RELEVER LE DÉFI DE LA CONFORMITÉ DANS LE CLOUD : LES STRATÉGIES SONT ESSENTIELLES

FORCEPOINT

RELEVER LE DÉFI DE LA CONFORMITÉ DANS LE CLOUD : LES POLITIQUES SONT ESSENTIELLES

Le Cloud Computing transforme la manière de travailler des entreprises. Alors que le cloud computing réduit les coûts et la complexité d'acquisition et de fonctionnement des ordinateurs et des réseaux, les entreprises perdent une partie de contrôle sur leurs données pour tirer parti des avantages du cloud. Cela est particulièrement vrai pour les entreprises qui utilisent des applications SaaS de stockage de fichiers , comme Microsoft Sharepoint, OneDrive, Google Drive, Dropbox et bien d'autres. Cependant, même si les équipes IT ne contrôlent pas les terminaux ou les applications cloud, la protection des biens et des informations de leur entreprise reste toujours sous leur responsabilité. Elles doivent s'assurer que les applications cloud sont en conformité avec les politiques IT de l'entreprise.

LES VECTEURS DE CONFORMITÉ INTERNES ET EXTERNES

"Conformité" est devenu un mot populaire qui revêt plusieurs significations et signifie divers objectifs, souvent dictés par votre rôle dans l'entreprise. Les exigences de conformité externe se concentrent sur le suivi des règlementations, des standards et des lois imposées par des gouvernements et des normes industrielles ou d'entreprise. Parmi deux exemples de régulations externes importantes, citons le Health Insurance Portability and Accountability Act (HIPAA), qui régit l'usage des informations relatives aux patients, et le standard PCI DSS de l'industrie des cartes de paiement qui régit comment les entreprises doivent stocker, traiter et manipuler les données relatives aux cartes de crédit. Être en conformité signifie qu'à un instant donné, un audit réalisé sur vos technologies logicielles, vos procédures et vos flux de travail vous permettent de vous conformer à un ensemble de règles, de politiques et de lois. Les exigences de conformité externes, en elles-mêmes, n'indiquent pas comment vous devez assurer la sécurité des informations.

Par contraste, la conformité interne se concentre sur l'adhésion à des standards et des meilleures pratiques incorporées dans les politiques internes et gérées via la gouvernance de l'entreprise. La conformité interne est définie par l'entreprise et se concentre sur la protection des données comme les propriétés intellectuelles, les plans stratégiques et les archives commerciales.

Le besoin de sécuriser les données d'entreprise partage de nombreux objectifs avec le maintien de la conformité via les politiques internes et externes. Cependant, la sécurité se concentre spécifiquement sur les acteurs malveillants, ce qui nécessite des stratégies appropriées. Bien que les initiatives visant à maintenir la conformité et la sécurité se juxtaposent, ces projets nécessitent chacun un traitement individuel et ne peuvent en aucun cas se substituer l'un à l'autre.

LE PÉRIPLE POUR LA CONFORMITÉ CLOUD

L'un des défis majeurs posés aux entreprises lorsqu'elles établissent un programme de conformité est de savoir par où commencer. Elles se rendent compte que la conformité consiste à gérer les interactions entre les personnes, les données et les IP critiques, et qu'elles doivent respecter des lois et règlementations fédérales ou nationales. Malheureusement, peu comprennent que de bonnes politiques sont les fondations d'un programme de conformité efficace, et que développer des politiques adéquates demande un certain temps. De nombreuses entreprises ne réalisent pas que les exigences de conformité pour le cloud et sur site sont identiques – les données restent les données, où qu'elles se trouvent. Cependant, quand on est confronté à des applications SaaS dans le cloud, les entreprises n'ont pas de contrôle sur l'environnement des données. Ce facteur critique doit être pris en compte lorsque l'on choisit des outils pour gérer et faire appliquer des initiatives de sécurité et de respect de la conformité.

> **Il est important pour les entreprises d'utiliser des mesures de sécurité qui les aident à être en conformité, plutôt que de se reposer sur la conformité pour piloter la sécurité.**

CRÉATION ET APPLICATION DE POLITIQUES : LES BASES D'UN PROGRAMME EFFICACE DE CONFORMITÉ

Les premiers pas à effectuer pour développer des politiques de conformité est de créer des classifications pour les données, les utilisateurs et les applications, afin de définir comment interagissent les données, les utilisateurs et les applications. Avant de développer des classifications, vous devez déterminer la valeur relative de chaque bien pour l'entreprise.

