La sécurité du Cloud et votre entreprise

La sécurité de l'information n'est pas quelque chose que nous avons c'est quelque chose que nous faisons. La sécurité n'est pas non plus le résultat d'une ou deux choses qu'on a faites dans le passé, puis qu'on a oubliées. Comme vous le dira votre responsable de la sécurité de l'information, la sécurité est un processus continu et permanent qui exige une vigilance à long terme. Le succès de la sécurité dépend de l'engagement constant des personnes à appliquer les outils, les technologies et les processus les plus fiables pour ramener les risques à un niveau raisonnable. Vous ne réduirez jamais le risque à zéro, mais il est possible de réduire le risque à un niveau correspondant à la probabilité et à l'impact d'une violation de la sécurité, à un coût raisonnable.

Dans ce contexte, le débat sur la question de savoir si le Cloud computing est plus ou moins sécurisé que les données sur site est une abstraction qui se trompe de cible. Tant que votre système est connecté à Internet, qu'il s'agisse d'une solution Cloud ou d'un logiciel déployé sur site, vous encourez un risque de violation de la sécurité des données. La question essentielle est de savoir si vous avez mis en place des contrôles appropriés pour minimiser les risques pour la confidentialité, l'intégrité et la disponibilité de vos données.

L'importance et l'urgence de la sécurité et de la confidentialité des données ne peuvent être surestimées. 2017 a vu certaines des plus importantes violations de données de l'histoire, tandis que le coût direct de la résolution d'une violation de données s'est élevé en moyenne à **3,62 millions de dollars**. Mais les coûts directs ne sont rien par rapport aux dommages incalculables et durables infligés à la marque, à la réputation et à l'activité qu'un incident de sécurité des données peut entraîner.

Sommaire

Comprendre la menace

Les risques associés aux menaces de la sécurité de l'information augmentent chaque jour. Le nombre d'attaques potentielles s'étend également pour inclure non seulement des attaques indépendantes et des petits groupes, mais aussi des organisations de piratage sponsorisées par l'État qui sont beaucoup mieux organisées et financées. Ces groupes plus importants peuvent se permettre de consacrer de multiples ressources à la violation des défenses des petites et grandes entreprises sur une longue période de temps - un niveau d'engagement des attaquants autrefois réservé aux cibles les plus stratégiques.

Sauf si votre entreprise maintient un environnement qui interdit tout accès Internet externe, il est probable que votre environnement d'entreprise ait déjà subi une attaque réussie, même si c'est quelque chose d'aussi simple que la publication non autorisée de certaines données personnelles. Comme le dit **John Chambers, PDG de Cisco**, « Il n'y a que deux types de sociétés : celles qui ont été piratées et celles qui ne le savent pas encore. »

Ce n'est pas la faute de votre organisation informatique interne. L'environnement commercial actuel exige un niveau d'agilité et d'efficacité qui oblige les organisations à ouvrir leurs réseaux d'une manière qui aurait été inimaginable encore récemment. Cette ouverture, tout en s'avérant essentielle pour la compétitivité d'une entreprise, a rendu encore plus difficile le maintien d'un réseau sécurisé.

Des organisations telles que la Cloud Security Alliance et d'autres groupes de recherche citent fréquemment des raisons impérieuses de viser la meilleure sécurité possible, que vous utilisiez des logiciels déployés dans le Cloud ou des solutions déployées sur site.

Les 5 principales raisons de mettre à jour votre sécurité :

1. **Il y a de fortes chances pour que votre organisation subisse des changements**—**Les experts sont d'accord** qu'un éventail croissant de menaces pour la sécurité augmente les risques de transformation pour presque toutes les entreprises. Parmi les perturbations les plus coûteuses, citons les dénis de service, les initiés malveillants et les attaques Web. Mais les perturbations coûteuses pour la confidentialité, l'intégrité et la disponibilité de vos données peuvent provenir d'une grande variété de causes.
2. **Les initiés malveillants causent une proportion surprenante d'attaques**—Les employés sont les coupables les plus fréquemment cités des attaques de sécurité des données, selon une **étude de PWC**. À cet égard, les données sur site et les données dans le Cloud sont tout aussi vulnérables. Il est donc essentiel que l'infrastructure de sécurité de l'entreprise englobe à la fois le Cloud et les données sur site avec une égale vigilance.
3. **Les cyber-attaques demeurent coûteuses**—Une étude du **Ponemon Institute** a montré que le coût d'une cyber-attaque s'élevait en moyenne à 3,62 millions de dollars en 2016.
4. **L'informatique furtive (Shadow IT) a le vent en poupe**—Plus de 80 % des employés utilisent des applications Cloud ou SaaS qui n'ont pas été approuvées par les services informatiques, selon une étude de **Frost & Sullivan**. Cette habitude persiste malgré le fait que 15 % des employés déclarent avoir personnellement vécu des incidents de sécurité (y compris des infections de logiciels malveillants et des pertes de données) résultant de l'utilisation de ces applications.

5. **Les pratiques de BYOD ajoutent de nouveaux risques**—Pratiquement tous les employés arrivent aujourd'hui au travail avec un ou plusieurs dispositifs informatiques connectés au Web, principalement des smartphones et des tablettes, qui peuvent engendrer des risques de sécurité hors du contrôle du service informatique. Qu'il existe ou non une politique officielle en matière de « Apportez votre propre appareil (BYOD) », les risques créés par la profusion d'appareils appartenant aux employés sur le lieu de travail constituent un défi permanent pour votre processus de sécurité de l'information.

