

# GUIDE DU DIRECTEUR INFORMATIQUE POUR LA SÉCURITÉ MOBILE

Présentation générale et liste de contrôle



## SOMMAIRE

Aujourd'hui, les entreprises et organismes gouvernementaux équipent de plus en plus leurs employés d'appareils (mobiles). Les cadres supérieurs, les entrepreneurs, les fournisseurs et autres employés connectent leurs appareils mobiles aux serveurs de messagerie d'entreprise : les équipes de vente doivent avoir accès aux informations sur les clients et les commandes stockées dans les systèmes CRM de leur entreprise, les techniciens sur site doivent recevoir et interagir avec les informations de service et les responsables ont besoin d'un accès en temps réel aux données essentielles stockées sur le système de renseignement de leur entreprise. Dans de nombreuses entreprises, les utilisateurs cherchent à améliorer leur productivité en accédant à des données d'entreprise via des appareils mobiles.

Dans le même temps, les entreprises et organismes gouvernementaux négligent souvent les risques de sécurité potentiels liés à l'utilisation de ces appareils. Les entreprises doivent appréhender la sécurité des appareils mobiles de la même manière que la sécurité des composants câblés du réseau local (LAN) de l'entreprise, tels que les serveurs, les ordinateurs de bureau ou les ordinateurs portables. Les entreprises peuvent mettre en place une infrastructure de sécurité globale incluant les appareils mobiles en installant des fonctionnalités de sécurité sur ces derniers et en mettant en œuvre les stratégies de sécurité appropriées. Alors que la mise en œuvre de solutions de sécurité est essentielle, le principal problème rencontré par les personnes en charge de cette tâche est l'impact direct des mesures de sécurité sur l'expérience utilisateur. La création d'un environnement sécurisé sur un appareil mobile nécessite souvent une puissance de traitement, un stockage et une autonomie de batterie supplémentaire. Cela signifie que le renforcement de la sécurité d'un appareil nécessite davantage de ressources, ce qui affecte ses performances.

Ce document décrit six aspects clés de la sécurité informatique que les services informatiques doivent prendre en compte pour l'évaluation d'une solution de sécurité.

### **RÉDUCTION DES FAILLES DE SÉCURITÉ DE L'INFORMATIQUE MOBILE**

Les solutions de sécurité mobile permettent de sécuriser les transmissions de données via le cryptage, l'authentification, l'autorisation, le contrôle d'accès et la protection par pare-feu au niveau de l'appareil mobile. Alors que les solutions mobiles continuent de se développer et que le nombre d'appareils en résultant s'accroît, les besoins de gestion et de sécurisation de ces solutions augmentent.

La plupart des sociétés autorisent les employés distants disposant d'ordinateurs portables à se connecter aux systèmes situés derrière le pare-feu de l'entreprise uniquement via une connexion VPN. Toutefois, de nombreux appareils mobiles fonctionnent par défaut sans cette connexion VPN, accédant aux actifs de l'entreprise avec un niveau de sécurité faible ou inexistant.

Les appareils mobiles ont rapidement évolué suite à la commercialisation des téléphones cellulaires et des PDA pour des clients de base. Aujourd'hui, de nombreux appareils sont conçus pour interagir avec les actifs d'entreprise dans une architecture client-serveur. Par conséquent, le principal défi des administrateurs informatiques est de sécuriser un client résidant en dehors du réseau d'entreprise et accédant aux données sensibles stockées sur ce réseau. Lorsque des appareils sans fil accèdent à des données d'entreprise, des failles de sécurité peuvent exister dans les six domaines suivants (devant être pris en compte lors de l'évaluation d'une solution de sécurité mobile) :

## **1. INTÉGRITÉ DU PARE-FEU D'ENTREPRISE**

Les pare-feu d'entreprise sont des composants essentiels pour protéger le réseau d'une entreprise contre les attaques. Étant donné que les appareils mobiles sont utilisés en dehors du pare-feu, les administrateurs informatiques doivent sécuriser les ouvertures de ports et s'assurer que les modifications de configuration du pare-feu pour la prise en charge des connexions des appareils mobiles n'affectent pas les stratégies de sécurité existantes de l'entreprise.

## **2. CONFIDENTIALITÉ, INTÉGRITÉ ET AUTHENTICITÉ DU RÉSEAU**

Les administrateurs doivent s'assurer que les connexions au réseau mobile sont sécurisées pour garantir la confidentialité et l'intégrité des données, ainsi que pour authentifier leur origine. Un e-mail ou tout autre type de donnée est considéré comme confidentiel uniquement si le destinataire est le seul à pouvoir visualiser son contenu. L'intégrité permet à un destinataire de détecter si un message a été modifié par un tiers lors du transit. L'authenticité permet au destinataire d'identifier l'expéditeur et de garantir que ce dernier a bien envoyé le message.

## **3. CONFIDENTIALITÉ DES DONNÉES STOCKÉES SUR LES TERMINAUX**

Les appareils mobiles sont plus exposés à la perte, au vol ou à l'altération que les autres ressources informatiques car ils sont conçus pour être utilisés en dehors des frontières physiques de l'entreprise. Toutes les données présentes sur l'appareil mobile et tous les supports de mémoire amovibles doivent être cryptés afin de protéger les données utilisateur contre tout accès non autorisé en cas de vol de l'appareil.

