Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP)

SÉRIE GESTIONNAIRES

TLP:WHITE

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

Canada

Avant-propos

La présente publication intitulée *Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez vos appareils personnels (PAP) (ITSM.70.003)* est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

Pour obtenir de plus amples renseignements, communiquez par téléphone ou par courriel avec le Centre d'appel :

cyber.gc.ca
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le XX mois 202X.

Historique des révisions

Révision	Modifications	Date
1	Première diffusion.	XX mois 20XX

Vue d'ensemble

Le présent document présente les zones d'attaque potentiellement vulnérables associées aux appareils des utilisateurs finaux qui sont utilisés dans le cadre des modèles de déploiement Prenez vos appareils personnels (PAP) dans les organisations de toutes tailles. Il fournit également des techniques d'atténuation que votre organisation peut appliquer pour réduire les risques liés à la mise en œuvre d'un modèle PAP.

Les appareils mal configurés des utilisateurs finaux peuvent exposer votre organisation à des risques. Ils représentent des points d'entrée par lesquels les auteurs de menace peuvent obtenir un accès non autorisé à des données sensibles.
Les utilisateurs finaux ne possèdent peut-être pas l'expertise technique pour éviter les incidents de sécurité, et ils se fient aux stratégies et aux contrôles techniques propres aux appareils pour assurer leur sécurité et celle de leurs données.

Si votre organisation choisit d'adopter un modèle de déploiement PAP, vous devez être conscient du fait que les utilisateurs finaux peuvent exposer votre environnement à des risques supplémentaires sans le savoir. Il faut savoir que de nombreux contrôles définis dans les stratégies organisationnelles imposent des limitations permissives plutôt que des limitations strictes en raison des aspects juridiques liés à la propriété. Par ailleurs, les contrôles techniques sont limités sur les appareils en raison de la conception des systèmes qui les soutiennent.

ISBN 978-0-660-43393-6

CAT D97-4/70-003-2022F-PDF

Table des matières

1 Introduction

Le présent document présente les zones d'attaque potentiellement vulnérables associées aux appareils des utilisateurs finaux qui sont utilisés dans le cadre des modèles de déploiement Prenez vos appareils personnels (PAP) dans les organisations de toutes tailles. Il fournit également des techniques d'atténuation que votre organisation peut appliquer pour réduire les risques liés à la mise en œuvre d'un modèle PAP.

On entend par « PAP » la pratique qui consiste à autoriser les employés à utiliser leurs appareils personnels (p. ex., les téléphones, les ordinateurs portables et les tablettes) pour accéder aux données et aux systèmes d'entreprise à des fins opérationnelles. Le niveau de restriction des modèles de déploiement PAP varie. Certains modèles accordent aux utilisateurs un accès illimité aux systèmes et aux données, tandis que d'autres accordent uniquement l'accès aux systèmes et aux données non sensibles, ou encore un accès moyennant certaines conditions (comme le contrôle TI sur les appareils personnels et l'impossibilité de stocker des données localement sur les appareils personnels).

Au moment de décider si vous devriez déployer un modèle PAP dans votre organisation, vous devriez examiner les avantages et les risques connexes afin de déterminer si le modèle respecte le seuil de tolérance au risque de votre organisation.

1.1 Un modèle PAP convient-il à votre organisation?

Le Centre pour la cybersécurité recommande de considérer les exigences opérationnelles et de sécurité au moment de choisir un modèle de déploiement lié aux appareils mobiles. Dans la mesure du possible, nous conseillons de remettre aux employés des appareils appartenant à l'organisation puisque vous pouvez ainsi contrôler plus étroitement les configurations et les contrôles de sécurité appliqués sur les appareils. Si vous optez pour un modèle PAP, vous devez tenir compte des facteurs juridiques, technologiques et budgétaires de même que des facteurs de sécurité qui peuvent avoir une incidence sur la faisabilité du modèle. Pour obtenir plus d'information concernant les répercussions sur le respect de la vie privée associées à la gestion d'appareils PAP dans un environnement organisationnel, veuillez consulter la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) [1] et la *Loi sur la protection des renseignements personnels* [2].

Pour une vue d'ensemble des différents modèles de déploiement des appareils mobiles, veuillez consulter l'ITSAP.70.002, *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles* [3][1]. Pour en savoir plus sur les mesures de base que vous pouvez prendre pour protéger vos réseaux et votre information, lisez l'ITSM.10.089, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [4] et la version 1.2 du document *Contrôles de cybersécurité de base pour les petites et moyennes organisations* [5].

1.2 Zone d'attaque des appareils des utilisateurs finaux

Les modèles PAP font peser des risques sur les organisations dans lesquelles ils sont déployés. Certains risques sont liés aux données organisationnelles, d'autres aux implications sur le plan du respect de la vie privée. Voici une liste des risques les plus courants relatifs à l'adoption d'un modèle PAP :

[1] Les numéros entre crochets renvoient à des ressources figurant à la section Contenu complémentaire du présent document.

- **Applications non autorisées :** Les applications non autorisées qui sont installées sur les appareils peuvent soulever des préoccupations liées à la sécurité puisqu'elles menacent l'intégrité, la disponibilité et la confidentialité de l'information et des systèmes des organisations. Les auteurs de menace peuvent se servir des applications à des fins malveillantes et accéder à l'emplacement de l'appareil, aux paramètres réseau, de même qu'aux fichiers, aux applications et aux données stockés sur l'appareil. Les maliciels de minage peuvent aussi être très dommageables pour la disponibilité et l'intégrité des données.
- **Fuites de données :** Les appareils PAP sont susceptibles d'ouvrir la porte au partage ou à des fuites de données confidentielles ou sensibles d'une façon qui serait impossible si les employés utilisaient des appareils organisationnels. Des applications et comptes de médias sociaux sont souvent installés et configurés sur les appareils personnels et permettent aux utilisateurs de partager aisément du texte, des photos, ainsi que du contenu audio et vidéo à un vaste auditoire public. Les appareils personnels ne sont pas aussi sécurisés que les appareils organisationnels. Ils permettent aux utilisateurs d'accéder à divers sites Web et applications auxquels ils n'auraient probablement pas accès sur des appareils organisationnels. Ces applications et sites Web peuvent exposer votre organisation à des risques supplémentaires, comme fournir à des auteurs de menace des vecteurs additionnels pour exploiter et infiltrer vos systèmes et réseaux organisationnels. Les auteurs de menace ciblent les appareils PAP puisque ceux-ci contiennent un grand volume de données et fournissent un point d'entrée dans les systèmes et réseaux organisationnels connectés. De plus, les appareils PAP peuvent être davantage prédisposés aux atteintes à la vie privée que les appareils organisationnels qui ne contiennent pas de renseignements personnels, ce qui pourrait permettre à des auteurs de menace de s'emparer de vos données pour les vendre ou demander une rançon en échange.

  Les utilisateurs risquent aussi de se connecter plus fréquemment à des réseaux Wi-Fi non sécurisés au moyen de leurs appareils personnels. Après s'être connectés à un tel réseau, les appareils s'y reconnecteront souvent automatiquement par la suite. Il se peut également que les utilisateurs téléchargent et stockent de grands volumes de données hors ligne pour éviter d'attendre ou de dépasser leur allocation de bande passante. Puisqu'il est impossible d'appliquer autant de contrôles de sécurité aux appareils PAP qu'à votre infrastructure organisationnelle, le risque de fuites de données est nettement supérieur.
- **Préoccupations liées à la vie privée :** Comme il est possible d'acquérir une connaissance approfondie de l'environnement utilisateur sur l'appareil par l'entremise de la plupart des logiciels de gestion des appareils mobiles (MDM pour *Mobile Device Management*) et de gestion unifiée des terminaux (UEM pour *Unified Endpoint Management*), il est possible de visualiser des détails personnels (comme l'adresse de courrier électronique, des renseignements personnels conservés dans des applications et des fichiers, l'emplacement et d'autres aspects de l'identité de l'utilisateur) de façon accidentelle ou malveillante. Il se peut également que les employés hésitent à fournir une visibilité dans leurs appareils, et cette capacité limitée de votre organisation de surveiller ou de détecter les menaces élargit la zone d'attaque.
- **Partage des appareils :** Il est possible que des amis ou des membres de la famille partagent les appareils personnels, ce qui peut entraîner des fuites accidentelles d'information et compromettre l'intégrité des données stockées sur ces appareils.

