MobileIron

Bonnes pratiques pour le cloud : liste de contrôle applicable à la sécurité des terminaux

Cette liste de contrôle en 10 points présente les bonnes pratiques à respecter si vous voulez mettre en place une architecture de sécurité capable de protéger les données cloud au niveau des terminaux. Tandis que les employés recourent à un éventail croissant de services cloud professionnels via leurs applications mobiles, nous assistons, depuis ces dix dernières années, à un bouleversement de l'architecture informatique en entreprise. L'approche sécuritaire traditionnelle du périmètre réseau et du verrouillage des terminaux n'est plus adaptée aux méthodes de travail actuelles.

Généralement, les fournisseurs de services cloud sécurisent leurs centres de données dans le cadre d'une approche complète et structurée, réduisant ainsi le risque de violation. Une fois que ces données se trouvent sur l'appareil mobile d'un utilisateur final, toutefois, elles peuvent être facilement compromises ou perdues en l'absence de contrôles de sécurité appropriés.

Nombreuses sont les organisations qui devront procéder à des audits de sécurité internes ou externes pour évaluer le niveau de protection de leurs données, tant dans le cloud que sur les terminaux. Deux chartes sont alors susceptibles de régir les critères de ces audits : le cadre américain « NIST Cybersecurity Framework » (www.nist.gov/cyberframework) et le « Règlement général sur la protection des données » (RGPD - www.eugdpr.org) de l'Union européenne.

Plus qu'un cadre exhaustif, cette liste de contrôle fournit un point de départ. Il revient à chaque organisation d'effectuer son analyse et de définir ses contrôles en fonction de son environnement propre. Néanmoins, les niveaux de risques encourus seront d'autant plus importants que le déploiement choisi s'écartera de cette liste de contrôle.

MobileIron

info@mobileiron.com

www.mobileiron.com

Liste de contrôle pour audit de sécurité

1. Chiffrer les appareils et les protéger par mot de passe

Il est fréquent de perdre un appareil mobile. En chiffrant ce dernier et en y appliquant des mots de passe, il est possible d'empêcher toute personne qui entrerait en sa possession d'accéder facilement à son contenu. En fonction du niveau de risque, le chiffrement est une obligation en vertu de la loi HIPAA (Health Insurance Portability and Accountability Act) américaine et du RGPD. Si l'appareil est compatible avec cette technologie, la biométrie, telle que la reconnaissance faciale ou par empreinte digitale, permet de compliquer tout accès indésirable aux données.

2. Empêcher le partage de données entre les applications d'entreprise et les applications personnelles

Les systèmes d'exploitation mobiles autorisent le partage de données entre les différentes applications installées sur l'appareil. Les utilisateurs finaux peuvent, par exemple, recevoir des documents via leur messagerie professionnelle et les ouvrir dans d'autres applications, telles que des visionneuses de PDF ou des éditeurs de documents. Or, ces applications stockent ou transmettent ces documents selon un processus qui peut échapper au contrôle du service informatique. Ce procédé entraîne souvent la perte de données. Aucune application d'entreprise ne devrait pouvoir exporter des données vers une application personnelle.

3. Supprimer d'office les données d'entreprise stockées sur les appareils dont la sécurité a été compromise

Les appareils sont souvent en défaut de conformité avec les règles de sécurité. En cause, des problèmes de jailbreaking, d'accès en mode root, de logiciels malveillants ou de firmware obsolète, par exemple. L'automatisation des mesures correctives devrait être de mise afin qu'elles soient appliquées sans l'intervention manuelle du service informatique. En cas d'atteinte grave à la conformité, les données d'entreprise stockées sur l'appareil doivent pouvoir être supprimées automatiquement. Des actions de conformité en boucle fermée, de la détection à la correction, sont primordiales pour réduire les risques. Plus les données d'entreprise restent longtemps sur un appareil piraté, et plus le risque d'une violation est élevé. Afin de préserver la confidentialité, le service informatique doit pouvoir les supprimer de l'appareil tout en conservant les données personnelles.

4. Autoriser le tunneling des données d'entreprise sans toucher aux données personnelles

Ce point est similaire au point n° 3 de la liste de contrôle, mais, au lieu de préconiser la séparation des données professionnelles et personnelles sur l'appareil, il l'instaure sur le réseau. Un VPN au niveau de l'appareil envoie les données des applications, tant professionnelles que personnelles, sur le réseau d'entreprise. Un VPN par application, en revanche, peut être configuré pour n'envoyer sur ce dernier que le trafic issu des applications professionnelles. Ce trafic est alors protégé, de même que la confidentialité des données de l'utilisateur sur les réseaux sociaux ou toute autre communication privée.