## **4. PROTECTION CONTRE LES VIRUS ET AUTRES APPLICATIONS MALVEILLANTES**

Les appareils mobiles permettent d'augmenter la productivité des travailleurs mobiles. Toutefois, cette flexibilité induit des risques de sécurité, étant donné que les appareils mobiles constituent une cible potentielle pour les tiers malveillants cherchant à compromettre un appareil ou un réseau d'entreprise. Si des virus, chevaux de Troie, vers et autres applications malveillantes sont chargés sur l'appareil mobile, ils peuvent s'exécuter sans que l'utilisateur s'en aperçoive ou sans qu'il puisse intervenir. Une solution mobile doit réduire les risques liés aux applications malveillantes sur les réseaux d'entreprise et les appareils en empêchant ces dernières de se charger sur l'appareil ou en limitant leur champ d'action.

## **5. PRISE EN CHARGE DES NORMES DE SÉCURITÉ D'ENTREPRISE EXISTANTES**

La plupart des services informatiques ont déjà établi des normes de sécurité d'entreprise. Les déploiements mobiles ne doivent pas supprimer les stratégies existantes, mais prendre en charge ces normes afin d'étendre la sécurité de l'entreprise aux appareils mobiles.

## **6. ÉTABLIR, APPLIQUER ET METTRE À JOUR RÉGULIÈREMENT LES STRATÉGIES DE SÉCURITÉ**

Une sécurité mobile efficace inclut la possibilité d'exiger des mots de passe pour les utilisateurs, de supprimer des données à distance sur les appareils et de verrouiller les appareils à distance. Les administrateurs doivent également être en mesure d'établir, d'appliquer et de mettre à jour des configurations via des stratégies ou des paramètres et de disposer d'un contrôle complet sur l'ensemble des appareils.

## INTÉGRITÉ DU PARE-FEU D'ENTREPRISE

Le pare-feu d'entreprise est un composant essentiel pour protéger un réseau d'entreprise contre les attaques. Étant donné que les appareils mobiles sont utilisés en dehors du pare-feu, les administrateurs doivent sécuriser l'ouverture des ports de ce dernier, ainsi que les connexions entrantes et sortantes pour garantir que seules les adresses IP autorisées communiquent avec les ports activés.

Avec les connexions sortantes, la source et la destination des numéros de ports et des adresses IP sont connues du réseau d'entreprise. Les services informatiques peuvent mettre en place des contrôles internes détaillés de façon appropriée sur ces ports pour sécuriser les connexions sortantes. Lors de la modification de la configuration d'un pare-feu pour la prise en charge d'une solution mobile, le fait d'autoriser uniquement les connexions sortantes permet de réduire le risque d'accès non autorisé, comparé à l'utilisation de connexions entrantes.

## CONNEXIONS AU PARE-FEU ENTRANTES

Les administrateurs utilisent un pare-feu pour contrôler l'accès aux ressources du réseau d'entreprise. Une connexion entrante ouvre un port du pare-feu, permettant la connexion aux actifs de l'entreprise depuis des points d'accès externes, tels que les appareils mobiles, les ordinateurs partagés ou encore les points d'accès publics à Internet. Dans un modèle de connexion sortante, la source de toute tentative de connexion n'est pas connue à l'avance et n'est donc pas approuvée. Ce modèle nécessite donc la mise en œuvre de contrôles pour atténuer les risques potentiels inhérents à ce type de connexion.

Les utilisateurs externes, y compris ceux équipés d'appareils mobiles, établissent des connexions entrantes au réseau d'entreprise. De nombreuses entreprises choisissent une connexion SSL authentifiée par le client pour assurer le contrôle des connexions d'appareils. Ce type de connexion est conçu pour atténuer les risques inhérents aux connexions entrantes sur le réseau d'entreprise. Pour les solutions mobiles autorisant les connexions entrantes, il est recommandé d'augmenter le délai d'expiration de la connexion au pare-feu au delà de la limite acceptable et sécurisée. Cette méthode permet aux utilisateurs de recevoir les e-mails et autres données quasiment en temps réel, tout en préservant la faible autonomie de la batterie de l'appareil (chaque fois qu'une connexion est perdue, puis établie à nouveau, la batterie est déchargée). Toutefois, l'augmentation du délai d'expiration de la connexion accroît le risque d'accès non autorisé sur vos réseaux internes, multipliant alors le risque de faille de sécurité sur le réseau d'entreprise.

## CONNEXIONS AU PARE-FEU SORTANTES

Avec les connexions sortantes, le logiciel situé derrière le pare-feu contacte généralement le centre d'opérations réseau (NOC), qui établit les connexions avec chacun des réseaux mobiles disponibles pour les utilisateurs d'appareils mobiles. Lorsque la connexion est établie depuis un emplacement situé à l'intérieur du réseau d'entreprise, les utilisateurs sont informés de la source et de la destination de la connexion. Ils peuvent alors configurer le pare-feu en fonction de ces deux éléments et définir un port spécifique pour la connexion.

Lors de la connexion à un NOC tiers via une connexion au pare-feu sortante, une solution sécurisée utilise un protocole de sécurité pour déterminer les informations de connexion et autoriser cette dernière : si l'authentification échoue, la connexion n'est pas établie. Toutefois, une fois que la connexion est autorisée et établie, une session de communication persistante avec l'appareil mobile n'est possible que via le NOC. Le pare-feu élimine tout autre trafic entrant depuis un hôte tiers. Étant donné que le pare-feu ne répond pas aux connexions entrantes, il ne répond pas non plus aux paquets malveillants entrants.

L'utilisation d'un NOC pour optimiser l'intégrité du pare-feu fournit plusieurs avantages. Une solution NOC permet aux entreprises de se décharger de la responsabilité de gestion des connexions sortantes avec les opérateurs mobiles. Les entreprises peuvent également utiliser une variété d'opérateurs ou migrer vers de nouveaux opérateurs sans avoir à modifier leur technologie mobile. Une architecture basée sur NOC permet également d'améliorer la sécurité car elle ne nécessite pas que les entreprises ouvrent des ports entrants dans leurs pare-feu. De plus, un NOC fournit une méthode de communication alternative si le système de télécommunication interne des équipes échoue.

