Considérations de sécurité associées au déploiement d'appareils mobiles

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Octobre 2024 | ITSAP.70.002

Au moment de déterminer une approche pour déployer les appareils mobiles dans votre organisation, vous pouvez choisir parmi différents modèles de déploiement ayant chacun leurs avantages et leurs risques. La gestion des risques liés aux appareils mobiles repose en partie sur la collaboration du personnel et sur sa volonté d'accepter les restrictions d'utilisation, la surveillance et l'accès par l'organisation aux fins de sécurité. Elle dépend également des vulnérabilités propres à chaque type d'appareils. Afin de choisir un modèle de déploiement qui offre le meilleur équilibre entre ces éléments pour votre organisation, considérez l'expérience utilisateur, la confidentialité et les exigences de sécurité.

Modèles de déploiement d'appareils mobiles

Le présent document décrit les modèles de déploiement d'appareils mobiles suivants ainsi que les avantages et les risques propres à chacun :

- appareils réservés au travail et appartenant à l'organisation (COBO pour *Corporately owned, business only);*
- appareils pouvant servir à des fins personnelles et appartenant à l'organisation (COPE pour *Corporately owned, personally enabled*);
- appareils personnels (BYOD pour *Bring your own device*).

Appareils réservés au travail et appartenant à l'organisation (COBO)

Dans le modèle COBO, votre organisation est la propriétaire des appareils que les membres du personnel utilisent uniquement à des fins professionnelles. Ce modèle permet un flux opérationnel efficace réservé au travail et assure la sécurité du travail à distance ainsi que la gestion, le soutien et la maintenance normalisés des appareils, y compris les mises à jour. Il permet également à votre organisation d'avoir le plein contrôle des stratégies de sécurité, ce qui comprend la complexité des mots de passe, le chiffrement des données, les restrictions d'accès et la gestion des vulnérabilités.

Les avantages du modèle COBO comprennent :

- un risque accru découlant de configurations trop restrictives sur les appareils COBO si les membres du personnel trouvent que les appareils fournis par l'organisation limitent leur capacité de travailler efficacement et décident alors d'utiliser leurs appareils personnels;
- la capacité de contrôler les mises à jour des appareils;
- l'option de travailler à distance;
- aucun risque lié au téléchargement d'applications malveillantes puisque votre organisation peut limiter les applications à seulement celles qui ont été évaluées comme étant sûres et offrant une valeur opérationnelle.

Les risques associés au modèle COBO comprennent :

- overly restrictive configurations for COBO may increase risk if employees feel that corporately issued devices restrict their ability to work efficiently and opt to use personal devices
- une flexibilité réduite pour les membres du personnel, puisqu'elles et ils peuvent seulement utiliser une sélection limitée d'applications;
- des vulnérabilités issues de l'assouplissement de restrictions pour autoriser les connexions Bluetooth, à des réseaux Wi-Fi publics ou non sécurisés, à des appareils USB ou à d'autres supports de stockage amovibles;
- des vulnérabilités dues à la tunnellisation partagée de réseaux privés virtuels (RPV), où certain trafic d'application ou d'appareil est acheminé par un RPV chiffré, tandis que d'autre trafic a un accès direct à Internet.

Cat. No. D97-1/70-002-2024F-PDF ISBN 978-0-660-73535-1

Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Appareils pouvant servir à des fins personnelles et appartenant à l'organisation (COPE)

Dans le modèle COPE, votre organisation est propriétaire des appareils, en assure le contrôle et la surveillance, et peut appliquer des stratégies de sécurité plus strictes. Ce modèle hybride offre certains avantages du modèle COBO et d'autres du modèle BYOD. Les membres du personnel peuvent utiliser les appareils à des fins personnelles, mais votre organisation contrôle les mesures de sécurité mises en œuvre. Si vous permettez aux employées et employés de choisir leur propre appareil, le coût pourrait s'avérer plus élevé. Vous devrez évaluer et obtenir de multiples appareils, élaborer plusieurs procédures de soutien et composer avec les niveaux variés de contrôles de sécurité fournis par différents fabricants.

Les avantages du modèle COPE comprennent :

- une plus grande satisfaction au travail et chez les employées et employés;
- un travail plus efficace et flexible;
- la capacité de contrôler les mises à jour des appareils;
- l'option de travailler à distance.

Les risques associés au modèle COPE comprennent :

- l'utilisation d'applications et de réseaux non fiables;
- de mauvaises pratiques exemplaires en cybersécurité de la part des utilisatrices et utilisateurs et des pratiques risquées sur Internet;
- aucun filtrage des courriels et des navigateurs Internet;
- le trafiquage intentionnel des contrôles de sécurité;
- aucun contrôle d'audit et de surveillance;
- des téléchargements d'applications malveillantes, permettant aux pirates informatiques d'accéder aux données organisationnelles;
- la perte de données, puisque le stockage de données personnelles et opérationnelles sur le même appareil peut entraîner des fuites de données;
- le relâchement de contrôles de sécurité stricts en faveur de l'utilisabilité ou d'autres exigences opérationnelles ou directoriales.

Appareils personnels (Bring your own device)

Le modèle BYOD permet aux employées et employés d'utiliser leurs propres appareils à des fins professionnelles. Vous pouvez également choisir de subventionner certains des frais connexes. Toutefois, puisque ces appareils n'appartiennent pas à votre organisation, vous avez peu de contrôle sur les mesures de sécurité mises en place sur les appareils. Les risques liés à ce modèle sont les mêmes que ceux associés au modèle COPE, mais avec un nombre inférieur de contrôles de sécurité disponibles.