- **Débridage d'appareil :** Les appareils personnels sont parfois débridés, ce qui signifie que certaines autorisations standards de sécurité ont été retirées et donnent ainsi aux utilisateurs et aux applications un plus grand accès au système d'exploitation. Ces appareils risquent davantage de contourner les contrôles de sécurité mis en œuvre par votre organisation et d'exposer vos données, vos réseaux et vos applications à des risques accrus. Pour atténuer les risques, vous devriez interdire les appareils qui ont été modifiés au-delà de l'utilisation et des autorisations prévues. Par ailleurs, il est important de définir les données organisationnelles qui sont permises sur les appareils PAP à l'aide de stratégies et de formations. Celles-ci présentent des conseils aux employés sur l'utilisation appropriée (p. ex., les activités personnelles autorisées), la protection des données et les mesures de sécurité s'appliquant à leurs appareils.
- **Impossibilité d'appliquer des correctifs et des mises à jour :** Si votre organisation adopte un modèle PAP, il est possible que votre capacité de fournir et d'appliquer les mises à jour aux systèmes d'exploitation, aux applications et aux environnements de bureau soit limitée. Pour veiller à ce que les nouvelles mises à jour de sécurité soient installées de façon opportune, votre organisation peut choisir de permettre uniquement l'utilisation d'appareils PAP autorisés qui répondent aux exigences organisationnelles en matière de conformité (ils doivent être corrigés et pris en charge par le fabricant).

2 Pratiques exemplaires

La section suivante décrit les pratiques exemplaires en matière de sécurité que votre organisation peut instaurer afin de réduire les risques associés aux appareils personnels. Dans un modèle PAP, vous pouvez suivre des lignes directrices générales pour sécuriser les appareils des utilisateurs finaux, notamment :

- la mise en œuvre de stratégies;
- la création de procédures d'intégration et d'annulation de l'intégration;
- le traitement sécurisé des données;
- l'application de contrôles de sécurité techniques;
- la formation de tous les employés, y compris les cadres, les entrepreneurs, les bénévoles et les étudiants.

Votre organisation devrait harmoniser ses stratégies et contrôles de sécurité avec ses exigences en matière d'opérations, de sécurité et de respect de la vie privée. Vous devriez appliquer plusieurs couches de mesures de sécurité (approche de défense en profondeur) pour protéger la confidentialité, l'intégrité et la disponibilité des réseaux, des systèmes et des données organisationnels.

Vous devriez également tenir compte des répercussions de vos stratégies et de vos exigences sur les plans juridiques et du respect de la vie privée avant de les mettre en œuvre. Les considérations juridiques peuvent comprendre des restrictions imposées aux données utilisées sur un appareil PAP, comme les données assujetties à une entente de confidentialité ou les données qui pourraient exposer les renseignements personnels de Canadiens. Veuillez prendre note que les conseils énoncés dans le présent document ne constituent pas des avis juridiques. Vous devriez obtenir les conseils d'un avocat pour vous assurer que vous respectez toutes les lois canadiennes.

2.1 Mise en œuvre de stratégies

La mise en œuvre de stratégies organisationnelles normalise les rôles, les responsabilités et les comportements attendus de tous les employés. Vous devriez obtenir l'approbation et l'appui des membres de la haute direction et des cadres supérieurs de votre organisation en ce qui a trait à ces stratégies. Celles-ci peuvent aider à définir la façon d'appliquer les pratiques exemplaires, de même que la raison et le moment de leur application. Elles fournissent également une structure pour la gouvernance des données. Votre organisation devrait examiner ses stratégies régulièrement pour s'assurer qu'elles sont toujours pertinentes et les mettre à jour au besoin.

2.1.1 Stratégie d'utilisation acceptable

Ce type de stratégie permet de clarifier les services, les réseaux, les systèmes ou les sites Web qui peuvent être utilisés ou non, en vue de réduire la responsabilité légale et de donner aux utilisateurs des paramètres clairs. Il est recommandé que tous les employés, actuels et nouveaux, signent la stratégie d'utilisation acceptable. Autrement, vous pouvez leur faire signer un document distinct pour attester qu'ils ont lu la stratégie, qu'ils la comprennent et qu'ils l'acceptent.
Votre organisation peut choisir de demander aux employés de signer ce document périodiquement (annuellement, par exemple) ou lorsque des changements sont apportés à la stratégie.

2.1.2 Stratégie PAP

Une stratégie PAP doit mettre en œuvre les restrictions supplémentaires qui s'appliquent aux appareils visés par un modèle de déploiement PAP et établir les employés qui peuvent utiliser le modèle PAP au sein de l'organisation. La stratégie doit définir clairement les rôles de l'organisation et ceux des utilisateurs finaux en ce qui a trait à la sécurisation des données et des systèmes.

Votre stratégie doit également s'aligner sur la stratégie organisationnelle de gestion de l'information et décrire les procédures appropriées de conservation, de copie, de synchronisation ou d'élimination des données organisationnelles.

Voici quelques exemples d'aspects que vous devriez aborder dans la stratégie :

- les responsabilités des utilisateurs;
- la responsabilité liée au plan de téléphonie cellulaire;
- les exigences d'installation d'un logiciel MDM ou de gestion des applications mobiles (MAM pour *Mobile Application Management*);
- le maintien de l'accès limité aux données organisationnelles;
- les pratiques organisationnelles en vigueur relatives à la protection des renseignements personnels dans le cadre de l'utilisation d'un appareil PAP à des fins personnelles et professionnelles;
- les appareils, systèmes d'exploitation et logiciels approuvés;
- les classes de données autorisées ou interdites aux fins d'accès, de développement ou de stockage sur les appareils PAP.

La stratégie PAP doit également préciser les utilisations sanctionnées de l'environnement conteneurisé ou de type bac à sable (défini à la section 2.4.1.5) sur un appareil PAP et la gestion acceptable de l'appareil par l'entreprise sans dépasser certaines limites. Les appareils débridés devraient être interdits puisque ces appareils modifiés sont plus permissifs et fournissent un accès système accru tout en évitant certaines mesures de sécurité. Il est également recommandé d'établir les technologies MAM, MDM et UEM précises de même que les types d'appareils auxquels elles s'appliquent.

Les solutions de défense contre les menaces visant les applications mobiles (MTD pour *Mobile Threat Defender*) vont plus loin en vous offrant des détails sur les risques associés à une application précise. Ces solutions intègrent habituellement des plateformes de protection des terminaux (EPP pour *Endpoint Protection Plateform*) mobiles ou des agents de détection et d'intervention sur les terminaux (EDR pour *Endpoint Detection and Response*) mobiles qui sont contrôlés soit par la stratégie de l'administrateur, soit de façon interactive par l'utilisateur en lui demandant s'il souhaite autoriser l'exécution d'une application potentiellement risquée.