Classifications des données – Déterminer la classification des données que l'entreprise autorise à être créées, manipulées et stockées dans le cloud, ainsi que les personnes qui peuvent avoir accès à chaque classification et dans quelles circonstances.

- Établir des classifications de données pour établir l'impact dans l'entreprise.
- Établir des types de données liées à leur utilisation fonctionnelle (par ex. rapports de ventes, collaboration interservices, outils marketing).
- Établir une matrice de types de classification et déterminer l'éligibilité de chaque élément à utiliser dans une configuration cloud, ainsi que les éventuelles protections nécessaires qui déterminent l'éligibilité, par exemple l'absence de partage public de fichiers.
- Déterminer les utilisateurs des données autorisés et les actions permises, comme l'accès, la suppression et le stockage selon des critères d'heure, de lieu et d'appareil.
- Déterminer l'intervention et la correction des actions qui ne sont pas cohérentes avec les politiques créées.
- Établir des protections pour estimer et effectuer une détermination finale des risques/gains de ces données classifiées si le vol, la destruction ou la corruption des données classifiéesposent un risque au maintien de la conformité.

Classification des personnes/utilisateurs – Déterminer une classification des utilisateurs de l'entreprise qui permet de définir les actes autorisés par un utilisateur, comme créer, partager ou modifier, selon la base d'une classification de données et sous quelles circonstances.

- Établir des groupes et des classifications d'utilisateurs qui conditionnent les usages permis des données.
- Établir des paramètres d'usage acceptable pour chaque utilisation et établir une matrice des éléments selon l'action (par ex., créer et supprimer), l'emplacement géographique, la chronologie et l'appareil (en incluant les caractéristiques de l'appareil).
- Déterminer des exceptions aux politiques pour correspondre aux besoins organisationnels comme les voyages d'affaires, les rôles spécifiques et les individus.
- Identifier les comportements qui peuvent indiquer soit un comportement à risque non intentionnel ou potentiellement malveillant, et déterminer les interventions qui correspondent au niveau de risque en utilisant un schéma "Si-Donc".

Classification des applications – Établir des politiques pour les applications autorisées ou non aux utilisateurs, qui définissent les types d'applications permises (par ex. collaboration, CRM et Finance), incluant le déploiement de politiques de données veillant à déterminer les zones de risque acceptables.

- Identifier clairement ce qui constitue une application utilisateur par contraste avec les sites web passifs.
- Établir les métriques des risques acceptables d'application selon les exigences règlementaires, les certifications d'industrie et vos propres bancs d'essai internes. Prêter attention aux capacités de manipulations de données comme le partage, l'audit et le contrôle du changement pour des actions comme la suppression.
- Établir des paramètres d'usage acceptable pour chaque élément de matrice d'application utilisateur prenant en compte chaque type d'application, l'emplacement géographique, la chronologie et les caractéristiques de l'appareil.
- Établir une limite acceptable d'utilisation simultanée d'applications en prenant en considération les comptes d'entreprise et les comptes personnels.
- Établir des politiques d'approbation des applications pour les nouvelles applications, y compris les catégories d'applications SANS obligation d'approbation
- Déterminer l'intervention et la correction des actions qui ne sont pas cohérentes avec les politiques créées.

Les programmes de conformité deviennent des éléments essentiels du paysage économique, mais ils peuvent s'avérer compliqués à établir et maintenir. Les politiques forment la clé de voute du programme de sécurité et de conformité d'une entreprise, mais développer des politiques efficaces prend du temps. De plus, sans politiques clairement définies, les investissements en sécurité et en outils de conformité ne peuvent pas être optimisés. Il faut investir le temps et les ressources nécessaires pour établir des politiques correctes ou courir le risque d'exposer des informations critiques, et affronter les conséquences négatives d'un échec lors d'un audit de la conformité.

À PROPOS DE FORCEPOINT

Grâce à nos systèmes sans concession, les entreprises peuvent accorder à leurs employés un accès sans restriction aux données confidentielles, tout en assurant la protection de la propriété intellectuelle et la simplification de la conformité.

CONTACT

www.forcepoint.com/contact

© 2018 Forcepoint. Forcepoint et le logo FORCEPOINT sont des marques déposées par Forcepoint. Raytheon est une marque déposée de Raytheon Company. Toutes les autres marques citées dans ce document appartiennent à leurs propriétaires respectifs.

[SOLUTION-BRIEF-FR] 700015.101718