## **CONFIDENTIALITÉ, AUTHENTICITÉ ET INTÉGRITÉ SUR LE RÉSEAU D'ENTREPRISE**

Étant donné que le réseau d'entreprise réside en dehors de l'environnement professionnel, les entreprises doivent prendre en compte le fait qu'il n'existe aucune protection des données. Les ressources d'information les plus précieuses d'une entreprise peuvent être transmises via le réseau mobile ; par conséquent, la protection des données d'entreprise en transit est essentielle. L'un des éléments permettant à une entreprise d'évaluer le niveau de sécurité d'une solution mobile est sa capacité à garantir la confidentialité, l'intégrité et l'authenticité des données.

### **CONFIDENTIALITÉ DES DONNÉES EN TRANSIT**

La confidentialité se rapporte au processus interdisant l'accès à des informations à toute personne autre que le destinataire souhaité. Les solutions mobiles assurent généralement la confidentialité des données via le cryptage et l'utilisation d'un tunnel crypté lors de leur transmission.

Le cryptage des données est un codage basé sur une clé secrète. L'accès à cette clé secrète est requis pour le décryptage et la lecture des données. Deux des normes de cryptage des données les plus utilisées aujourd'hui sont AES (Advanced Encryption Standard) et Tripe DES (Triple Data Encryption Standard) ; ces deux méthodes sont des algorithmes standards communément utilisés par les organismes gouvernementaux et financiers. AES est considérée comme l'approche consommant le moins de ressources ; il s'agit en outre de la méthode choisie par le gouvernement des États-Unis, ainsi que par d'autres gouvernements et entreprises exigeants en termes de sécurité dans le monde.

Les tunnels cryptés sont généralement établis à l'aide du protocole SSL. Il s'agit d'un niveau de protection acceptable pour la plupart des entreprises ; il est utilisé notamment dans de nombreuses applications et banques en ligne.

Toutefois, l'utilisation d'une connexion protégée par SSL nécessite une connexion entrante au pare-feu. De plus, pour bénéficier d'une méthode de type « push » permettant l'envoi des informations quasiment en temps réel, la connexion doit constamment être coupée puis rétablie. Cette méthode peut consommer une grande quantité de ressources et affecter l'autonomie de la batterie des appareils mobiles.

## **AUTHENTICITÉ DES DONNÉES**

L'authenticité permet au destinataire d'identifier l'expéditeur et de garantir que ce dernier a bien envoyé le message. Afin d'empêcher tout utilisateur non autorisé d'usurper l'identité de l'appareil, ce dernier doit s'authentifier auprès du réseau et des systèmes de l'entreprise. De la même manière, le serveur de l'entreprise doit s'authentifier auprès de l'appareil pour empêcher des utilisateurs non autorisés d'usurper l'identité du serveur.

L'authentification peut être effectuée via l'utilisation d'un système de clé cryptographique partagé. Un système de clé partagé nécessite qu'un composant d'authentification (tel qu'un serveur) et qu'un composant de requête (tel qu'un appareil mobile) disposent d'une clé secrète. Lors d'une tentative de connexion, le serveur envoie la clé secrète et l'appareil mobile l'accepte ou la rejette. Avant de crypter les données, l'appareil mobile vérifie la correspondance des clés auprès du système principal. Pour que la transmission de données s'effectue correctement, les clés du serveur et de l'appareil doivent correspondre. Si les clés ne correspondent pas, le serveur et l'appareil ne peuvent pas s'échanger de données.

## **INTÉGRITÉ DES DONNÉES**

L'intégrité des données se rapporte à leur validité (ex. si les données ont été modifiées lors du transit). La fiabilité des données peut être déterminée via divers mécanismes de prévention et de détection. Avec des données cryptées, un message d'échec s'affiche automatiquement si le format du message n'est pas reconnu par le processus de décryptage. De la même manière, un échec se produit si le message reçu a été crypté à l'aide d'une clé de cryptage erronée ou si les données ont été modifiées lors du transit. La solution sans fil en question doit supprimer automatiquement les paquets de données modifiés pour garantir que les données malveillantes ou erronées n'ont pas remplacé les données valides.

## CONFIDENTIALITÉ DES DONNÉES SUR LES TERMINAUX

Les informations d'entreprise stockées sur un appareil mobile doivent être aussi sécurisées que celles stockées sur un réseau d'entreprise. Pour certaines entreprises, l'accès à des données d'entreprise par des tiers non autorisés ne constitue un problème grave. Toutefois, l'accès non autorisé à des appareils peut être synonyme d'usurpation d'identité ou d'espionnage industriel. Pour les entreprises publiques ou les organismes financiers, la perte d'un appareil peut se traduire par la violation de la loi Sarbanes-Oxley ou de la loi Gramm-Leach-Bliley, lesquels imposent un contrôle strict sur la divulgation des informations financières. Pour les médecins et les organismes sanitaires, la perte des données d'un patient peut compromettre sa confidentialité, laquelle est protégée par la loi HIPAA (Health Insurance Portability and Accountability Act).

Les données stockées sur un appareil peuvent être sécurisées en contrôlant l'accès à l'appareil lui-même de différentes manières. Cela inclut l'utilisation de mots de passe et/ou de dispositifs d'authentification à deux facteurs, le cryptage des données stockées sur l'appareil et sur des supports amovibles et la sécurisation des accès non physiques au terminal, par exemple via la technologie Bluetooth®.