2.1.3 Stratégie de chiffrement et de sécurité des données

Le chiffrement protège la confidentialité et l'intégrité de données sensibles. Votre stratégie de chiffrement et de sécurité des données définit les exigences en matière de chiffrement des données, les algorithmes de chiffrement acceptables ainsi que les paramètres que votre organisation considère comme sécurisés. Elle devrait aborder le chiffrement des supports amovibles, des données au repos et de la couche transport. La stratégie devrait également définir la norme à adopter selon la classe de données en question.

Pour obtenir des recommandations sur les algorithmes cryptographiques, veuillez consulter l'ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* [6].

2.1.4 Stratégie de gouvernance des données ou de gestion de l'information

La gouvernance des données désigne le processus de gestion de la disponibilité, de l'utilisabilité, de l'intégrité et de la sécurité des données organisationnelles. Votre stratégie de gouvernance des données définit les rôles et responsabilités relatifs à la gestion de l'information pour en assurer l'alignement sur les exigences législatives et réglementaires ainsi que sur les besoins opérationnels. Cette stratégie permet d'assurer l'utilisation appropriée des données et leur conformité à une norme appliquée dans l'ensemble de l'organisation. La stratégie de gouvernance des données devrait décrire les exigences relatives à la conservation et à l'élimination des données, les méthodes d'élimination acceptables et le cycle de vie général des données en fonction de leur catégorie ou de leur classification. Elle devrait également établir les exigences en matière de résidence des données de même que les contrôles des données.

2.1.5 Stratégie d'authentification

Une stratégie d'authentification définit les exigences organisationnelles relatives à un processus sécurisé et acceptable d'autorisation des appareils, des applications et des conteneurs. Dans les environnements à faible sensibilité, il peut s'avérer suffisant d'adopter des pratiques exemplaires minimales relatives à la création de mots de passe. Pour les organisations qui recueillent et conservent des renseignements sensibles, comme des renseignements de nature médicale ou financière, les exigences doivent être beaucoup plus rigoureuses compte tenu des exigences accrues en matière de sécurité et de confidentialité des systèmes et des données auxquels les personnes autorisées ont accès. L'authentification multifacteur (MFA pour *Multi-Factor Authentication*) devrait être mise en œuvre dans la mesure du possible et un modèle de contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*) devrait être suivi pour les appareils PAP.
La stratégie organisationnelle devrait établir les périodes d'expiration des mots de passe, si la réutilisation deS mots de passe est autorisée, les personnes autorisées à réinitialiser ou à changer un mot de passe, de même que les mécanismes employés pour stocker les justificatifs d'identité de façon sécurisée.

Pour obtenir d'autres pratiques exemplaires en matière de mots de passe, consultez l'ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe* [7].

2.1.6 Stratégie d'application des correctifs

Chaque jour, de nouveaux exploits qui menacent les terminaux sont découverts. Afin de protéger vos terminaux contre ces exploits et contre les cybermenaces, vous devez mettre à jour régulièrement tous les systèmes d'exploitation et toutes les applications sur vos appareils, et installer les correctifs de sécurité. Une stratégie d'application des correctifs permet à votre organisation d'établir ce qui doit être corrigé régulièrement, comme les systèmes d'exploitation, les applications, les systèmes antimaliciels ou antihameçonnage et l'équipement réseau sur les ordinateurs ou appareils mobiles. La stratégie doit également définir les processus d'identification, d'acquisition, de mise à l'essai, d'installation et de vérification des correctifs. Elle doit désigner les personnes qui sont autorisées à exécuter les processus d'application des correctifs ainsi que les personnes devant être informées advenant l'échec de l'application d'un correctif et dans quel laps de temps.

De plus, vous devez être conscient que l'application des correctifs aux appareils PAP peut s'avérer complexe. Les difficultés découlent du fait que ces appareils appartiennent aux utilisateurs finaux et sont donc gérés par ceux-ci. Vous devez déterminer la façon dont vous répondrez aux exigences liées à l'application des correctifs et atténuerez les vulnérabilités de sécurité potentielles sur les appareils personnels. Les attaques modernes ciblent couramment le mode noyau, lequel donne un accès complet et de bas niveau à votre appareil. Afin d'atténuer les nombreuses vulnérabilités de sécurité du noyau et du mode noyau, il est nécessaire d'appliquer les correctifs aux appareils.

Pour obtenir de plus amples renseignements sur l'application des correctifs, consultez l'ITSAP.10.096, *Application des mises à jour sur les dispositifs* [8].

2.1.7 Stratégie d'utilisation des réseaux Wi-Fi publics

Vous devriez élaborer une stratégie distincte, ou une section dans une autre stratégie, sur l'autorisation ou l'interdiction d'utiliser les réseaux Wi-Fi publics ou non fiables, tels que les réseaux offerts dans les cafés ou dans les hôtels et les réseaux non gérés. Cette stratégie ou section devrait dicter les exigences de votre organisation, notamment l'utilisation d'un réseau privé virtuel (RPV) organisationnel, l'accès limité aux classes de données moins confidentielles ou les mesures de précaution supplémentaires à prendre pour empêcher les auteurs de menace d'effectuer de l'écoute électronique et d'obtenir des données.

Pour connaître les pratiques exemplaires concernant l'utilisation des réseaux Wi-Fi et des RPV, lisez l'ITSAP.80.009, *Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation* [9] et l'ITSAP.80.101, *Les réseaux privés virtuels* [10].

2.1.8 Stratégie de gestion des incidents

Une stratégie de gestion des incidents doit décrire les mesures d'intervention organisationnelles en cas d'incident de sécurité, d'atteinte à la vie privée ou de fuite de données. Elle doit détailler les procédures de détection, de confinement, d'examen, d'atténuation et de signalement pour chaque type d'incident. Compte tenu de la nature des modèles PAP, ces procédures reposent ultimement sur le principe que le propriétaire de l'appareil doit être suffisamment technophile pour remarquer une atteinte à la sécurité (sur l'appareil ou dans une application organisationnelle) et que l'utilisateur final doit signaler l'incident. La stratégie doit identifier les responsables pour chaque élément et devrait faire partie de la formation donnée aux employés. Il convient de noter qu'à la suite d'un incident de sécurité, il faut souvent prendre des mesures radicales, comme le nettoyage complet d'un appareil, et que de telles mesures ne sont généralement pas bien accueillies par les propriétaires d'appareils personnels. Enfin, votre organisation doit revoir et mettre à l'essai régulièrement cette stratégie pour veiller à ce qu'elle soit à jour.

2.2 Création de procédures d'intégration et d'annulation de l'intégration

Vous devez avoir des processus et des procédures clairement définis pour l'intégration ainsi que l'annulation de l'intégration des appareils PAP dans votre environnement organisationnel.

Pour ce qui est de la stratégie PAP de votre organisation, vous pouvez choisir d'autoriser uniquement certains appareils précis aux fins d'intégration. Vous devez vous assurer que tous les utilisateurs finaux ont lu et comprennent bien leurs rôles et responsabilités à l'égard de toutes les stratégies de l'organisation. Au cours de l'intégration, assurez-vous que toutes les activités suivantes sont réalisées :

- assurer le suivi de tous les appareils en stock;
- balayer les appareils pour détecter les applications et logiciels malveillants (maliciels) à l'aide d'une solution de défense contre les menaces visant les applications mobiles (MTD);
- informer les utilisateurs des politiques et de l'exigence concernant la sécurisation des appareils au moyen d'un mécanisme d'authentification qui répond à la stratégie organisationnelle;
- utiliser une liste d'appareils PAP approuvés pendant le processus d'intégration;
- activer le chiffrement sur l'appareil, un conteneur ou un bac à sable, ainsi que des canaux de communication utilisés aux fins organisationnelles, comme pour le courrier électronique et les applications;
- corriger et atténuer les vulnérabilités logicielles qui peuvent être présentes sur l'appareil.