5. Empêcher les appareils non autorisés d'accéder aux services cloud professionnels

La plupart du temps, les organisations exécutent des services cloud professionnels de plusieurs fournisseurs, par exemple, une suite d'outils de productivité Microsoft et une solution CRM Salesforce. Tout appareil non autorisé qui accéderait à l'un de ces services est en mesure d'en récupérer les données, lesquelles échappent alors au contrôle du service informatique. Ce problème se pose souvent lorsque, pour des questions de commodité, un utilisateur télécharge une application professionnelle sur un appareil personnel. À moins que le service informatique ne soit à même de supprimer des applications et de contrôler le partage de données sur ces appareils, aucune donnée professionnelle ne devrait y être stockée. Ces contrôles de sécurité doivent impérativement être appliqués dans tous les services cloud professionnels, indépendamment du fournisseur. La seule sécurisation d'Office 365 est insuffisante. Ces contrôles sont conformes à la fois au RGPD et au cadre « NIST Cybersecurity Framework Category DE.CM-7 » (Surveillance des connexions, accès, appareils et logiciels non autorisés), car ils bloquent l'accès des appareils non autorisés aux données d'entreprise.

6. Empêcher les applications non autorisées d'accéder aux services cloud professionnels

La protection des données passe par la sécurisation des appareils et des logiciels accédant aux services cloud. Si les premiers sont sécurisés, mais pas les seconds, des données seront perdues. Le téléchargement d'applications professionnelles directement depuis des services grand public, tels que l'App Store d'Apple ou Google Play, au lieu du magasin d'applications interne à l'entreprise, en est un bon exemple. Même si l'application paraît identique pour l'utilisateur final et qu'elle s'exécute sur un appareil sécurisé, elle échappe au contrôle du service informatique qui ne peut ni la supprimer, ni contrôler le partage de ses données. Il est donc impératif d'empêcher toute application non autorisée d'accéder aux services cloud de l'entreprise, quels qu'ils soient, pas seulement Office 365. Ces contrôles sont conformes à la fois au RGPD et au cadre NIST DE.CM-7, car ils interdisent aux logiciels non approuvés l'accès aux données professionnelles.

7. Détecter et corriger les failles « zero-day »

Les contrôles précédents limitent les risques de perte de données. Les pirates découvrent cependant sans cesse de nouvelles failles à exploiter, que ce soit sur le matériel, dans les logiciels ou dans les comportements. Une analyse permanente de ces menaces, basée sur l'apprentissage automatique, combinée à la possibilité de corriger les problèmes au niveau des terminaux, permet de remédier rapidement à ces problèmes.

8. Protéger les systèmes Android, iOS, macOS et Windows 10 au moyen de contrôles de sécurité avancés

L'époque où Windows était l'un des seuls systèmes d'exploitation utilisés est révolue. La plupart des organisations gèrent désormais tout un éventail de systèmes différents. Si les anciens systèmes d'exploitation, tels que Windows 7, utilisent des outils de sécurité désuets, les systèmes plus récents, à l'instar d'Android, iOS, macOS et Windows 10, sont compatibles avec des solutions de sécurité multiplateformes unifiées. Il est alors conseillé de privilégier les solutions dont les contrôles avancés tirent pleinement parti de l'infrastructure de sécurité native de ces systèmes.

9. Certifier la sécurité des appareils (Common Criteria Protection Profile for MDM)

« Common Criteria » est une norme internationale dédiée à la certification de la sécurité informatique. Le Profil de protection pour la gestion des appareils mobiles (MDM) définit la manière dont les règles de sécurité doivent être appliquées aux appareils mobiles en vue du traitement des données professionnelles et de la connexion au réseau d'entreprise. Cette norme est souvent imposée par les institutions gouvernementales et les organisations sous haute sécurité. Il est conseillé de choisir une solution de sécurité ayant obtenu cette certification.

10. Certifier la sécurité dans le cloud (SOC 2 Type 2 et FedRAMP)

Si la solution de sécurité déployée est basée sur le cloud, elle doit être certifiée « Service Organization Controls (SOC) 2 Type 2 » et être assortie d'une description détaillée du test d'audit relatif aux contrôles de conformité et de fonctionnement. Ce test garantit l'efficacité des contrôles portant sur la sécurité, la disponibilité, l'intégrité des traitements, le respect de la vie privée et la confidentialité des systèmes du fournisseur. FedRAMP ATO (Authority to Operate) est une certification américaine officielle qui atteste que le fournisseur remplit les exigences fédérales en matière de gestion des risques de sécurité. Il est conseillé de choisir une solution de sécurité ayant obtenu ces certifications.

Cette liste de contrôle en 10 points distille les bonnes pratiques constatées chez les clients MobileIron. Elle fait partie des éléments à prendre en considération lorsque vous définissez des règles de sécurité, de conformité et d'ordre juridique. Chaque organisation devra mettre en place des mesures adaptées à son secteur d'activité, à sa situation géographique et à sa tolérance aux risques.

La sécurité dans le cloud avec MobileIron

MobileIron est une plateforme de sécurité pour le cloud et les terminaux conforme aux exigences des pouvoirs publics. Voici comment nos clients tirent parti de la technologie MobileIron pour respecter la liste de contrôle ci-dessus :

Points n° 1, 2, 3 et 8

Inscription d'un appareil dans MobileIron : MobileIron installe un profil de configuration sur l'appareil qui sert au service informatique pour les mesures de sécurité nécessaires à la protection des données d'entreprise.

Définition de règles de sécurité : vous définissez les règles de mot de passe et de chiffrement appropriées dans MobileIron. Le cas échéant, recourez à la biométrie pour les processus d'authentification. Si un appareil ne respecte plus les règles de conformité, vous le placez automatiquement en zone de quarantaine ou effacez ses données. Lorsqu'un employé quitte votre organisation, vous procédez à un effacement complet des données de son appareil si ce dernier était détenu par l'entreprise, ou à un effacement sélectif dans le cas contraire.

Gestion des applications d'entreprise : MobileIron permet de distribuer les applications d'entreprise via le magasin d'applications professionnelles Apps@Work ou Google Play d'entreprise. Une fois installées, ces applications sont gérées par le biais des règles définies dans MobileIron. Le service informatique peut alors empêcher le partage de données entre des applications professionnelles et grand public, et supprimer des applications à distance en cas de besoin. Il garde un œil sur les données d'entreprise tout en préservant la confidentialité des données personnelles stockées sur l'appareil.

Point n° 4

Déploiement d'un VPN par application : vous configurez les applications d'entreprise avec MobileIron de sorte qu'elles ne se connectent aux services sur site que par le biais du VPN par application MobileIron Tunnel. Le trafic généré par les applications professionnelles est ainsi séparé de celui des applications grand public, et les données personnelles en sus ne transitent pas par le réseau d'entreprise.

Points n° 5 et 6

Accès aux services cloud accordé uniquement aux appareils et aux applications de confiance : MobileIron Access vous aide à empêcher l'authentification d'appareils et d'applications non gérés, non autorisés ou non conformes auprès des services cloud, tels qu'Office 365, Salesforce, ServiceNow, Workday, etc. Élaborée à partir de normes, la solution MobileIron Access multicloud et multi-identité est compatible avec les nombreux services cloud et fournisseurs d'identité que peut compter une entreprise.

Point n° 7

Détection des failles « zero-day » et correctifs : MobileIron Threat Defense analyse vos appareils, vos applications et vos réseaux à la recherche de toute activité suspecte. Dès qu'il en détecte une, des règles MobileIron sont déclenchées afin que les mesures correctives appropriées, comme l'envoi d'une notification à l'utilisateur, la mise en quarantaine de son appareil ou l'effacement de ses données, soient mises en œuvre.

Points n° 9 et 10

Aucun compromis sur les certifications de sécurité : MobileIron a été la première solution à obtenir la certification « Common Criteria Protection Profile for MDM v2 ». MobileIron est également certifié « SOC 2 Type 2 » et « FedRAMP ATO » (Authority to Operate).

Face à l'évolution des mesures de sécurité, les professionnels de l'informatique se demandent parfois si Microsoft Intune peut répondre aux différents points de cette liste de contrôle. Selon nous, la réponse est non, en particulier en ce qui concerne les points n° 3, 4, 5, 6, 7, 8, 9 et 10. MobileIron s'engage à fournir une architecture de sécurité multi-OS, multicloud et multi-identité, capable de gérer les technologies de pointe mises en œuvre par les entreprises modernes.

Résumé

Dans les années à venir, la plupart des organisations connaîtront un audit de sécurité, qu'il soit interne ou externe. Si l'objectif reste le même, à savoir protéger les données contre toute perte accidentelle et tout acte malveillant, les méthodes employées pour y parvenir diffèrent sensiblement selon que l'architecture de sécurité est traditionnelle ou récente. Une liste de contrôle structurée peut vous aider à investir dans les technologies, les processus et les ressources humaines qui vous permettront de tirer parti rapidement et en toute sécurité de l'innovation des services cloud.

Dans tout déploiement cloud, la sécurité des terminaux doit rester la priorité afin de garantir la conformité au RGPD, au cadre « NIST Cybersecurity Framework » et à tout autre modèle de conformité similaire. Les utilisateurs n'imaginent pas utiliser les services cloud autrement que via des applications récentes sur des terminaux modernes. Sans sécurisation de ces applications et de ces terminaux, toutefois, la perte de données est inévitable. Le volume de données sacrifié dépendra de la rapidité avec laquelle les organisations déploieront une solution de sécurité multicloud end-to-end, telle que MobileIron, lors de leur transition vers Microsoft Office 365, Salesforce, ServiceNow, Workday et au-delà.