### AUTHENTIFICATION UTILISATEUR

Les informations stockées sur le terminal sont protégées de différentes manières ; la plus connue est l'utilisation d'un mot de passe individuel. Le but du mot de passe est de garantir que seul le propriétaire du terminal a accès aux données et aux fonctionnalités qu'il contient. Les stratégies de sécurité mobile doivent imposer l'utilisation de mots de passe privés. Idéalement, la syntaxe du mot de passe doit être applicable et son expiration doit être planifiée afin que les utilisateurs en changent régulièrement.

Les entreprises plus exigeantes en matière de sécurité peuvent demander que les appareils mobiles d'entreprise prennent en charge l'authentification à plusieurs facteurs, via l'utilisation de cartes à puce ou autres dispositifs similaires. L'authentification à deux facteurs améliore la sécurité en garantissant que l'accès au terminal nécessite non seulement un élément connu de l'utilisateur (le mot de passe du terminal), mais également un élément qu'il possède (par exemple une carte à puce) ou encore qui lui est propre (par exemple, une empreinte digitale).

### SÉCURITÉ DES DONNÉES STOCKÉES SUR DES TERMINAUX MOBILES

Selon le groupe Gartner, plus de 250 000 PDA ont été perdus pour la seule année 2001. La perte d'appareils mobiles présente de nombreuses menaces potentielles, y compris l'accès non autorisé aux :

- données et fonctionnalités de l'appareil
- serveurs et applications de l'entreprise

De nombreuses solutions actuelles permettent de supprimer les données de l'appareil à distance. Toutefois, il existe souvent un laps de temps entre le moment où l'utilisateur perd l'appareil et le moment où il contacte le service informatique pour signaler la perte. Un utilisateur non autorisé pourrait alors accéder à l'appareil et en extraire les données pendant ce laps de temps. Pour éviter cela, une solution sans fil doit permettre le cryptage en temps réel des données de l'appareil.

## SÉCURITÉ DES DONNÉES AMOVIBLES SUR DES APPAREILS MOBILES

Lorsque des données sont stockées sur un appareil mobile, les utilisateurs peuvent souhaiter les transférer sur un appareil non professionnel via des supports amovibles. Pour certaines entreprises, cela est parfaitement acceptable, pourvu que les employés prennent des précautions nécessaires lorsqu'ils partagent des données avec d'autres personnes. Pour d'autres organismes—généralement gouvernementaux, juridiques, sanitaires, pharmaceutiques et financiers—ce n'est pas acceptable en raison des enjeux juridiques inhérents aux données juridiques sensibles. De plus, les entreprises interdisent parfois l'utilisation de supports amovibles car ils présentent un risque d'introduction de virus sur l'appareil et le réseau d'entreprise.

Si une entreprise autorise l'utilisation de ces supports, la solution mobile doit fournir une option de cryptage des données et de définition de stratégie de sécurité mobile afin de spécifier les groupes d'utilisateurs autorisés à utiliser ce type de support.

## SÉCURITÉ DES CONNEXIONS BLUETOOTH SUR DES APPAREILS MOBILES

Bluetooth est une technologie mobile permettant aux appareils compatibles Bluetooth d'établir une connexion sans fil avec d'autres appareils compatibles Bluetooth situés dans une portée définie. Pour garantir la sécurité, chaque fois qu'un utilisateur tente de se connecter via la technologie Bluetooth, l'appareil doit avertir l'utilisateur et lui demander de confirmer qu'il se connecte à un appareil approuvé. De plus, l'ensemble des données transmises entre les deux appareils mobiles connectés doit être crypté. Cela permet d'éviter que des pirates se connectent et téléchargent des données à l'insu de l'utilisateur et d'empêcher le « reniflage » du trafic lors de la transmission.

Les appareils compatibles Bluetooth peuvent également être la cible d'attaques par refus de service (DoS). Les attaques DoS bombardent généralement l'appareil de requêtes, ce qui provoque son blocage ou le déchargement de la batterie. De plus, les vers de téléphones portables tels que Cabir peuvent utiliser la technologie Bluetooth pour se propager.

Les profils Bluetooth spécifient la manière dont les applications installées sur des appareils compatibles Bluetooth se connectent et interagissent. Les stratégies de sécurité sont souvent nécessaires pour contrôler les appareils qui se connectent à l'aide de la technologie Bluetooth et les profils Bluetooth qui sont disponibles sur ces appareils. Certaines entreprises autorisent les casques Bluetooth pour la voix, mais pas l'accès Bluetooth à des données depuis des ordinateurs portables et autres appareils mobiles. Dans d'autres cas, seuls certains employés sont autorisés à utiliser la technologie Bluetooth pour se connecter à des appareils spécifiques compatibles Bluetooth tels que les lecteurs de carte à puce, les scanners de code à barres ou encore les lecteurs de carte de crédit.

## PROTECTION CONTRE LES VIRUS ET AUTRES APPLICATIONS MALVEILLANTES

De la même manière qu'ils attaquent et prolifèrent sur les ordinateurs de bureau et les ordinateurs portables, les virus, chevaux de Troie, vers et logiciels espions (regroupés sous le nom d'applications malveillantes) peuvent se charger sur des appareils mobiles et s'exécuter sans que l'utilisateur en ait connaissance ou puisse intervenir. Si une application malveillante réussit à s'installer et à s'exécuter sur un appareil mobile, elle peut utiliser toute la mémoire disponible et sérieusement altérer les performances de l'appareil. Certaines applications malveillantes plus dangereuses peuvent se propager via le réseau mobile, en contournant certains systèmes de sécurité du réseau d'entreprise et potentiellement altérer d'autres composants du réseau.