Pendant le processus d'annulation de l'intégration, les données organisationnelles qui sont conservées sur l'appareil doivent être nettoyées et l'accès aux ressources de l'organisation doit être retiré pour empêcher les atteintes à la protection des données et les fuites de données découlant d'un appareil non géré. Pour réaliser un nettoyage complet de l'appareil, il faut d'abord obtenir le consentement de l'utilisateur puisque celui-ci est le propriétaire de l'appareil et que toutes ses données personnelles seront effacées. Dans la mesure du possible, réalisez un nettoyage sélectif afin de nettoyer uniquement les données associées au compte organisationnel. Pour obtenir de plus amples renseignements sur le nettoyage, consultez l'ITSAP.40.006, *Nettoyage et élimination d'appareils électroniques* [11] et l'ITSP.40.006, *Nettoyage des supports de TI* [12].

Lorsqu'un employé change de poste au sein de votre organisation, vous devez examiner l'information stockée sur son appareil et évaluer si le principe du besoin de connaître s'applique. Les données ou les applications qui ne sont plus pertinentes dans le cadre du nouveau poste de l'employé doivent être retirées de l'appareil. Cette mesure permettra d'assurer la protection des données organisationnelles de grande valeur.

2.3 Protection et traitement sécurisés des données

La protection et le traitement des données de façon sécurisée permettent de veiller à ce que tout incident de sécurité ou toute activité malveillante dans une application, un dispositif, un réseau ou un système se limite à la zone ou au périmètre de sécurité. Il existe quatre mesures que votre organisation peut mettre en œuvre afin d'accroître la sécurité de ses données.

2.3.1 Classification des données

La classification des données permet de veiller à ce que les données sensibles ne sortent jamais d'une zone où elles ne peuvent être protégées et de limiter les dommages potentiels advenant une atteinte à la protection des données.
Elle consiste à appliquer des contrôles précis à chaque classe de données en fonction du niveau requis de confidentialité, d'intégrité et de disponibilité des données. Les données devraient être structurées selon les exigences de l'organisation, de même que les exigences en matière de sécurité et de confidentialité. Les ministères et organismes du gouvernement du Canada (GC) doivent suivre les exigences du GC relatives à la classification des données.

Vous trouverez ci-dessous un exemple de méthode pour structurer les classes de données :

Classe 1 : Données publiques

Cette classe de données sert à définir les données accessibles au public. Le traitement de ces données en interne ou en externe ne porte pas atteinte à l'entreprise, aux clients, au personnel ou aux fournisseurs. Les exemples de données publiques comprennent les pages Web publiques, les brochures et les cartes professionnelles de l'entreprise.

Classe 2 : Données réservées à une utilisation interne

Ce type de données ne doit être utilisé qu'au sein de l'entreprise par le personnel autorisé. Les données réservées à une utilisation interne contiennent de l'information légèrement sensible (c.-à-d. qui ne comprend pas de l'information nominative [PII pour *Personally Identifiable Information*]) au sujet des opérations, des politiques et des plans d'activités de l'organisation. Les notes de service et les courriels de nature professionnelle en sont des exemples. La divulgation de ces données à des personnes non autorisées poserait un risque minimal pour l'entreprise.

Classe 3 : Données confidentielles

Ces données, qui se limitent à un groupe particulier au sein de l'organisation, exigent un niveau d'habilitation spécial ou des autorisations claires pour ce qui est de leur utilisation et de leur accès. Les données confidentielles peuvent contenir de l'information nominative qui risque de causer des dommages considérables pour l'organisation, les employés et les parties concernées advenant sa compromission. En règle générale, ces données sont protégées en vertu des Normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS pour *Payment Card Industry Data Security Standard*) et de la Health Insurance Portability and Accountability Act (HIPAA) ou régies par l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM) ou l'Association canadienne des courtiers de fonds mutuels (ACFM). Parmi les exemples de données confidentielles, on retrouve les données commerciales exclusives, les données de recherche, le code source d'un logiciel, la propriété intellectuelle et l'information nominative.

Il existe plusieurs autres méthodes de classification des données. Pour obtenir une liste des différentes méthodes et de l'information additionnelle, veuillez consulter la *Loi sur la protection des renseignements personnels et les documents électroniques* [1] et la *Loi sur la protection des renseignements personnels* [2].

La mise en place de stratégies et des contrôles de sécurité n'élimine pas le risque résiduel. Afin de réduire les risques liés aux appareils compromis des utilisateurs finaux, votre organisation doit limiter l'information à laquelle les appareils peuvent accéder ainsi que l'information stockée ou synchronisée sur ces appareils. À titre d'exemple, il se peut que vous deviez synchroniser vos courriels avec l'appareil pour les consulter hors ligne, mais vous ne devriez pas synchroniser l'ensemble de votre boîte aux lettres; la boîte de réception d'un utilisateur devrait uniquement afficher les courriels récents (des dernières semaines). Les utilisateurs finaux ne doivent pas être en mesure d'accéder aux systèmes qui contiennent des données sensibles, telles que des justificatifs d'identité ou des numéros d'assurance sociale (NAS), au moyen de leurs appareils personnels. Ils doivent seulement être autorisés à accéder à de l'information non sensible.

Afin de déterminer l'information à laquelle les appareils personnels peuvent accéder ou l'information pouvant être stockée ou synchronisée sur ces appareils, consultez la structure des classes de données de votre organisation. N'oubliez pas que de nombreux services auxquels accèdent les appareils mobiles sont maintenant hébergés dans le nuage. Par conséquent, les données pourraient ne pas être stockées localement, comme dans un cache hors ligne.

2.3.2 Segmentation réseau

Vous devriez segmenter les réseaux de votre organisation en différentes zones de sécurité. Une zone est un périmètre clairement délimité avec des points de connexion. Les zones présentent divers niveaux de sensibilité et contiennent différentes classes de données. Si vous adoptez un modèle de déploiement PAP, vous pouvez utiliser la segmentation réseau pour réduire votre zone d'attaque ainsi que les risques d'accès non autorisé aux données ou de divulgation des données. Il convient toutefois de noter que la segmentation réseau n'empêchera pas les appareils mobiles d'accéder directement aux services infonuagiques. Elle empêchera seulement l'accès des appareils mobiles aux services offerts sur votre réseau local.

Pour obtenir de plus amples détails sur la segmentation réseau, consultez l'ITSP.80.022, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada* [13] et l'ITSG-38, *Zones de sécurité des réseaux – Considérations en matière de conception liées au placement de services dans des zones* [14].

2.3.3 Séparation entre les données personnelles et les données de l'entreprise

Comme il a été mentionné précédemment, limiter l'accès aux données selon le principe du besoin de connaître permettra de réduire la zone d'attaque d'un auteur de menace advenant la compromission d'un compte ou d'un système. La séparation entre les répertoires de données organisationnelles et les données personnelles fait partie intégrante de la protection des données de l'entreprise. Vous devriez envisager de séparer les types de données suivants si vous déployez un modèle PAP dans votre organisation. Dans la plupart des cas, vous pouvez employer un logiciel de gestion des appareils mobiles (MDM), un logiciel de gestion unifiée des terminaux (UEM) ou un logiciel de gestion des applications mobiles (MAM) accompagné d'une solution de défense contre les menaces visant les applications mobiles (MTD).

