Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Juillet 2013

Gestion des risques associés aux iPad

Conseils à l'intention du gouvernement du Canada

ITSB-65

Introduction

La facilité d'utilisation de la tablette iPad, son court délai de démarrage et sa portabilité en font un dispositif bien plus convivial qu'un portable traditionnel. Pour les employés, le iPad est un excellent appareil compagnon, qu'ils utilisent en remplacement du papier pour prendre des notes au cours des réunions et pour lire des documents pendant leurs déplacements. Les iPad présentent toutefois de nouveaux risques pour les activités d'une organisation et pour la sécurité de ses données.

Les risques pour la sécurité sont nombreux, et il faut les évaluer avec soin, s'assurer de bien les comprendre et mettre en place des contrôles de sécurité et des mesures de protection avant d'autoriser tout accès par des iPad à un réseau ministériel. Le présent bulletin développe les thèmes abordés dans le document CSG-30 : *Caractéristiques de sécurité et pratiques exemplaires pour l'iPad d'Apple*, et prend en considération certaines des fonctionnalités les plus récemment incorporées dans les dernières versions du système d'exploitation de la tablette.

Répercussions sur la sécurité

Les systèmes d'exploitation des dispositifs mobiles sont beaucoup moins évolués que ceux des postes de travail et portables traditionnels. Par conséquent, la robustesse et la granularité de contrôle propres au système d'exploitation de l'iPad ne permettent pas d'obtenir un niveau d'assurance équivalent.

La nature des contrôles de sécurité à mettre en place pour le déploiement des iPad doit être déterminée en fonction du profil de menaces et de risques du ministère. Le guide ITSG-33, La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie, décrit un processus de gestion des risques de sécurité en vertu duquel on peut adapter une série prédéfinie de contrôles de sécurité de base de manière à répondre aux besoins spécifiques d'un ministère en matière de sécurité. Les contrôles de sécurité doivent être déployés et vérifiés pour l'ensemble du système d'information, et ce, du dispositif iPad individuel jusqu'aux services de réseau du ministère qui gèrent les processus opérationnels et les biens d'information.

Le présent bulletin décrit les cinq principales vulnérabilités associées aux iPad, de même que les stratégies d'atténuation et les mesures de protection potentielles. Il importe de souligner que cette liste n'est pas exhaustive, et que même dans une situation où toutes les stratégies d'atténuation potentielles ont été correctement mises en place, il existera toujours un risque résiduel pour le réseau et les biens d'information du ministère. Par conséquent, il n'est pas recommandé d'utiliser des iPad pour le traitement de données classifiées au niveau « SECRET » ou à un niveau supérieur.

Les 5 principales vulnérabilités de l'iPad et les stratégies d'atténuation potentielles

N° 1 – Données inactives

Risques : La fonctionnalité de chiffrement matériel offerte par Apple ne protège pas les données inactives; elle vise principalement à faciliter l'effacement à distance des données si le dispositif est perdu ou égaré. La fonctionnalité de protection renforcée des données (EDP pour *Enhanced Data Protection*) est la solution mise en œuvre par Apple pour la protection des données inactives. Chaque application doit toutefois activer indépendamment l'EDP, sinon ses données seront stockées en clair.

L'application de courrier d'Apple est la seule application fournie nativement avec le dispositif qui utilise l'EDP. Néanmoins, toute activité d'exportation (p. ex. un document sous forme de pièce jointe envoyé à une application de lecture de documents) peut laisser les données sans protection si l'application secondaire n'utilise pas elle aussi l'EDP.

Stratégies d'atténuation : Il est recommandé que les ministères déterminent quelles applications tirent parti de la fonctionnalité d'EDP et utilisent uniquement ces applications pour traiter les données du Gouvernement du Canada (GC). La version iOS 5 du système d'exploitation a ajouté la capacité pour les organisations de renouveler la

signature numérique d'une application et d'activer l'EDP. Pour assurer l'efficacité de cette méthode, chaque ministère doit toutefois installer et maintenir un environnement de vitrine interne (Enterprise Storefront).

En plus de la fonctionnalité d'EDP, de nombreuses solutions de gestion de dispositifs mobiles (MDM pour *Mobile Device Management*) font appel à des agents logiciels pour créer un « contenant sécurisé » sur l'iPad : un entrepôt chiffré de données ministérielles qui demeure distinct de tout système de chiffrement fourni par Apple.

La meilleure solution consiste néanmoins à ne stocker aucune donnée du GC sur l'iPad. Il existe différentes solutions de client léger et de bureau à distance qui permettent aux utilisateurs de consulter et de manipuler des données stockées sur un serveur du GC sans avoir à télécharger les données sur un iPad.