### PROTECTION CONTRE LES APPLICATIONS MALVEILLANTES

La méthode la plus communément utilisée pour empêcher la transmission et la propagation d'applications malveillantes sur des ordinateurs est l'installation d'un logiciel d'analyse anti-virus en temps réel. Ce type de logiciel est conçu pour détecter et isoler les applications malveillantes.

Alors que les ordinateurs de bureau disposent généralement des ressources suffisantes pour prendre en charge un logiciel anti-virus, les appareils mobiles sont limités en mémoire, puissance de traitement et autonomie de batterie. La détection des applications malveillantes nécessite une base de données locale volumineuse et régulièrement mise à jour ou un accès permanent à une base de donnée en ligne. Par conséquent l'appareil télécharge de nouvelles données et exécute des processus en permanence. Ces tâches peuvent avoir un impact significatif sur la durée de vie de la batterie, augmenter le trafic du réseau et ralentir les autres opérations de l'appareil.

Une autre méthode permettant de protéger les appareils mobiles des applications malveillantes est d'empêcher proactivement ces derniers de charger et d'exécuter du code non autorisé. Cette approche permet aux administrateurs système d'effectuer les opérations suivantes :

- spécifier exactement quelles applications (applications approuvées ou approuvées par l'entreprise uniquement) sont autorisées sur l'appareil
- empêcher les applications tierces d'utiliser un stockage persistant sur l'appareil
- déterminer les ressources (telle que les e-mails, téléphones, clé de cryptage et magasins de certificats) auxquelles peuvent accéder les applications tierces sur l'appareil
- restreindre les types de connexions (telles que les connexions réseau à l'intérieur du pare-feu) pouvant être établies par les applications tierces s'exécutant sur l'appareil
- empêcher toutes les applications tierces de se charger et de s'exécuter sur l'appareil

## **VISUALISATION DES PIÈCES JOINTES ET APPLICATIONS MALVEILLANTES**

Les pièces jointes ouvertes par les utilisateurs sur l'appareil peuvent contenir des virus et autres applications malveillantes. Les solutions proactives utilisant un service de pièces jointes emploient un rendu plutôt qu'une prise en charge des fichiers natifs. Dans ce scénario, les utilisateurs peuvent toujours afficher et manipuler les données, mais le fichier n'est pas ouvert de façon native sur l'appareil. Cette méthode permet d'éviter que les applications malveillantes n'accèdent aux données stockées sur l'appareil.

Si une solution mobile utilise un serveur distant protégé pour effectuer des opérations liées aux pièces jointes, le serveur de traitement des pièces jointes est toujours vulnérable aux attaques de virus et autres applications malveillantes. Toutefois, il est plus simple pour le service informatique d'installer un logiciel sur ce serveur plutôt que sur l'appareil mobile pour éviter ce type d'attaque. De plus, le serveur n'est pas soumis aux contraintes de puissance de traitement et d'autonomie de la batterie. Si nécessaire, le serveur de traitement des pièces jointes peut être isolé du réseau d'entreprise étant donné qu'il réside à l'intérieur de l'infrastructure de l'entreprise.

## PRISE EN CHARGE DES NORMES DE SÉCURITÉ D'ENTREPRISE EXISTANTES

La plupart des entreprises informatiques ont déjà établi des normes de sécurité d'entreprise et la solution mobile doit pouvoir les prendre en charge. Le Tableau 1 répertorie les normes de sécurité les plus utilisées aujourd'hui et décrit comment elles peuvent être intégrées dans une solution mobile.

Normes de sécurité	Utilisation mobile
Lecteurs de cartes à puce	Les cartes à puce peuvent être utilisées pour l'authentification à deux facteurs, la messagerie sécurisée et la navigation Web sécurisée.
Prise en charge de l'authentification RSA SecurID	Deux types de prise en charge RSA SecurID sont actuellement disponibles : 1. Les utilisateurs peuvent accéder à une application sur l'appareil mobile qui génère des numéros de jeton, puis utiliser leur ordinateur portable ou VPN pour accéder aux systèmes d'entreprise. 2. L'appareil mobile communique avec les serveurs d'entreprise RSA pour sécuriser la connexion avant de transmettre les données. Par exemple, lorsqu'un utilisateur navigue vers un site ou une application nécessitant une authentification sur l'appareil mobile, ce dernier invite l'utilisateur à entrer son nom d'utilisateur et son mot de passe de jeton.
Prise en charge du cryptage entre l'expéditeur et le destinataire	Les normes telles que le cryptage natif S/MIME, PGP et Lotus Notes permettent la confidentialité, l'intégrité et l'authentification entre l'expéditeur et le destinataire.
HTTPS, SSL/TLS	Une connexion par protocole HTTP (Hypertext Transfer Protocol) peut être établie via SSL/TLS (Secure Socket Layer/Transport Layer Security) pour fournir une authentification et une sécurité supplémentaires si un appareil mobile accède à un serveur sur Internet. De nombreuses transactions sécurisées via Internet utilisent le protocole HTTPS (Hypertext Transfer Protocol Secure).
WTLS	Le protocole WTLS (Wireless Transport Layer Security) est conçu pour fournir une couche de sécurité supplémentaire lors de la connexion à une passerelle WAP (Wireless Application Protocol). Le protocole WTLS nécessite une passerelle WAP pour fournir un accès WAP standard à Internet. Pour utiliser une passerelle WAP, une entreprise doit travailler avec l'opérateur réseau ou le fournisseur de services.

# ÉTABLIR, APPLIQUER ET METTRE À JOUR RÉGULIÈREMENT LES STRATÉGIES DE SÉCURITÉ

## STRATÉGIES DE SÉCURITÉ CONTRÔLÉES PAR LES ADMINISTRATEURS INFORMATIQUES

La plupart des entreprises mettent en œuvre les mesures de sécurité appropriées pour garantir que seuls les appareils autorisés (câblés ou mobiles) sont connectés au réseau. Ces mesures incluent les stratégies standard relatives à l'authentification utilisateur, la sécurité réseau et la protection contre les virus.

