



Conseils en matière de sécurité pour la BlackBerry® PlayBook^{MC} de RIM

Introduction

Research in Motion (RIM) est le fabricant de la gamme de produits innovateurs BlackBerry® qui comprend le téléphone intelligent bien connu BlackBerry, les logiciels connexes et la nouvelle BlackBerry PlayBook.

La BlackBerry PlayBook est une tablette électronique qui prend en charge des fonctions de sécurité assurant des connexions chiffrées et authentifiées avec un téléphone intelligent BlackBerry¹. La version 1.0.7 du système d'exploitation (SE) de la PlayBook est validée en vertu du Programme de validation des modules cryptographiques (PVMC).

L'utilisation de la BlackBerry PlayBook de RIM n'est pas autorisée pour le traitement de l'information classifiée ou PROTÉGÉ C du gouvernement du Canada (GC). Après avoir mis en œuvre les mesures de sécurité recommandées ci-après, les ministères du GC qui connectent des Playbook aux réseaux du GC ou qui utilisent des PlayBook pour traiter de l'information PROTÉGÉ A ou PROTÉGÉ B assumeront des risques légèrement plus élevés que s'ils traitaient une telle information uniquement sur des téléphones intelligents BlackBerry.

Sécurité

Voici les considérations de sécurité associées aux PlayBook connectées aux réseaux du GC ou utilisées pour traiter de l'information du GC :

- Contrairement au téléphone intelligent BlackBerry, qui comporte de nombreuses règles de stratégie informatique d'entreprise, les seules règles qui s'appliquent à la version actuelle de la PlayBook sont les suivantes :
 - la règle *BlackBerry Bridge* qui est activée par défaut afin d'autoriser à une BlackBerry PlayBook de se connecter à un téléphone intelligent BlackBerry;

- la règle *BlackBerry PlayBook Log Submission* qui autorise une PlayBook à envoyer des fichiers journaux au BlackBerry Technical Solution Centre (centre de solutions techniques BlackBerry) de RIM.

À part les règles susmentionnées, la version actuelle de la PlayBook ne prend en charge aucune fonction additionnelle de gestion d'entreprise ni contrôle d'applications tierces.

- Les pratiques d'assurance de la sécurité de RIM pour les applications tierces disponibles à partir de la boutique BlackBerry App World comprennent la technologie du bac à sable² et visent à protéger la PlayBook et les données qui y sont stockées en limitant l'accès du système de fichiers d'une application au répertoire bac à sable de cette dernière. Or, étant donné que les applications sont autorisées à accéder à des données à l'extérieur de leur répertoire bac à sable, comme les fichiers stockés dans des répertoires partagés par exemple, il est possible que des applications tierces malveillantes exploitent cette fonction pour accéder au contenu de fichiers sensibles.
- La PlayBook peut se connecter à Internet de trois manières : 1) à l'aide de BlackBerry Bridge, 2) par connexion Wi-Fi et 3) au moyen de la fonction modem 3G sur une liaison Bluetooth. Les connexions à l'aide de BlackBerry Bridge font appel aux connexions de données Enterprise du téléphone BlackBerry, lesquelles devraient être protégées par les coupe-feux, contrôles et filtres de l'organisme. Les connexions Wi-Fi et 3G, par contre, ne sont pas assujetties aux règles de stratégie informatique, et l'accès à Internet par l'intermédiaire de ces connexions ne sera pas protégé par les mesures de protection de l'organisme.

¹ S'applique au téléphone intelligent BlackBerry tournant sous le SE BlackBerry Handheld, version 5 ou ultérieure, et à l'application BlackBerry Bridge, version 1.0.4.9.

² Le bac à sable est un mécanisme de protection dynamique pour les applications où l'accès aux fonctions ou aux données est contrôlé.

Mesures de sécurité recommandées

Pour remédier aux problèmes de sécurité mentionnés plus haut, la liste ci-après propose plusieurs mesures de sécurité et recommandations en matière de stratégie informatique visant l'utilisation de la PlayBook au GC.

