection native des données en mobilité apparaît en fait comme un point de départ essentiel, mais pas suffisant. Pour profiter pleinement de ce que peuvent offrir les systèmes d'exploitation mobiles modernes, il convient d'utiliser une solution de gestion de la mobilité d'entreprise (EMM) pour enrôler les appareils acceptables et provisionner leurs réglages, en commençant par des points tels que la robustesse du mot de passe, le recours au lecteur d'empreintes digitales, ou encore le nombre de tentatives autorisées. Une authentification robuste est critique parce que des codes PIN faciles à deviner peuvent neutraliser un chiffrement fort. Il convient aussi d'activer l'effacement à distance et de recueillir le consentement explicite de l'utilisateur durant l'enrôlement à l'invocation de cette fonctionnalité en cas de dernier recours, et dans des conditions très précises.
Article original de Lisa Phife

Réagissez à cet article

Original de l’article mis en page : Trois étapes pour mieux protéger les données en mobilité