Lors de l'extension des stratégies de sécurité d'une entreprise à des appareils mobiles, les administrateurs informatiques doivent être en mesure d'imposer des mots de passe pour les utilisateurs d'appareils mobiles et d'en supprimer les données à distance. Les administrateurs informatiques doivent pouvoir établir, appliquer et mettre à jour les configurations des appareils mobiles via des stratégies ou des paramètres permettant un contrôle complet sur l'ensemble de ces derniers. Pour contrôler la manière dont les utilisateurs interagissent avec l'environnement d'entreprise, les administrateurs ont besoin d'un point de gestion des appareils mobiles unique, qui doit résider derrière le pare-feu de l'entreprise. Cela signifie que les administrateurs, plutôt que les utilisateurs d'appareils mobiles, doivent déterminer la méthode de protection des données.

Dans les premières années suivant l'émergence de l'accès aux données mobiles, les stratégies de sécurité mobile de première génération étaient étendues et couvraient un grand nombre d'aspects, y compris la confidentialité et l'utilisation appropriée de l'appareil. Généralement, une stratégie de sécurité unique couvrait plusieurs aspects. Toutefois, alors que l'accès mobile aux informations devient de plus en plus répandu et que les entreprises sont de plus en plus dépendantes de la mobilité, une série limitée de stratégies de sécurité étendues ne suffit plus à répondre aux besoins de la plupart d'entre elles. En revanche, un ensemble robuste de stratégies de sécurité fournit un contrôle optimal de tous les aspects de la solution mobile.

Les exemples de stratégies suivants définissent les niveaux de sécurité et les fonctionnalités acceptables pour les appareils mobiles d'entreprise.

### 1. Définir une authentification utilisateur acceptable :

- forcer une authentification utilisateur sur l'appareil à l'aide d'un mot de passe de sécurité ;
- configurer les fonctionnalités telles que l'expiration, les limites de tentatives de saisie, la longueur et la force du mot de passe ;
- forcer et définir les mots de passe et phrases de passe acceptables sur les appareils mobiles de votre entreprise.

### 2. Définir des mesures protégeant les appareils mobiles contre toute utilisation non autorisée :

- restreindre les connexions autorisées sur les appareils mobiles ;
- utiliser le cryptage des données en transit entre l'expéditeur et le destinataire de données mobiles ;
- crypter les supports amovibles utilisés avec des appareils mobiles ;
- crypter les données stockées sur des appareils mobiles.

**3. Définir un cryptage acceptable pour les données stockées sur des appareils mobiles :**

- imposer une norme spécifique pour le niveau de cryptage.

**4. Définir des mesures de protection contre les virus et les utilisateurs malveillants :**

- empêcher les appareils mobiles de télécharger des applications tierces sur le réseau mobile ;
- spécifier si les applications, y compris les applications tierces installées sur l'appareil mobile, peuvent établir des types de connexion spécifiques.

Les administrateurs informatiques doivent être en mesure de déployer des stratégies de groupe reflétant les besoins des différents utilisateurs et équipes présents dans l'entreprise.

Toutes les configurations de stratégies doivent être synchronisées et attribuées à l'appareil à l'aide d'une connexion mobile.

Une fois qu'un administrateur informatique a défini une stratégie d'appareil mobile, les utilisateurs ne doivent pas pouvoir intervenir ni empêcher son application. L'administrateur doit également pouvoir effectuer un audit pour vérifier que la stratégie de sécurité mobile a bien été appliquée sur l'appareil mobile.

## EXEMPLE DE LISTE DE CONTRÔLE DE SÉCURITÉ

La liste de contrôle ci-dessous répertorie les aspects clés à prendre en compte lors de l'évaluation d'une solution mobile. La colonne « Inclus » peut être utilisée pour indiquer que la fonctionnalité est disponible dans la solution et la colonne « Ajout » indique si des composants supplémentaires doivent être achetés pour bénéficier de la fonctionnalité requise.

Fonctionnalités de la solution mobile	Option A de la solution mobile		Option B de la solution mobile	
	Inclus	Ajout	Inclus	Ajout
<b>Sécurité des données mobiles</b>				
Utilise le cryptage pour protéger les données en transit (ex. AES-256, AES-192, AES-128, Triple DES, etc.)				
Utilise une connexion sortante pour l'authentification du serveur				
Possibilité de désactiver la technologie Bluetooth				
Possibilité de désactiver les messages SMS et MMS				
Prise en charge du cryptage d'e-mail IBM® Lotus Notes®				
<b>Sécurité des données de l'appareil</b>				
Cryptage des données de l'appareil quasiment en temps réel				
Suppression des données en option lors du nettoyage de l'appareil				
Possibilité de désactiver la visualisation des pièces jointes				
Possibilité de forcer le cryptage des données sur les cartes de stockage externes				

Fonctionnalités de la solution mobile	Option A de la solution mobile		Option B de la solution mobile	
	Inclus	Ajout	Inclus	Ajout
<b>Authentification utilisateur</b>				
Possibilité de forcer l'authentification par mot de passe sur l'appareil				
Possibilité d'appliquer des mots de passe forts sur l'appareil				
Possibilité d'appliquer une liste de mots de passe interdits				
Possibilité de forcer l'appareil à se verrouiller après un certain délai d'inactivité				
<b>Contrôle à distance</b>				
Possibilité de modifier le mot de passe de l'appareil à distance				
Possibilité de nettoyer l'appareil à distance				
<b>Contrôle des applications</b>				
Possibilité de forcer l'installation des applications importantes				
Possibilité de désactiver le téléchargement de toutes les applications tierces				
Possibilité de désactiver une application particulière sur tous les appareils				
Options de sécurité améliorées				
Prise en charge du cryptage S/MIME				
Prise en charge du cryptage PGP				
Prise en charge de l'authentification à deux facteurs				