- Il est recommandé que les ministères du GC assurent l'achat et l'activation des PlayBook au nom de chaque utilisateur.
- Comme pour tout appareil du GC, une PlayBook fournie par le GC ne devrait pas être connectée à un ordinateur non gouvernemental, comme l'ordinateur personnel de l'utilisateur par exemple, afin d'éviter la compromission de la configuration de l'appareil, des règles de stratégie informatique ou des paramètres sélectionnés pour protéger l'information du GC.
- Seuls les téléphones Enterprise BlackBerry connectés à un serveur d'entreprise BlackBerry (BES pour *BlackBerry Enterprise Server*) du GC devraient être jumelés à une PlayBook. Les dispositifs personnels ou non reliés à un BES ne doivent pas être jumelés à une PlayBook du GC.
- En l'absence de règles de stratégie informatique liées à la PlayBook, les administrateurs devraient appliquer une politique d'utilisation obligeant l'emploi d'un mot de passe robuste sur la PlayBook. Ce mot de passe devrait être différent de celui du téléphone intelligent BlackBerry. Par ailleurs, la politique sur l'utilisation devrait indiquer clairement comment utiliser les connexions Wi-Fi et la fonction modem 3G en fonction des objectifs de sécurité et de la politique sur l'utilisation d'Internet du ministère.
- Les administrateurs devraient désactiver le jumelage Bluetooth, l'option *Délectable (discoverability)* et tous les profils Bluetooth non nécessaires une fois que l'utilisateur a établi une connexion de jumelage entre sa tablette PlayBook et son téléphone intelligent BlackBerry. Les dispositifs jumelés pourront ainsi communiquer entre eux, mais interdiront les connexions avec d'autres dispositifs Bluetooth non fiabilisés.
- Les administrateurs devraient vérifier si les applications tierces ne représentent pas un risque de sécurité pour l'organisme avant de procéder à

leur installation. Une bonne stratégie informatique interne pour les administrateurs serait d'installer les applications tierces requises sur les PlayBook au moment du déploiement.

- Dans les cas où le ministère limite l'utilisation d'applications tierces sur les téléphones intelligents BlackBerry, les administrateurs devraient ajouter l'application BlackBerry Bridge de RIM à la liste des applications autorisées (liste blanche) afin de permettre aux utilisateurs de télécharger et d'installer cette application, mais devraient continuer d'interdire les autres applications tierces.
- Une solution client léger permet d'offrir un niveau de sécurité plus élevé lorsqu'on accède aux réseaux du GC et à la messagerie électronique du ministère à l'aide de la PlayBook. En pareil cas, il faudrait désactiver la fonctionnalité couper-coller pour limiter le risque d'exfiltration de l'information du GC.
- Les administrateurs peuvent opter de désactiver la fonctionnalité de la carte de mémoire microSD³ pour empêcher les applications tierces de la PlayBook d'accéder au contenu de cette carte. À noter toutefois que cela empêchera également aux utilisateurs de visualiser les pièces jointes de courriels sur la tablette.
- Étant donné que la sécurité de BlackBerry Bridge et les droits d'accès sont liés au téléphone intelligent BlackBerry jumelé à la tablette, les administrateurs devraient régler la valeur de la Temporisation de sécurité maximum⁴ (*Maximum Security Timeout*) sur les téléphones BlackBerry à une durée qui ne nuit pas à leur convivialité mais qui réduit l'exposition des données par l'intermédiaire de la PlayBook.

³ *microSD* est une marque de commerce de SanDisk pour le type de mémoire utilisée dans un téléphone intelligent BlackBerry.

⁴ Règle de stratégie informatique Temporisation de sécurité maximum (*Maximum Security Timeout IT Policy Rule*) – Cette règle sert à définir la période maximale d'inactivité d'un téléphone BlackBerry (ou par l'intermédiaire du BlackBerry Bridge dans le cas de la PlayBook) avant qu'il ne soit verrouillé automatiquement.