Les avantages du modèle BYOD comprennent :

- une plus grande satisfaction au travail et chez les employées et employés;
- un travail plus efficace et flexible;
- l'option de travailler à distance;
- une utilisation personnelle et professionnelle;
- la réduction des dépenses liées au matériel.

Les risques associés au modèle BYOD comprennent :

- la capacité extrêmement limitée de l'organisation d'atténuer les compromissions puisque les appareils ne lui appartiennent pas;
- des téléchargements d'applications malveillantes, permettant aux pirates informatiques d'accéder aux données organisationnelles;
- une utilisation non sécurisée des appareils, puisque les utilisatrices et utilisateurs peuvent accéder à de l'information sur un Wi-Fi public ou permettre à d'autres personnes d'utiliser leur appareil;
- une perte de contrôle sur la gestion des mises à jour logicielles et des téléchargements;
- le trafiquage des fonctions de sécurité et le déverrouillage des restrictions de configuration;
- la perte de données, puisque le stockage de données personnelles et opérationnelles sur le même appareil peut entraîner des fuites de données.

Il convient de noter que les avantages et les risques peuvent varier selon les besoins et les exigences en matière de sécurité de votre organisation ainsi que selon vos utilisatrices et utilisateurs. Au moment de choisir un modèle de déploiement, vous devriez également envisager le modèle qui permettra à votre organisation d'établir un équilibre entre la fonctionnalité, l'expérience utilisateur et la sécurité.

Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mesures d'atténuation des risques liés au déploiement d'appareils mobiles

Il existe des façons de réduire les risques que représentent les appareils mobiles pour votre organisation. Les modèles COBO et COPE permettent les mesures d'atténuation suivantes :

- exiger l'utilisation de mots de passe et de mécanismes d'authentification robustes sur les appareils;
- mettre en place des contrôles de sécurité;
- limiter l'information transmise entre les appareils;
- offrir un soutien TI pour les appareils;
- utiliser des logiciels conçus ou achetés expressément et vérifiés par l'organisation;
- accéder aux applications de travail en utilisant l'infrastructure réseau de l'organisation;
- gérer les appareils et les données au départ d'une employée ou d'un employé.

La seule mesure d'atténuation concrète que fournit le modèle BYOD est la capacité d'utiliser le réseau organisationnel. La plupart des risques associés au modèle BYOD sont hors du contrôle de l'organisation puisque les appareils appartiennent aux membres du personnel.

Considérations pour le déploiement d'appareils mobiles

Votre organisation devrait choisir le modèle de déploiement qui correspond le mieux à ses besoins opérationnels en considérant les éléments suivants :

- le niveau de contrôle nécessaire selon la sensibilité de votre information;
- le budget disponible pour chacun des modèles de déploiement, y compris l'approvisionnement en matériel et le soutien TI;
- le meilleur équilibre entre les besoins opérationnels et la satisfaction au travail.

Gestion unifiée des terminaux

La gestion unifiée des terminaux (UEM pour Unified Endpoint Management) est une stratégie de distribution, de gestion et de contrôle des terminaux, à savoir les appareils mobiles et les ordinateurs de bureau, dans le lieu de travail. Elle combine des caractéristiques provenant des processus de gestion des appareils mobiles et de la mobilité d'entreprise afin de répondre aux préoccupations de sécurité liées à la gestion des données organisationnelles tout en augmentant la connectivité et la productivité. L'UEM inclut des fonctions qui aident à assurer la sécurité de l'information organisationnelle et des données des membres du personnel. Ces fonctions comprennent notamment :

- la surveillance uniforme des appareils, au bureau ou à distance;
- la séparation des plateformes d'application, que l'on appelle la mise en bac à sable;
- l'application de justificatifs d'identité d'authentification robustes;
- l'intégration de services de messagerie;
- la préparation des appareils pour la configuration et l'inscription;
- le chiffrement des données inactives et en transit;
- l'exécution à distance de la surveillance, du verrouillage et de l'effacement;
- la détection lorsque des utilisatrices ou utilisateurs retirent des autorisations de sécurité;
- la mise à jour automatique des correctifs de sécurité et des antimaliciels;
- la mise en place de listes d'applications autorisées et interdites.

Votre organisation peut utiliser la gestion unifiée des terminaux pour assurer la sécurité des appareils mobiles. Vous pouvez l'employer avec le modèle BYOD, mais votre capacité à gérer les appareils est minimale puisque ceux-ci appartiennent aux employées et employés. Dans un modèle COPE ou COBO, vous pouvez mettre en œuvre l'UEM plus efficacement puisque vous avez le contrôle complet sur la surveillance et la sécurité des appareils.

Enfin, choisissez les contrôles de sécurité soigneusement lorsque vous adoptez l'UEM. Il est important de comprendre chaque réglage et ses implications en matière de sécurité et d'utilisabilité. Bien qu'il soit tentant de le faire, l'activation de toutes les restrictions offertes peut amoindrir l'expérience utilisateur et l'utilisabilité d'un appareil. Ces restrictions peuvent également motiver les utilisatrices et utilisateurs à contourner intentionnellement les contrôles de sécurité ou à choisir d'utiliser des appareils personnels moins limitatifs, même s'ils savent que ces choix sont moins sécurisés et enfreignent les politiques organisationnelles.

Pour en savoir plus

- Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP) (ITSM.70.003)
- Application des mises à jour sur les dispositifs (ITSAP.10.096)
- Dispositifs mobiles et voyages d'affaires (ITSAP.00.087)
- Conseils sur les appareils mobiles à l'intention des voyageurs connus du public (ITSAP.00.088)
- La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux (ITSAP.00.007)
- Conseils de sécurité pour les organisations dont les employées et employés travaillent à distance (ITSAP.10.016)

Canada