Risques résiduels : Les fonctions d'effacement à distance des données ne sont activées que si le dispositif est sous tension et connecté au réseau. Tout délai dans le signalement de la perte d'un dispositif mobile par un utilisateur peut compromettre la capacité d'exécuter un effacement à distance et exposer les données stockées sur ce dispositif. Certaines applications tierces utilisées pour traiter des données du GC peuvent comporter des risques de fuite de données qui ne peuvent pas être atténués par la fonctionnalité d'EDP.

N° 2 – Maliciels

Risques : La principale voie d'introduction de logiciels malveillants sur un iPad dérive du téléchargement d'applications tierces. Bien qu'Apple affirme avoir mis en place un processus d'approbation pour les applications vendues par l'entremise d'iTunes, le processus ne valide en fait que les fonctionnalités proposées et l'absence de contenus inacceptables. Apple n'exécute aucun examen ni analyse du code; par conséquent, ses processus de validation n'offrent aucune protection contre une intention malveillante.

Une voie d'introduction secondaire est le navigateur Safari conçu à partir du moteur WebKit, qui a été par le passé la cible de cyberattaques, et qui s'est révélé être une voie d'accès privilégiée pour l'introduction de logiciels malveillants sur la plateforme iOS.

Stratégies d'atténuation : Apple surveille continuellement l'environnement des maliciels et met à jour régulièrement son système d'exploitation et les applications intégrées afin d'atténuer les risques d'exploitation par maliciels. Il est recommandé que les ministères établissent un programme permettant de s'assurer que les versions les plus récentes des logiciels sont installées sur tous les dispositifs Apple.

Le Centre de la sécurité des télécommunications Canada (CSTC) recommande de plus d'interdire tout téléchargement d'applications tierces non explicitement autorisées. Les applications jugées nécessaires doivent être achetées auprès de fournisseurs bien connus et établis, et doivent être évaluées par le ministère à la recherche de signes d'intention malveillante et de possibilités de fuite de données avant leur distribution sur la vitrine interne du ministère.

Certaines solutions MDM peuvent offrir des fonctionnalités qui permettent non seulement à une organisation de spécifier à quelles applications un utilisateur peut accéder, mais aussi de déployer à distance une application ou une mise à jour logicielle. Certaines solutions peuvent également offrir des fonctionnalités de détection et de suppression d'applications non autorisées.

Il est possible de désactiver le navigateur Safari si aucun accès à Internet n'est requis. Une autre solution consiste à installer un navigateur fondé sur un agent MDM, qui transmettra les données par le biais de l'infrastructure et des coupe-feu du ministère. S'il faut absolument utiliser Safari, il convient d'activer les fonctionnalités intégrées de détection des sites frauduleux et de blocage des fenêtres de publicité.

Risques résiduels : Les mesures de sécurité mises en œuvre dans chaque application se limitent à cette application seulement. L'efficacité de telles mesures n'a pas été démontrée, et la plupart peuvent être aisément contournées de la même façon que le sont les restrictions par signature du code au niveau du système d'exploitation dans un dispositif qui a été « débridé ».

L'efficacité d'une solution MDM pour ce qui est de la gestion des applications dépend des capacités du magasin d'applications, de la plateforme mobile et des agents logiciels en matière de mise en œuvre de fonctionnalités de contrôle, de détection et de suppression d'applications. Une application malveillante qui

est consciente de son environnement pourrait être en mesure de contourner de telles mesures et d'accéder aux données stockées sur le dispositif.

N° 3 – Débridage

Risques : L'expression « débridage » désigne le processus visant à désactiver les fonctionnalités de vérification de signature du code intégrées au système d'exploitation d'Apple; une telle action brise la « chaîne de confiance » fondamentale qui est établie lorsqu'Apple signe une application. Un dispositif débridé peut exécuter une application non autorisée en mode d'élévation de privilège, ce qui peut lui donner accès aux données non sécurisées stockées sur le dispositif.

En règle générale, le débridage nécessite un accès physique à un dispositif mobile (scénario de perte ou de vol), mais il a été démontré à plusieurs occasions qu'on peut l'exécuter à distance en exploitant des failles dans des navigateurs Web et des lecteurs de documents.

Stratégies d'atténuation : Certaines solutions MDM affirment être en mesure de détecter les dispositifs débridés et d'atténuer les risques connexes grâce à un agent logiciel tournant sur le dispositif. Il est recommandé d'utiliser des contenants et enveloppeurs sécurisés créés par un agent MDM, qui exigent l'authentification de l'utilisateur pour accéder au contenu stocké sur le dispositif ou sur le réseau (l'authentification multifactorielle est également recommandée pour les données de nature particulièrement délicate), de manière à limiter toute possibilité d'accès direct en cas de débridage non détecté.