## SYNTHÈSE

Alors que de plus en plus d'entreprises utilisent des appareils mobiles, les sociétés et organismes gouvernementaux doivent prendre les mesures nécessaires pour garantir la sécurité de leurs e-mails et données d'application. Via l'utilisation d'appareils mobiles, les données sont de plus en plus stockées en dehors du réseau d'entreprise, c'est à dire sur des appareils mobiles situés en dehors des frontières physiques de l'entreprise. Les appareils mobiles sont potentiellement vulnérables aux attaques par immixtion, attaques DoS, menaces d'applications malveillantes et autres failles de données. Alors que la perte de données ne constitue pas une faille de sécurité grave pour certaines entreprises, cela peut engendrer des risques juridiques et financiers dans de nombreux cas.

Une solution mobile efficace doit être conçue pour la sécurité au niveau de l'entreprise et fournir une architecture spécifiquement adaptée aux différents aspects de la mobilité. Dans de nombreux cas, les solutions fonctionnant dans un environnement de bureau ne peuvent pas être utilisées pour l'informatique mobile, étant donné les contraintes de traitement, de mémoire et d'autonomie de batterie des appareils mobiles. Le pare-feu d'entreprise est un composant essentiel pour protéger les données d'une entreprise contre les attaques et utilisations malveillantes. La connexion au réseau mobile doit être sécurisée pour garantir la confidentialité, l'authenticité et l'intégrité des données transmises. Enfin, les appareils mobiles doivent être protégés contre la perte et l'altération des données ou encore l'infection par des applications malveillantes.

## RESSOURCES CONNEXES

Pour en savoir plus sur la manière dont BlackBerry® Enterprise Solution aide les entreprises à développer, planifier et mettre en œuvre leurs initiatives de sécurité mobile, rendez-vous sur les sites :

[www.blackberry.com/security](http://www.blackberry.com/security)

[www.blackberry.com/go/getthefacts](http://www.blackberry.com/go/getthefacts)

Ressources	Informations
Sécurité de la solution BlackBerry Enterprise Solution	<ul style="list-style-type: none"> <li>• Décrit les fonctionnalités de sécurité de la solution BlackBerry Enterprise</li> <li>• Fournit une présentation de l'architecture de sécurité BlackBerry®</li> </ul>
Glossaire d'acronymes de sécurité BlackBerry Enterprise Solution	<ul style="list-style-type: none"> <li>• Définit les acronymes utilisés dans ce document et d'autres documents de sécurité</li> </ul>
Guide d'administration de BlackBerry Signing Authority Tool	<ul style="list-style-type: none"> <li>• La mise en œuvre de la cryptographie à clé publique de BlackBerry Signing Authority Tool</li> </ul>
Livre blanc sur la sécurité du lecteur BlackBerry Smart Card Reader	<ul style="list-style-type: none"> <li>• Couplage sécurisé entre le terminal BlackBerry et le lecteur BlackBerry® Smart Card Reader</li> <li>• Protocole d'établissement de clés initial</li> <li>• Protocole d'établissement de clés de connexion</li> </ul>
Guide de référence sur les stratégies	<ul style="list-style-type: none"> <li>• Utilisation des stratégies informatiques BlackBerry Enterprise Server</li> </ul>
Livre blanc sur PGP Support Package	<ul style="list-style-type: none"> <li>• Cryptage et sécurité PGP</li> <li>• Utilisation du serveur PGP Universal pour stocker et gérer les clés PGP</li> <li>• Recherche et validation des clés PGP</li> <li>• Envoi et réception de messages PGP</li> </ul>
Supplément du guide de l'utilisateur de PGP Support Package	<ul style="list-style-type: none"> <li>• Installation de PGP Support Package</li> <li>• Gestion des clés PGP sur le terminal BlackBerry</li> <li>• Configuration des options PGP pour la signature numérique et le cryptage des messages</li> </ul>
Livre blanc sur S/MIME Support Package	<ul style="list-style-type: none"> <li>• Sécurité et cryptage S/MIME</li> <li>• Gestion des certificats S/MIME sur le terminal BlackBerry et sur les ordinateurs de bureau</li> </ul>
Supplément du guide de l'utilisateur de S/MIME Support Package	<ul style="list-style-type: none"> <li>• Installation de S/MIME Support Package</li> <li>• Gestion des certificats sur le terminal BlackBerry et sur les ordinateurs de bureau</li> <li>• Configuration des options S/MIME pour la signature numérique et le cryptage des messages</li> <li>• Envoi et réception de messages S/MIME</li> </ul>
Sécurité des terminaux BlackBerry avec la technologie sans fil Bluetooth	<ul style="list-style-type: none"> <li>• Présentation de la technologie sans fil Bluetooth</li> <li>• Utilisation et protection des terminaux BlackBerry compatibles Bluetooth</li> <li>• Risques liés à l'utilisation de la technologie sans fil Bluetooth sur des appareils mobiles</li> </ul>
Présentation technique de l'activation Entreprise mobile BlackBerry	<ul style="list-style-type: none"> <li>• Processus d'activation Entreprise mobile</li> <li>• Génération de clé de cryptage principale mobile</li> <li>• Protocole d'établissement de clés initial</li> <li>• Protocole de rotation des clés</li> </ul>
Sécurité de réseau local (LAN) mobile	<ul style="list-style-type: none"> <li>• Options de sécurité pour la mise en œuvre d'un terminal BlackBerry pris en charge sur un WLAN</li> </ul>

\*Vérifiez auprès de votre fournisseur de services la disponibilité, les accords d'itinérance et les plans de service. Certaines fonctionnalités décrites dans ce document peuvent nécessiter une version minimale des logiciels BlackBerry Enterprise Server, BlackBerry Desktop Software et/ou BlackBerry Device Software. Peut nécessiter le développement d'applications supplémentaires. Avant de vous abonner ou d'implémenter des produits ou services tiers, il est de votre responsabilité de vérifier que le fournisseur de services que vous utilisez prend en charge toutes les fonctions des produits et services tiers. L'installation et l'utilisation de produits et services tiers avec des produits et services RIM peuvent nécessiter un ou plusieurs brevets, marques de commerce ou licences de copyright à des fins de protection de la propriété intellectuelle. Vous êtes seul responsable de l'identification et de l'acquisition des dites licences tierces requises le cas échéant. Dans la mesure où lesdites licences de propriété intellectuelle s'avèrent nécessaires, RIM vous recommande expressément de ne pas installer ni utiliser les produits et services concernés tant que l'intégralité des dites licences requises n'ont pas été acquises par vous, directement ou indirectement. Votre utilisation de logiciels tiers sera régie le cas échéant par les dispositions de licences logicielles distinctes au titre des produits ou services tiers y afférents, sous réserve de votre acceptation des dites dispositions. Les produits ou services tiers fournis avec les produits et services RIM sont fournis «en l'état». RIM rejette toute déclaration, garantie et responsabilité de quelque nature que ce soit en cas de dommages concernant les produits et services tiers, quand bien même RIM aurait été explicitement prévenu de l'éventualité de tels dommages ou est en mesure de les anticiper.

© 2006 Research In Motion Limited. Tous droits réservés. Research In Motion, le logo RIM, BlackBerry, ainsi que la conception BlackBerry et des flux de données sont déposés auprès du Patent and Trademark Office des États-Unis, et peuvent être en attente ou déposées dans d'autres pays. Ces marques, images et symboles sont la propriété de Research In Motion Limited.

Tous les autres noms de produit, marques, noms de société et marques déposées sont la propriété de leurs détenteurs respectifs.

Le terminal mobile et/ou les logiciels associés sont protégés par copyright ainsi que par des accords internationaux et différents brevets, y compris un ou plusieurs des brevets suivants déposés aux États-Unis : 6 278 442 ; 6 271 605 ; 6 219 694 ; 6 075 470 ; 6 073 318 ; D 445 428 ; D 433 460 ; D 416 256. D'autres brevets sont enregistrés ou en attente dans plusieurs pays du monde. Visitez le site [www.rim.net/patents.shtml](http://www.rim.net/patents.shtml) pour obtenir la liste actuelle des brevets applicables.

Ce document vous est fourni « en l'état » et Research In Motion Limited (RIM) dégage toute responsabilité en cas d'erreurs typographiques, techniques ou d'une autre nature pouvant être contenues dans les présentes. RIM se réserve le droit de modifier périodiquement les informations contenues dans le présent document ; toutefois, RIM n'est en aucun cas tenu de vous fournir les modifications, mises à jour, améliorations ou autres compléments apportés au présent document au moment opportun. RIM N'OFFRE AUCUNE REPRÉSENTATION, GARANTIE, CONDITION OU CONVENTION, EXPRESSE OU TACITE (Y COMPRIS, SANS S'Y LIMITER, DES GARANTIES OU DES CONDITIONS EXPRESSES OU TACITES D'ADÉQUATION À UN BUT PARTICULIER, DE NON INFRACTION, DE COMMERCIALISATION, DE DURABILITÉ, DE TITRE OU RELATIVES À LA PERFORMANCE OU LA NON PERFORMANCE DES LOGICIELS RÉFÉRENCÉS DANS CETTE DOCUMENTATION, OU À LA PERFORMANCE DES SERVICES RÉFÉRENCÉS DANS CETTE DOCUMENTATION). RIM, SES FILIALES ET LEURS DIRIGEANTS, MEMBRES DE LA DIRECTION, EMPLOYÉS OU CONSULTANTS, NE PEUVENT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLES À VOTRE ENCONTRE DES ÉVENTUELS DOMMAGES DIRECTS, ÉCONOMIQUES, COMMERCIAUX, PARTICULIERS, SECONDAIRES, ACCESSOIRES, EXEMPLAIRES, INDIRECTS OU DÉCOULANT DE L'UTILISATION DE LA PRÉSENTE DOCUMENTATION, Y COMPRIS LES PERTES DE BÉNÉFICES OU DE DONNÉES, LES DOMMAGES OCCASIONNÉS PAR DES RETARDS, LE MANQUE À GAGNER OU L'IMPOSSIBILITÉ DE RÉALISER LES ÉCONOMIES ATTENDUES, MÊME SI RIM A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

Le présent document peut contenir des références à des sources d'informations et / ou des sites tiers (« Informations tierces »). RIM ne contrôle pas ces Informations tierces, et ne serait donc être tenu responsable de leur contenu, de leur exactitude, de leur respect des droits d'auteur, de leur légalité, de leur décence, de leurs liens ou de tout autre aspect quel qu'il soit. L'inclusion d'informations tierces dans le présent document ne saurait être considérée comme une approbation par RIM desdites tierces parties de quelque manière que ce soit. Toute transaction avec des tiers, incluant notamment le respect des licences applicables, ainsi que leurs termes et conditions, n'impliquent que vous-même et le tiers. La responsabilité de RIM ne pourra en aucun cas être engagée dans ces relations.