- Contacts
- Service d'envoi de messages courts (SMS pour *Short Message Service*) ou service de messagerie multimédia (MMS pour *Multimedia Messaging Service*)
- Comptes de courrier électronique
- Comptes de médias sociaux
- Accès aux applications (capacités d'interaction avec les applications organisationnelles et personnelles)

2.4 Application de contrôles de sécurité techniques

Tandis que les stratégies aident à régir la réglementation appliquée à l'échelle de l'organisation, les contrôles techniques aident à appliquer les exigences relatives à ces stratégies. Les contrôles techniques sont déployés avec des logiciels ou du matériel informatique pour prévenir les incidents de sécurité ou en réduire les effets. Ces contrôles peuvent être appliqués automatiquement ou faire partie d'un processus manuel.

Pour mettre en œuvre les contrôles techniques de façon appropriée, vous pourriez nécessiter un soutien technique additionnel.

2.4.1 Contrôles liés aux appareils des utilisateurs finaux

2.4.1.1 Gestion des appareils

Les logiciels MDM, MAM ou UEM peuvent fournir une visibilité dans les appareils, appliquer les stratégies et contrôles techniques aux appareils, de même que limiter les types d'attaques employés pour compromettre la sécurité des appareils. Les logiciels MDM, MAM ou UEM peuvent être hébergés de façon autonome, dans le nuage ou par le fournisseur, selon les exigences organisationnelles. Certains fabricants d'appareils intègrent des méthodes pour connecter un appareil à un logiciel MDM. Cependant, un logiciel tiers est généralement employé pour mettre en œuvre toutes les fonctionnalités du produit choisi.

Un logiciel MAM contrôle seulement les applications sur l'appareil et n'appliquera pas de façon uniforme les stratégies visant l'ensemble de l'appareil. En règle générale, un logiciel MAM sert à contrôler les fonctions d'une application, à forcer l'application de paramètres par défaut plus sécurisés ou à isoler les applications d'entreprise des applications personnelles.

Un logiciel MDM ou UEM assure la configuration uniforme et fiable du matériel à l'aide de mécanismes automatisés. Il peut limiter les fonctionnalités au profit d'un environnement mieux sécurisé, installer des applications ou fonctions requises, et aider à diagnostiquer et à résoudre les problèmes touchant les appareils. Dans un environnement PAP, les organisations peuvent imposer peu de fonctions d'un logiciel MDM ou UEM puisque celles-ci doivent s'appliquer uniquement aux applications d'entreprise, et non à l'ensemble de l'appareil (à l'exception du mot de passe de l'appareil et du verrouillage automatique après un délai d'inactivité). De nombreux logiciels MDM peuvent également empêcher la connexion des appareils débridés.

2.4.1.2 Antimaliciels, solutions de défense contre les menaces visant les applications mobiles (MTD) et plateformes de protection des terminaux (EPP)

Un antimaliciel est un logiciel qui combat les éléments de code malveillants. Il est fortement recommandé de déployer un antimaliciel non seulement sur les appareils d'entreprise, mais également sur les ordinateurs portables et les ordinateurs de bureau personnels, puisqu'il fournit une confirmation de plus que l'appareil n'a pas été infecté. Comme l'état antérieur des appareils PAP est inconnu, ces appareils doivent faire l'objet d'un balayage avant d'être autorisés à établir une connexion et constamment lors de leur utilisation continue.

Mettez à jour les définitions régulièrement pour veiller à ce que la base de données utilisée par le logiciel contienne les signatures et les heuristiques les plus récentes de façon à détecter le plus d'applications malveillantes possible.

Vous devriez prévoir des balayages s'ils ne sont pas configurés automatiquement par l'antimaliciel. Les balayages prévus permettent de trouver tout maliciel que le balayeur en temps réel peut avoir manqué ou qui a été placé sur l'appareil par un vecteur non surveillé.

N'oubliez pas qu'un antimaliciel n'est pas la première ligne de défense. Il sert simplement à découvrir les logiciels malveillants qui passent entre les mailles du filet.

Vous devez faire appel à des agents MTD et EPP pour assurer la sécurité des appareils mobiles tels que les téléphones cellulaires et les tablettes, puisque les antimaliciels ne sont pas efficaces à eux seuls sur ces plateformes.
Les solutions MTD et EPP sont avantageuses non seulement pour l'organisation, mais également pour le propriétaire de l'appareil, et elles peuvent être anonymisées pour éliminer toute préoccupation relative à la protection de la vie privée.

2.4.1.3 Applications et autorisations

Habituellement, les applications sont vérifiées initialement par le Google Play Store ou l'App Store d'Apple si elles sont installées à partir de l'une de ces sources. Toutefois, vous ne devez pas vous fier uniquement à ce processus de vérification initial. Les logiciels MDM et UEM peuvent réaliser un examen minutieux des applications d'entreprise en fonction de l'application particulière et des besoins en matière de sécurité de votre organisation. Par exemple, un logiciel MDM peut aider à réglementer des applications fiables et vérifiées qui sont autorisées aux fins d'utilisation dans l'espace de travail organisationnel de l'appareil mobile (voir la section 2.4.1.5, Cadres de bac à sable et mise en conteneur), et les stratégies relatives aux appareils mobiles ou PAP devraient aider à définir les exigences en ce qui a trait aux applications ou aux types d'applications autorisés.

Au cours de la vérification des applications, vous devriez considérer les autorisations que détiennent les applications et veiller à ce que seules les autorisations nécessaires leur soient accordées. À titre d'exemple, une application de calcul ne devrait pas avoir besoin d'accéder à l'emplacement GPS ou aux contacts, à moins que l'application offre une fonction qui l'exige. Passez toujours en revue l'accès qu'une application demande avant de l'accorder.

Les autorisations d'accès aux contacts de l'entreprise ne doivent pas être accordées depuis l'environnement de bac à sable personnel de l'appareil (voir la section 2.4.1.5, Cadres de bac à sable et mise en conteneur), puisque les applications non fiables dans le bac à sable personnel pourraient accéder aux coordonnées ou à d'autres informations sensibles (comme de l'information nominative) et les compromettre. Une solution de bac à sable, MDM ou UEM utilise généralement une liste de contacts distincte pour les besoins de l'entreprise.

Votre organisation devrait interdire les appareils mobiles débridés sur le réseau d'entreprise, puisque ceux-ci peuvent contourner certaines fonctions et autorisations de sécurité intégrées.

2.4.1.4 Stratégies de sécurité

Vous devriez utiliser diverses technologies pour appliquer vos stratégies écrites, notamment des stratégies de sécurité, des listes de contrôle d'accès (LCA) et des solutions MDM ou UEM, MAM et MTD. Les stratégies de sécurité permettent entre autres de limiter les fonctions (ou leur utilisation), d'appliquer des algorithmes sécurisés, d'assurer l'entropie des mots de passe et d'établir les applications pouvant être installées. Généralement, on applique les stratégies de sécurité à l'infrastructure réseau par l'entremise d'une solution MDM ou UEM, puis l'appareil de l'utilisateur final les met en application.

Une solution MDM réalisera les stratégies de sécurité s'appliquant à l'ensemble de l'appareil, comme l'entropie des mots de passe et les applications autorisées. Une solution MAM réalisera les stratégies propres aux applications, telles que les fonctions permises ou la capacité de copier-coller des données. Contrairement à une solution MDM qui met en œuvre des restrictions à grande échelle et de niveau plus élevé, une solution MAM s'occupe des contrôles plus pointus dans les applications.

2.4.1.5 Cadres de bac à sable et mise en conteneur

Un bac à sable est un environnement isolé qui limite l'accès d'autres applications et ressources de l'environnement de bac à sable, et qui limite l'accès à celles-ci. Le recours à un bac à sable sur un appareil PAP est particulièrement important puisque l'appareil contient des données et des applications de nature personnelle et professionnelle. En l'absence d'un bac à sable, un utilisateur pourrait installer une application malveillante (accidentellement ou intentionnellement) qui, dans certaines circonstances, pourrait accéder à des données confidentielles stockées dans une application d'entreprise ou perturber le fonctionnement de l'application. En revanche, un bac à sable ne donne aucune garantie que les ressources resteront séparées de façon sécurisée et, dans un modèle PAP, le propriétaire d'un appareil personnel peut, intentionnellement ou non, affaiblir la sécurité du bac à sable. Il est donc essentiel que le propriétaire de l'appareil assure la sécurité du système d'exploitation hôte.

Les exemples de cadres de bac à sable comprennent Samsung KNOX, un logiciel de kiosque, l'App Sandbox d'Apple et une machine virtuelle (MV) spécialisée qui est verrouillée ou en lecture seule. Certaines fonctions de ces cadres sont déjà activées sur les terminaux dans leur configuration d'usine, mais deviennent plus utiles lorsqu'elles sont accompagnées d'une solution MDM, UEM ou MAM.

Il arrive fréquemment que les cadres de bac à sabre entraînent des étapes supplémentaires ou des inconvénients mineurs pour l'utilisateur final. Ce dernier peut, par exemple, être appelé à obtenir des autorisations supplémentaires ou à autoriser un utilisateur, une application ou un code. Ainsi, vous devriez vous assurer que tous les utilisateurs comprennent pourquoi certains contrôles techniques sont en place et leurs répercussions sur la sécurité.

2.4.2 Contrôles liés à l'infrastructure

2.4.2.1 Filtrage de système d'adressage par domaines (DNS)

Le système d'adressage par domaines (DNS pour *Domain Name System*) est employé par tous les appareils connectés à Internet pour traduire du texte en adresse IP et ainsi vous permettre d'accéder aux ressources dont vous avez besoin. Un DNS peut servir à filtrer les hôtes malveillants et à empêcher toute redirection vers un site Web malveillant.

Les fournisseurs d'accès Internet (FAI) offrent leurs propres serveurs DNS publics, mais nous recommandons d'utiliser un service DNS différent pour profiter d'un meilleur rendement ainsi que de mesures de sécurité et de protection de la vie privée additionnelles. D'autres organisations offrent aussi des services DNS publics gratuits qui filtrent les requêtes DNS provenant de sites Web, d'hôtes et de systèmes malveillants. L'Autorité canadienne pour les enregistrements Internet (ACEI), un organisme sans but lucratif qui gère le domaine Internet .ca, offre un service DNS protégé sans frais appelé Bouclier canadien.

2.4.2.2 Analyse du comportement

Cette technique permet d'analyser les événements qui se produisent sur un appareil, un réseau, un système ou un service. Dans le cas d'un modèle PAP, cette analyse se limite généralement aux appareils, aux réseaux, aux systèmes et aux services contrôlés par l'entreprise. À titre d'exemple, l'analyse du comportement permet de détecter un appareil mobile qui consulte soudainement tous les dossiers des employés dans une application qui n'accède normalement qu'à quelques dossiers en très peu de temps, ou encore un appareil qui tente de se connecter à des milliers de ports TCP/UDP (*Transmission Control Protocol and User Data Protocol*) sur un réseau dans un délai très court. La surveillance réseau devrait être combinée à l'application de contrôles basés sur l'accès (comme les listes de contrôle d'accès [LCA]) et la restriction du volume de données pouvant être téléchargé sur un appareil PAP.

Les systèmes d'analyse du comportement comprennent par exemple les systèmes de détection d'intrusion (SDI), les systèmes de prévention d'intrusion (SPI) ainsi que les applications ou appliances de sécurité qui ont recours à l'intelligence artificielle pour analyser les habitudes d'utilisation et signaler les anomalies. Les solutions de défense contre les menaces visant les applications mobiles (MTD) sont employées couramment avec des composants RPP et EDR mobiles intégrés pour évaluer une application, puis autoriser ou interdire une action de l'application en ayant recours à une interaction avec l'utilisateur ou à l'application automatique de règles.

2.4.2.3 Logiciels antihameçonnage et antipourriels

Les technologies antihameçonnage et antipourriels sont essentielles à la protection des domaines de courrier électronique de votre organisation. Les normes utilisées couramment pour protéger les domaines de courrier électronique comprennent notamment les enregistrements pointeurs (PTR pour *Point Record*), les enregistrements DNS, les enregistrements SPF (pour *Sender Policy Framework*), les enregistrements DKIM (pour *DomainKeys Identified Mail*) de même que les enregistrements DMARC (pour *Domain-Based Message Authentication, Reporting, and Conformance*).

Par ailleurs, vous pouvez choisir d'utiliser un service antipourriel axé sur l'heuristique et sur les signatures. Normalement, ces services offrent aussi des services antimaliciels pour les messages en transit et filtrent en fonction de règles précises. Bien que bon nombre de ces applications fonctionnent au niveau de l'infrastructure, il existe des antimaliciels et suites de sécurité qui intègrent ces applications pour ordinateurs portables et ordinateurs de bureau. Les appareils mobiles tels que les téléphones cellulaires ne peuvent pas facilement exécuter des fichiers malveillants sur les appareils. Par conséquent, ces plateformes ont tendance à utiliser exclusivement les solutions fournies par l'infrastructure.

Il n'existe pas de solution ou de logiciel parfait, mais une bonne solution peut réduire considérablement la quantité de pourriels et de courriels malveillants qui réussissent à se rendre aux utilisateurs et ainsi réduire le risque de compromission.

Pour obtenir de plus amples renseignements sur la protection des domaines de votre organisation contre l'usurpation d'adresses électroniques, consultez l'ITSP.40.065, *Directives de mise en œuvre : Protection du domaine de courrier* [15].

2.4.2.4 Listes de contrôle d'accès et sensibilité des données

Sur les plateformes qui les prennent en charge (ordinateurs portables et de bureau), les listes de contrôle d'accès vous permettent de définir les autorisations accordées à un groupe ou à un utilisateur précis concernant l'accès aux ressources organisationnelles (p. ex., un lecteur réseau, une boîte de réception, des fonctions administratives). Si vous avez recours à un modèle de déploiement PAP, vous devez définir l'accès accordé aux appareils. Vous devriez appliquer le principe du droit d'accès minimal pour veiller à ce que les employés aient accès uniquement aux ressources et à l'information dont ils ont besoin pour réaliser leurs tâches professionnelles. Limiter l'accès réduit la zone d'attaque et les dommages advenant la compromission d'un appareil.

Par exemple, vous pourriez établir un périmètre sécurisé sur le réseau pour vous assurer que seuls les appareils appartenant à l'organisation y ont accès.

2.4.2.5 Réseaux privés virtuels (RPV)

Un RPV est une connexion sécurisée entre deux points, comme entre un ordinateur portable et le réseau de votre organisation ou entre une application et un serveur. Le RPV sert de tunnel par l'entremise duquel vous pouvez envoyer et recevoir des données sécurisées sur un réseau physique existant. Lorsque vous utilisez un RPV, les données sont chiffrées pendant leur transmission. En cas d'interception, un attaquant ne pourrait donc pas visualiser les données à moins de détenir la clé de déchiffrement.