Risques résiduels : Les agents MDM ne détecteront pas nécessairement tous les types et toutes les situations de débridage et d'élévation de privilège. Tout processus exécuté en mode d'élévation de privilège peut être capable de contourner la plupart des mesures et contrôles de sécurité installés, même après la prise de mesures de sécurité robustes (sous la forme d'agents MDM et d'enveloppeurs sécurisés), et ainsi d'exposer les données stockées sur le dispositif.

N° 4 – Accès par le biais du réseau sans fil

Risques : Le système d'exploitation iOS d'Apple ne permet pas à une organisation de désactiver l'accès aux réseaux sans fil, ni de restreindre la liste des réseaux auxquels un utilisateur peut se connecter (c.-à-d. un utilisateur peut créer des profils pour se connecter à un réseau sans fil domestique ou public).

Stratégies d'atténuation : Il était possible d'ouvrir les modèles d'iPad plus anciens pour retirer de façon permanente la capacité sans fil du dispositif. Cette solution est toutefois difficile à mettre en œuvre avec les générations plus récentes de l'iPad. On peut empêcher les connexions à un réseau 3G/4G en collant le logement de la carte SIM (nécessaire pour accéder à un réseau) afin d'empêcher son insertion.

Pour contrôler les accès à un réseau sans fil, un ministère peut utiliser la fonctionnalité « RPV sur demande » et dresser la liste de tous les domaines de premier niveau (.com, .org, .net, .ca, .us, .gov, etc.) en tant que domaines correspondants et diriger la connexion vers une passerelle RPV contrôlée par le GC qui ne permet aucun accès réel au réseau.

Enfin, on peut mettre en place une politique écrite et des ententes d'utilisation afin que les utilisateurs désactivent manuellement les fonctions de connexion sans fil.

Risques résiduels : Il n'existe aucune solution efficace permettant d'atténuer les risques associés aux connexions Bluetooth. Même avec la fonctionnalité de RPV sur demande, les applications intégrées d'Apple conservent la capacité de se connecter à l'infrastructure d'Apple, en contournant le RPV (tunnels fractionnés), chaque fois qu'une connexion est établie avec un réseau sans fil. Cette situation pourrait ainsi permettre une connexion non autorisée au réseau ministériel.

N° 5 – Configuration et gestion

Risques : L'activation d'un dispositif iOS nécessite l'installation du logiciel iTunes et la création d'un compte d'utilisateur. Ces dispositifs ont été développés pour le marché de la consommation et ne sont pas bien adaptés à un déploiement au sein d'une grande entreprise ou d'un organisme gouvernemental. Il est difficile de maintenir une configuration opérationnelle réellement hors ligne en raison de la nécessité de maintenir une connexion à Internet. Le profil de l'utilisateur et l'information sur le dispositif, les données

d'application, les bibliothèques iTunes et les données sauvegardées de l'utilisateur sont tous des cibles potentielles qui peuvent être exposées si les mesures de contrôle appropriées ne sont pas mises en place.

Les produits de configuration et de gestion présentent des capacités extrêmement diverses qui sont par ailleurs toujours limitées par les fonctionnalités intégrées à iOS.

Stratégies d'atténuation : Les services de configuration et de gestion doivent uniquement être exécutés au moyen de systèmes capables de fournir le niveau approprié d'assurance de sécurité pour ce qui est de l'accès, du stockage et du traitement de l'information nécessaire. Ces services ne doivent pas nécessiter une connexion directe à Internet (ils doivent pouvoir être exécutés dans la zone d'accès restreint).

De plus, les profils d'utilisateur, l'information sur le dispositif, les données d'application et les bibliothèques iTunes qui sont jugés non essentiels doivent être supprimés, et les renseignements essentiels et les données sauvegardées sur le dispositif doivent être protégés au moyen de mesures de protection et de chiffrement suffisantes. L'utilitaire Apple Configurator et les solutions MDM permettent de mettre en œuvre jusqu'à un certain degré des capacités opérationnelles de configuration et de gestion.

Risques résiduels : Toute fonctionnalité de sécurité offerte par une solution MDM dépend de l'API iOS fournie par Apple, ce qui pourrait permettre l'établissement de connexions non autorisées à Internet.

Sommaire

Il est nécessaire d'élaborer une architecture sécurisée pour l'accès à distance des dispositifs mobiles et de la déployer au moyen d'une approche fondée sur la gestion du risque (ITSG-33). Une évaluation des menaces et des risques (EMR) doit être effectuée afin de déterminer le niveau d'assurance approprié en matière d'information.

Renseignements supplémentaires

Pour obtenir des conseils et de l'orientation en matière de sécurité des dispositifs mobiles, prière de communiquer avec les Services à la clientèle de la Sécurité des TI : itsclientservices@cse-cst.gc.ca.

Références

ITSB-64 : Solutions de gestion de dispositifs mobiles (MDM)

CSG-30 : Caractéristiques de sécurité et pratiques exemplaires pour l'iPad d'Apple

ITSG-33 : La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie