Microsoft

Protégez vos données : Sept façons d'améliorer l'état de la sécurité dans votre entreprise

Cela ne fait aucun doute : la mobilité d'entreprise, le déluge des appareils utilisés en milieu de travail, les applications SaaS et le nuage ont transformé le mode de fonctionnement de l'entreprise.

Les entreprises s'appuient sur la collaboration et la mobilité pour gagner en agilité, améliorer le rendement et guider la prise de décision. Les appareils mobiles et les applications, notamment, constituent de puissants outils de productivité. Cependant, au fur et à mesure que le nombre d'appareils mobiles augmente, l'hébergement des applications se déplace des réseaux propriétaires vers les réseaux publics ou hors domaine, et la disparition du périmètre traditionnel de l'entreprise, maintenant dépassé, expose les entreprises à des risques accrus en matière de sécurité et de conformité.

Par exemple, les ouvertures de session multiples, le stockage des informations dans des emplacements disparates et non gérés ou le partage d'information en l'absence de protection complète accroît la vulnérabilité et les risques de perte de données, y compris le risque que des concurrents s'emparent d'informations propriétaires ou que des données critiques soient mises en péril ou endommagées. La question qui se pose est donc la suivante :

Est-il possible d'offrir aux employés la mobilité et la productivité dont ils souhaitent profiter tout en assurant la protection des données?

Est-il possible de laisser les groupes d'activité utiliser les nouvelles applications et les nouveaux systèmes afin d'accroître leur agilité?

Dans ce livre électronique, nous discuterons de sept préoccupations courantes concernant la protection des données auxquelles font face des entreprises comme la vôtre, et des mesures que vous pouvez prendre pour réduire les risques. Le présent document constitue le premier volume d'une série de livres électroniques sur la sécurité qui seront publiés par Microsoft.

Sept façons d'améliorer l'état de la sécurité dans votre entreprise

- Réduire les risques grâce à la gestion de l'identité et de l'accès
- Gérer les applications et les appareils mobiles
- Tirer parti de l'accès conditionnel
- Augmenter la protection des données de l'entreprise
- Prévenir la perte de données
- Permettre la collaboration sécurisée
- Arrêter les programmes malveillants

Réduire les risques grâce à la gestion de l'identité et de l'accès

Comme vous le savez, le maintien du contrôle des applications à la fois dans les centres de données d'entreprise et sur les plateformes d'infonuagique publiques est devenu un défi de taille. Les employés souhaitent accéder aux ressources de données depuis différents appareils et emplacements. Une fois sur le réseau, ils ont besoin d'accéder à différentes ressources variables dans le temps. Les employés peuvent en outre demander l'accès aux ressources de l'entreprise afin de faire leur travail ailleurs qu'à leur bureau.

Malheureusement, les employés constituent souvent le maillon faible, occasionnant par exemple de façon accidentelle la fuite de données sensibles ou révélant leurs informations d'identification dans les réseaux sociaux. De l'extérieur de l'entreprise, un pirate peut utiliser ces informations de connexion pour accéder au réseau et voler des renseignements sur les clients, des biens intellectuels et d'autres données sensibles. Les brèches de sécurité internes mettent également vos données en péril. Comment pouvez-vous contrôler les différents aspects (quoi, quand, où et qui) de l'accès aux applications?

La gestion de l'accès et des identités permet de réduire les risques.

- Éliminez le besoin d'informations de connexion multiples au moyen d'une identité unique permettant d'accéder aux ressources dans le nuage et sur place.
- Limitez l'accès des employés à ce dont chacun a besoin pour faire son travail.
- Révoquez les privilèges d'accès lorsqu'un employé change de rôle, quitte l'entreprise ou n'a plus besoin d'avoir accès à certaines données partagées.
- Mettez en place l'authentification faisant appel à un second facteur en fonction des comportements à risque.

- *Plus de 80 % des employés admettent avoir recours à des applications de type logiciel-service (SaaS) non approuvées dans le cadre de leur travail*[1]

[1] Source : The hidden truth behind shadow IT – six trends impacting your security posture » (Frost & Sullivan)

En savoir plus :

- *Gestion de l'accès et des identités*

Gérer les applications et les appareils mobiles

Avec l'essor de la tendance « Apportez votre propre appareil » (AVPA) et l'utilisation croissante des applications de type logiciel-service (SaaS), les problèmes de sécurité se multiplient. À mesure que les entreprises s'appuient davantage sur les applications SaaS, certaines de leurs données critiques se retrouvent dans le nuage public; ces données sont par conséquent exposées à des risques plus élevés et ne sont pas contrôlées selon les normes mises en place par les services des TI d'aujourd'hui.

Chaque fois qu'un appareil est volé, perdu ou laissé sans surveillance, vos données sont vulnérables, sans protection suffisante. La vulnérabilité existe également lorsque les données d'entreprise se retrouvent dans des applications personnelles et risquent de tomber entre de mauvaises mains. À l'ère de l'AVPA, comment protégez-vous vos données sans nuire à la productivité des employés?

Commencer par les bases :

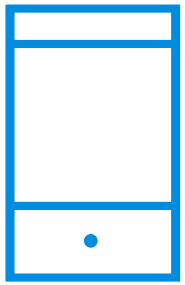
- Ne perturbez pas le flux d'utilisation; faites en sorte que l'observation des normes par les utilisateurs soit facile et naturelle.
- Faites preuve de transparence en ce qui concerne l'effet des mesures prises par le service des TI sur leurs appareils.
- Protégez uniquement les données de l'entreprise.

- *Environ cinquante-deux pour cent des travailleurs de l'information répartis dans 17 pays ont déclaré utiliser plus de trois appareils dans le cadre de leur travail*[1]

[1]Source : Employee devices bring added security concerns », par Cindy Bates (blogue pour PME de Microsoft aux États-Unis)

En savoir plus :

- *Microsoft Intune*



Tirer parti de l'accès conditionnel

L'accès conditionnel consiste à limiter l'accès aux ressources de l'entreprise en fonction de l'identité de l'utilisateur ou de l'intégrité de l'appareil. L'accès conditionnel consiste aussi à faire respecter les politiques de l'entreprise en fonction de l'emplacement et du niveau de sensibilité des données d'application.

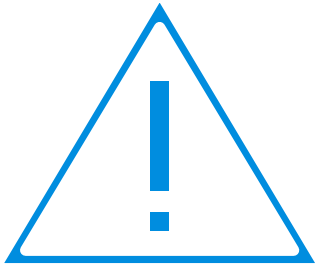
Par exemple, l'accès à une application de gestion de la relation client depuis un café nécessite l'authentification multifacteur en raison de l'endroit où se trouve l'utilisateur et de la sensibilité des données de ce type d'application. Un autre exemple réside dans le courriel. L'appareil utilisé doit être conforme aux politiques de l'entreprise, notamment en ce qui a trait au chiffrement et à l'utilisation d'un NIP, pour permettre l'accès au courriel d'entreprise.

Quelles sont les premières étapes?

- Mettez en place une politique d'accès pour les appareils mobiles. Vous pouvez exiger la gestion intégrale de l'appareil ou seulement des applications telles qu'Outlook pour l'accès au courriel d'entreprise.
- Tirez parti des groupes dynamiques pour permettre aux employés d'accéder aux applications dont ils ont besoin en fonction de leur rôle.
- Mettez en place l'authentification multifacteur, qui ajoute une protection supplémentaire en exigeant des utilisateurs qu'ils s'authentifient de deux façons différentes. La première méthode peut correspondre à la combinaison habituelle d'un nom d'utilisateur et d'un mot de passe. La deuxième méthode comporte souvent un aspect physique qui serait pratiquement impossible à reproduire. Par exemple, glisser une carte-clé et entrer un NIP, se connecter à un site Web et entrer un mot de passe à utilisation unique, se connecter à l'aide d'un client RPV comportant un certificat numérique ou lire l'empreinte digitale de l'utilisateur.

En savoir plus :

- *L'accès conditionnel et Azure Active Directory*
- *Présentation de l'accès conditionnel*
- *L'accès conditionnel et Microsoft Intune*
- *Office 365 et Microsoft Intune*
- *Windows 10*



Augmenter la protection des données de l'entreprise

Le fait de permettre aux employés d'utiliser leurs propres appareils fait augmenter le risque de fuite de données par l'intermédiaire des applications et des services tels que le courriel, les médias sociaux et le nuage. Ces facteurs échappent à votre contrôle. Par exemple, un employé peut envoyer les plus récentes photos d'ingénierie depuis son compte de courriel personnel, copier et coller des informations dans des médias sociaux ou enregistrer un rapport en cours de rédaction dans son espace de stockage personnel dans le nuage. Vous souhaitez permettre l'utilisation des appareils personnels sans mettre en péril la sécurité de vos données. Comment y parvenir?

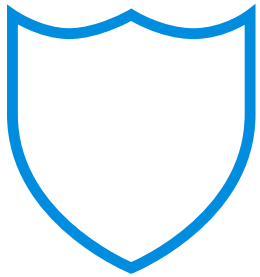
La solution de protection des données Enterprise Data Protection (EDP) contribue à prévenir ces fuites de données potentielles vers des applications ou des sites non autorisés sans nuire à l'expérience d'utilisation de l'employé.

Pour commencer :

- Activez la solution EDP dans votre environnement d'entreprise, de manière à pouvoir gérer et contrôler les applications et les données sans introduire de changements superflus.

Pour en savoir plus :

- *Protection des données de l'entreprise sous Windows 10*
- *Présentation de BitLocker*
- *Microsoft Intune*



Prévenir la perte de données

L'erreur est humaine, mais tout le monde sait que le coût peut en être élevé. Le partage de documents par courriel est un outil de productivité important pour les employés, de sorte que les professionnels en sécurité font face à un véritable casse-tête : comment permettre aux employés de partager des fichiers par courriel sans mettre en danger les informations sensibles?

Commencez par réduire la probabilité de fuite :

- Familiarisez-vous avec les capacités de prévention de la perte de données de votre environnement afin de protéger vos données là où elles sont stockées, lorsqu'elles sont déplacées et lorsqu'elles sont partagées. Par exemple, un courriel peut être distribué de façon limitée à l'intérieur de l'organisation ou comporter une qualification de gestion des droits numériques déterminant à qui il est permis d'ouvrir le message.
- Déployez la prévention de la perte de données au-delà du courriel. Certains programmes de traitement de texte, de feuilles de calcul et de présentation offrent également des options d'accès restreint qui empêchent l'ouverture des documents par des utilisateurs non autorisés.

Pour en savoir plus :

- *Office 365 et la prévention de la perte de données*
- *Microsoft Office 365*

Permettre la collaboration sécurisée

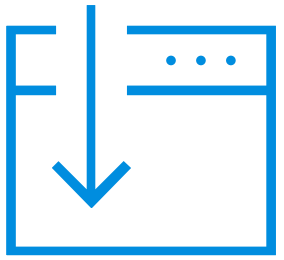
Lorsqu'il s'agit de partager des informations, la commodité l'emporte souvent sur la sécurité, ce qui transforme en cauchemar la vie des professionnels en sécurité. Les employés peuvent faire preuve de créativité lorsqu'il s'agit de partager les informations, mettant vos données en péril et faisant courir à votre entreprise le risque de perdre des données critiques. Comment encourager la collaboration entre les employés tout en réduisant au minimum le risque de compromettre les informations?

Offrez une solution souple, facile à utiliser et sécurisée qui répond à leurs besoins.

- Établissez des outils sécurisés pour le partage des informations et assurez-vous que l'accès est restreint aux employés autorisés. Ces mesures comprennent une solution de partage de documents sécurisée, comme SharePoint, le partage réseau à accès restreint ou une solution en nuage.
- Exigez l'utilisation de la gestion des droits numériques ou d'une autre solution de courriel sécurisée lors de l'envoi de documents sensibles par courriel.
- Procurez un flux de travail de partage des informations facile et sécurisé afin de permettre la collaboration interne et externe.

En savoir plus :

- *Azure Rights Management*
- *Partage de fichiers protégés*
- *Envoi de courriels chiffrés*
- *Microsoft Office 365*
- *SharePoint*
- *Microsoft Azure*



Arrêter les programmes malveillants

Les infections par les programmes malveillants sont souvent attribuables à une erreur de l'utilisateur. Les attaques d'hameçonnage et d'usurpation d'identité sont maintenant extrêmement sophistiquées; les pirates trompent et leurrent les utilisateurs à l'aide de faux reportages ou de courriels qui semblent provenir de marques de confiance et les persuadent de télécharger des applications en apparence inoffensives qui sont en réalité piégées. Vous ne pouvez empêcher les utilisateurs de naviguer sur le Web, d'utiliser les médias sociaux ou d'accéder à leur compte de courriel personnel sur leurs propres appareils. Comment les aider à accomplir ces tâches quotidiennes de manière plus sécuritaire?

L'éducation est votre première ligne de défense.

- Demandez aux employés de prendre connaissance d'un guide de base ou de suivre une formation sur les attaques de programme malveillant les plus courantes.
- Vérifiez les URL des courriels pour vous assurer qu'elles sont pertinentes, exactes et légitimes.
- Suggérez aux employés de se limiter aux applications téléchargées d'une source de confiance.

En savoir plus :

- *Windows 10*
- *Windows Defender*
- *Windows Device Guard*
- *Microsoft Office 365*

Concentrez-vous sur ces sept points en vue d'améliorer la sécurité de votre organisation

Le fait d'accorder la mobilité aux employés n'équivaut pas nécessairement à mettre en péril la sécurité de vos données. Grâce à une planification adéquate, aux outils appropriés et à l'éducation, vous pouvez donner à vos employés la liberté de travailler n'importe où, en tout temps, tout en réduisant le risque au minimum.

En savoir plus sur la cybersécurité

© Microsoft Corporation, 2016. Tous droits réservés. Ce document est publié à titre d'information seulement. Microsoft ne donne aucune garantie, explicite ou implicite, en ce qui concerne les renseignements dans le présent document.