Plusieurs types de RPV peuvent être employés dans un modèle de déploiement PAP :

- **D'hôte à passerelle (accès à distance) :** Ce type de connexion permet d'accéder à distance à un réseau d'entreprise à partir d'un appareil. Il s'agit de la méthode la plus courante dans un environnement d'entreprise pour permettre aux utilisateurs de se connecter aux ressources organisationnelles. Vous devriez faire appel à l'authentification multifacteur pour sécuriser la connexion à ce service et vous devriez, dans la mesure du possible, éviter la tunnellisation fractionnée qui permet à un hôte d'utiliser sa connexion Internet directe et le réseau distant simultanément**.**
- **D'hôte à hôte :** Ce type de connexion permet de connecter un hôte à une ressource particulière se trouvant sur un réseau d'entreprise ou à un autre hôte.
- **D'application à serveur ou accès réseau à vérification systématique (ZTNA pour *Zero Trust Network Access*) :** Certaines applications modernes créent un tunnel TLS (pour *Transport Layer Security*; sécurité de la couche transport) privé entre elles et leur serveur, ce qui fournit une connexion sécurisée pour transférer les données en dehors d'un tunnel RPV standard. Le ZTNA est également utilisé au niveau de l'application ou d'un groupe d'applications pour former une frontière basée sur le contexte et l'identité. Cette technologie authentifie chaque application et chaque utilisateur pour veiller au respect du principe du besoin de connaître. Alors que les RPV traditionnels fournissent un accès réseau, les connexions ZTNA ne fournissent pas de visibilité réseau par défaut.
- **RPV tiers :** Ce type de connexion consiste en une connexion sécurisée entre un point d'accès public (comme le réseau Wi-Fi d'un aéroport ou d'un hôtel) et le RPV d'un fournisseur tiers. Il redirige le trafic de l'utilisateur pour qu'il semble provenir du réseau du fournisseur tiers. Les RPV tiers ne sont pas recommandés pour les entreprises puisqu'ils n'offrent pas de réelles solutions de sécurité ou de protection des données de bout en bout au-delà du réseau local.

Si vous avez des employés qui travaillent à distance et doivent utiliser des réseaux publics ou non sécurisés, le recours à un RPV ou à des microtunnels ZTNA leur permettra d'établir une connexion sécurisée qui fait appel à l'authentification et assure la protection des données. L'authentification peut être réalisée à l'aide de certificats ou de justificatifs d'identité habituels et devrait être multifactorielle.

Pour en savoir plus sur les RPV, consultez l'ITSAP.80.101, *Les réseaux privés virtuels* [10].

2.4.2.6 Environnements infonuagiques

Les environnements infonuagiques fournissent une barrière à faible entrée permettant aux petites organisations de profiter de contrôles de sécurité sophistiqués qui peuvent les aider à sécuriser les appareils PAP de façon rentable. Vous pouvez ainsi tirer parti de fonctions de sécurité qui sont développées et gérées par les équipes étoffées du fournisseur de services infonuagiques et qui ne seraient pas accessibles autrement ou qui exigeraient un gros investissement financier. Si l'appareil d'un utilisateur final compromet le service infonuagique, les conséquences ne sont pas aussi dommageables puisque l'auteur de menace n'aura pas accès aux données stockées ailleurs que sur l'appareil. Par contre, même si vous utilisez des services infonuagiques, votre organisation est toujours légalement responsable de la protection de ses données.

2.5 Formation des employés

La formation est un élément essentiel de la cybersécurité de votre organisation et accroît la cybersécurité globale de votre organisation en responsabilisant les employés quant à leurs propres pratiques de cybersécurité. Quiconque a accès à vos réseaux, à vos systèmes, à vos appareils et à votre information doit comprendre ses rôles et responsabilités en matière de cybersécurité. En formant vos employés, vous leur donnez l'occasion de prendre connaissance de vos stratégies et des rudiments de la sécurité (p. ex., repérer les messages d'hameçonnage, appliquer l'authentification multifacteur, télétravailler en toute sécurité, signaler les incidents de sécurité et être conscients des atteintes à la vie privée).

Dans le contexte des modèles PAP, votre organisation devrait sensibiliser vos employés aux systèmes offerts sur les appareils personnels, aux classes de données qui peuvent être stockées sur les appareils personnels, à la formation sur les applications mobiles, aux calendriers de conservation et d'élimination des données organisationnelles, à leurs droits d'accès, aux conseils pour sécuriser leurs appareils personnels et aux pratiques de divulgation appropriées. Les stratégies et contrôles techniques PAP devraient être présentés comme des moyens d'augmenter la sensibilisation, la cohérence et la sécurité organisationnelles.

Les utilisateurs doivent avoir accès aux stratégies, aux guides opérationnels ou aux procédures qui énoncent la manière d'interagir avec les systèmes et les données en toute sécurité. Vous devriez revoir ces stratégies et instruments régulièrement et les mettre à jour au besoin.

Divers cours sur la sécurité sont offerts en ligne pour parfaire ses connaissances générales de la sécurité des appareils mobiles. Ces cours doivent mettre l'accent sur les façons de sécuriser un appareil mobile (comme un ordinateur portable, un téléphone cellulaire ou une tablette), sur la marche à suivre lorsque des invites de sécurité s'affichent ou sur les fausses perceptions courantes au sujet de la sécurité des appareils mobiles. Le Carrefour de l'apprentissage du Centre pour la cybersécurité propose des programmes et des activités de formation en classe et en ligne destinés à divers publics, notamment le personnel n'ayant pas de compétences techniques, les praticiens des TI et les gestionnaires de niveau supérieur. Actuellement, ces programmes et activités sont offerts essentiellement aux employés du gouvernement du Canada (GC) et des partenaires nationaux. Cependant, les employés des gouvernements et organismes provinciaux et municipaux, ainsi que des partenaires du secteur privé qui collaborent avec les ministères du GC, peuvent également y participer.

Les cours du Carrefour de l'apprentissage peuvent être offerts à l'ensemble d'une organisation, à de petits groupes ou à des employés en particulier. Ils portent sur les sujets suivants :

- la gestion des risques liés à la sécurité des TI;
- la cybersécurité pour les développeurs et les praticiens de la sécurité;
- la sécurité des communications;
- la sécurité cryptographique.

Les cours offerts peuvent changer à tout moment. Pour de plus amples renseignements à ce sujet, vous pouvez consulter le calendrier des cours sur le site Web du Carrefour de l'apprentissage.

Le cours *Sensibilisation à la protection de la vie privée* [16] offert par le GC est également une excellente ressource pour comprendre les engagements en matière de protection de la vie privée, y compris la gestion des risques et la conformité.

Pour en savoir plus sur la formation, consultez l'ITSM.10.093, *Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité* [17].

3 Sommaire

Il y a des avantages et des risques associés à chacun des modèles de déploiement des appareils mobiles. Cependant, certains modèles de déploiement permettent de mettre en œuvre un plus grand nombre de mesures d'atténuation que d'autres modèles. La plupart des risques liés aux modèles PAP sont incontrôlables puisque les appareils appartiennent aux employés. Les appareils appartenant à l'organisation permettent de mieux contrôler les données sur les appareils de même que les contrôles de sécurité techniques qui sont mis en œuvre.

Si vous optez pour un modèle PAP, votre organisation doit mener une évaluation des risques et mettre en place des stratégies et des contrôles techniques pour réduire les risques à un niveau acceptable. Vous devez également tenir compte du soutien technique additionnel ainsi que des répercussions sur le plan juridique associés à un modèle PAP, sans oublier les contrôles techniques que vous devez mettre en œuvre.

4 Contenu complémentaire

4.1 Liste des acronymes et des sigles

Acronyme ou sigle	Expression au long
ACFM	Association canadienne des courtiers de fonds mutuels
MMS	Service de messagerie multimédia (*Multimedia Messaging Service*)
CST	Centre de la sécurité des télécommunications
DKIM	Protocole DKIM (*DomainKeys Identified Mail*)
DMARC	Protocole DMARC (*Domain-based Message Authentication, Reporting and Conformance*)
DNS	Système d'adressage par domaines (*Domain Name System*)
EDR	Détection et intervention sur les terminaux (*Endpoint Detection and Response*)
EPP	Plateforme de protection des terminaux (*Endpoint Protection Platform*)
FAI	Fournisseur d'accès Internet
GC	Gouvernement du Canada
MAM	Gestion des applications mobiles (*Mobile Application Management*)
MDM	Gestion des appareils mobiles (*Mobile Device Management*)
MTD	Solution de défense contre les menaces visant les applications mobiles (*Mobile Threat Defender*)
NAS	Numéro d'assurance sociale
SMS	Service d'envoi de messages courts (*Short Message Service*)
OCRCVM	Organisme canadien de réglementation du commerce des valeurs mobilières
PAP	Prenez votre appareil personnel
PCI	Industrie des cartes de paiement (*Payment Card Industry*)
PCI DSS	Normes de sécurité sur les données de l'industrie des cartes de paiement (*Payment Card Industry Data Security Standard*)
PII	Information nominative (*Personally Identifiable Information*)
PTR	Enregistrement pointeur (*Point Record*)
RPV	Réseau privé virtuel
SDI	Système de détection d'intrusion
SPF	Protocole SPF (*Sender Policy Framework*)
SPI	Système de prévention d'intrusion
TCP/UDP	Protocole TCP/UDP (*Transmission Control Protocol and User Datagram Protocol*)
TLS	Protocole TLS (sécurité de la couche de transport; *Transport Layer Security*)
TI	Technologies de l'information
UEM	Gestion unifiée des terminaux (*Unified Endpoint Management*)

4.2 Glossaire

Terme	Définition
Bac à sable	Structure de sécurité permettant de séparer différents ensembles d'applications, comme les données personnelles et les données organisationnelles sur un appareil mobile.
Confidentialité	Aptitude à protéger l'information sensible contre les accès non autorisés.
Détection et intervention sur les terminaux (EDR)	Logiciel utilisé sur les terminaux, de pair avec une plateforme de protection des terminaux, pour détecter et prévenir les activités malveillantes. Il peut également assainir les terminaux de façon à rétablir l'état dans lequel ils se trouvaient avant l'infection.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, des logiciels et du matériel informatique (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés et les compromissions.
Gestion des appareils mobiles (MDM)	Logiciel capable de sécuriser, de fournir, de surveiller, de gérer et de prendre en charge les appareils mobiles déployés dans un réseau en contrôlant et en protégeant les données de même que les paramètres de configuration. Puisque la capacité des différents progiciels de gestion des appareils mobiles peut varier considérablement, il faut sélectionner la solution appropriée avec soin. Ce logiciel est différent d'un logiciel de gestion des applications mobiles en ce sens qu'il vise le système d'exploitation et l'appareil en tant que tels, plutôt que les détails des applications installées.
Gestion des applications mobiles (MAM)	Logiciel capable de sécuriser, de surveiller, de gérer et de prendre en charge les applications installées sur un appareil mobile configuré correctement ou sur lequel est installé l'agent logiciel. Ce logiciel est différent d'un logiciel de gestion des appareils mobiles en ce sens qu'il vise les applications exécutées sur l'appareil, plutôt que l'appareil en tant que tel, bien qu'il y ait parfois un chevauchement.
Gestion unifiée des terminaux (UEM)	Semblable à un logiciel de gestion des appareils mobiles, logiciel capable de sécuriser, d'approvisionner, de surveiller, de gérer et de prendre en charge des appareils tels que des tablettes, des téléphones cellulaires, des ordinateurs portables et des ordinateurs de bureau. Ce logiciel est différent d'un logiciel de gestion des appareils mobiles en ce sens qu'il a été conçu pour servir de point central de gestion pour tous les appareils, tous les systèmes d'exploitation et la sécurité de tous les terminaux.
Information nominative (PII)	Renseignement permettant de déterminer directement ou indirectement l'identité d'une personne.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles et inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Maliciel de minage	Programme malveillant dont l'objectif consiste à chiffrer les données et applications de la cible. Il est normalement accompagné d'une demande de rançon que la cible doit payer pour que ses fichiers soient déverrouillés ou déchiffrés.
Plateforme de protection des terminaux (EPP)	Solution logicielle utilisée sur les terminaux pour détecter et prévenir les activités malveillantes et les attaques par maliciel basées sur les fichiers. Elle permet également d'intervenir de façon dynamique en cas d'alerte et d'incident de sécurité.
Prenez vos appareils personnels (PAP)	Les employés utilisent leurs propres appareils à des fins opérationnelles, et l'organisation peut décider de rembourser certains coûts associés aux appareils. Toutefois, puisque ces appareils ne lui appartiennent pas, l'organisation a peu d'emprise sur les contrôles de sécurité mis en place sur les appareils.

Terme	Définition
Principe du droit d'accès minimal	Principe selon lequel il convient de n'accorder à l'utilisateur que les autorisations d'accès dont il a besoin pour accomplir les tâches autorisées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation accidentelle, incorrecte ou non autorisée d'un système d'information.
Risque	Probabilité qu'une menace donnée compromette des biens TI et cause un préjudice.
Sécurité de la couche transport (TLS)	Protocole qui permet de protéger la confidentialité, l'intégrité et la disponibilité des communications Internet entre le serveur et les applications clients.
Solution de défense contre les menaces visant les applications mobiles (MTD)	Logiciel qui détecte en temps réel les attaques contre les applications installées sur les appareils.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée en vue de compromettre les biens ou les activités d'une organisation.

4.3 Références

Numéro	Référence
1	*Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/
2	*Loi sur la protection des renseignements personnels*. https://laws-lois.justice.gc.ca/fra/lois/p-21/index.html
3	Centre canadien pour la cybersécurité, *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)*, juin 2020.
4	Centre canadien pour la cybersécurité, *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)*, septembre 2021.
5	Centre canadien pour la cybersécurité, *Contrôles de cybersécurité de base pour les petites et moyennes organisations*, février 2020.
6	Centre canadien pour la cybersécurité, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111)*, août 2016.
7	Centre canadien pour la cybersécurité, *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*, septembre 2019.
8.	Centre canadien pour la cybersécurité, *Application des mises à jour sur les dispositifs (ITSAP.10.096)*, *mars 2021*.
9	Centre canadien pour la cybersécurité, *Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009)*, octobre 2020.
10	Centre canadien pour la cybersécurité, *Les réseaux privés virtuels (ITSAP.80.101)*, octobre 2019.
11	Centre canadien pour la cybersécurité, *Nettoyage et élimination d'appareils électroniques (ITSAP.40.006)*, octobre 2020.
12	Centre canadien pour la cybersécurité, *Nettoyage des supports de TI (ITSP.40.006)*, juillet 2017.

Numéro	Référence
13	Centre canadien pour la cybersécurité, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau (ITSP.80.022)*, février 2021.
14	Centre canadien pour la cybersécurité, *Considérations de conception relatives au positionnement des services dans les zones (ITSG-38)*, mai 2009.
15	Centre canadien pour la cybersécurité, *Directives de mise en œuvre : Protection du domaine de courrier (ITSP.40.065)*, avril 2020.
16	Cours : Sensibilisation à la protection de la vie privée. https://learning-apprentissage.cse-cst.gc.ca/course/view.php?id=194#section-0
17	Centre canadien pour la cybersécurité, *Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité (ITSM.10.093)*, février 2020.