Le pouvoir des normes et de la conformité

Les normes jouent un rôle essentiel dans la sécurité de l'information, garantissant ainsi que les pratiques soient rigoureuses, cohérentes et efficaces. A priori, les normes mondiales les plus connues qui prescrivent un système efficace de gestion de la sécurité de l'information et les contrôles détaillés correspondants sont les normes ISO/IEC 27001:2013 et ISO/IEC 27002:2013, mais de nombreuses organisations choisissent de s'appuyer sur les normes NIST 800-53, la Cloud Security Alliance, SSAE 18, SOC 1, SOC 2 ou d'autres normes qui prescrivent généralement des contrôles similaires.

Ces normes décrivent en détail les contrôles de sécurité, les procédures et les processus qu'une organisation doit suivre pour se considérer comme conforme aux meilleures pratiques en vigueur. Un hôte Cloud conforme à la norme ISO 27001 doit également satisfaire à la norme dans plusieurs domaines clés, notamment :

- **Politiques de sécurité**—Tous les employés devraient être tenus responsables de la sécurité des informations non publiques et suivre les pratiques définies dans le système de gestion de la sécurité de l'information.
- **Organisation de la sécurité de l'information**—La direction doit s'engager en matière de sécurité et établir une organisation chargée de la sécurité des informations non publiques.
- **Gestion des équipements**—Les équipements doivent être strictement contrôlés et toutes les données doivent être classées, afin de déterminer les exigences appropriées en termes d'accès et de manipulation.
- **Pratiques de sécurité liées aux ressources humaines**—L'organisation doit effectuer une vérification complète des antécédents au moment de l'embauche de chaque employé et exiger que les employés se familiarisent avec les responsabilités en matière de sécurité et s'y conforment. En cas de départs ou de transferts d'employés, un processus formel doit être prévu pour supprimer ou mettre à jour leur accès physique et virtuel aux infrastructures de l'entreprise.

- **Sécurité physique et environnementale**—Les composants critiques doivent être placés dans des espaces contrôlés physiquement avec des contrôles d'accès suffisants pour sécuriser l'infrastructure. Les organisations doivent également fixer des règles sur qui a accès aux espaces contrôlés et dans quelles circonstances, et surveiller de manière cohérente le respect de ces règles. Les mesures de sécurité physiques et environnementales peuvent inclure des cartes d'identité, des badges ou des contrôles d'accès biométriques, et devraient limiter l'accès aux emplacements sécurisés en fonction du poste de travail.
- **Gestion des opérations**—L'organisation doit établir des contrôles concernant la planification du système, la protection contre les codes malveillants, les processus de sauvegarde, la sécurité des réseaux, la gestion des supports et l'échange d'informations. Ces contrôles doivent être constamment analysés et surveillés pour assurer qu'ils fournissent une protection raisonnable pour les données couvertes. Les fournisseurs de services tiers ayant accès à des informations confidentielles doivent respecter les exigences en matière de sécurité et de confidentialité qui sont cohérentes avec les propres politiques et procédures de l'organisation en matière de protection des informations confidentielles et au moins aussi restrictives qu'elles.
- **Contrôle d'accès**—Tout accès aux systèmes, réseaux et applications doit être contrôlé au niveau de l'utilisateur et de la ressource avec des techniques de privilèges en fonction des rôles. Cet accès devra être revu périodiquement pour s'assurer qu'un changement de personnel ou un changement de rôle n'a pas modifié les besoins d'accès de l'individu.
- **Développement de système**—Les exigences de sécurité de toutes les applications qui traitent des informations confidentielles doivent être définies au début de la phase de développement. Des techniques appropriées de protection des données doivent être intégrées dans l'application, et les modifications apportées aux logiciels développés doivent passer par un processus de gestion des changements élaboré.
- **Gestion des incidents**—En cas d'incident de sécurité réel ou suspecté, les équipes doivent immédiatement commencer à identifier la portée de l'impact, atténuer toute exposition, déterminer la cause de l'incident et prendre les mesures correctives appropriées, y compris l'escalade et la notification des incidents aux parties concernées, si nécessaire.

Rester vigilant

Si la sécurité de l'information était évaluée en fonction du risque, le score parfait serait zéro et irréalisable. Trop de menaces surviennent chaque jour pour s'attendre à une année sans exposition au risque. Mais vous pouvez tendre à ce genre d'idéal moyennant quelques précautions essentielles :

- **Adoptez un cadre sécurisé pour le Cloud**. Regroupez autant de capacités informatiques que possible dans un cadre qui a été certifié conforme à des normes reconnues telles que ISO 27001, ITAR et FedRAMP. Les principaux fournisseurs d'infrastructures Cloud se conforment généralement à ces normes et maintiennent un processus continu pour garantir la conformité de leurs produits aux normes de sécurité appropriées.
- **Assurez-vous que votre organisation respecte les normes de sécurité en vigueur dans votre secteur d'activité**. Les normes telles que HIPAA et ITAR, et les règlements de la FDA sont conçus pour optimiser la sécurité autour des types d'informations qui sont les plus critiques dans certains secteurs. Pour assurer une sécurité efficace, vous et votre fournisseur d'infrastructure Cloud devez respecter les normes de sécurité les plus pertinentes pour votre marché. C'est la force de son maillon le plus faible qui détermine celle de votre chaîne de sécurité.

  Les normes de sécurité évoluent également au fil du temps et constituent un point de repère qui permet de déterminer si les pratiques et les procédures de sécurité de votre organisation sont suffisantes pour maintenir vos risques aussi faibles que possible à un moment donné.
- **Envisagez un service de validation de la conformité**. Les consultants tiers spécialisés dans l'évaluation de la conformité en matière de réglementation et de sécurité peuvent fournir un référentiel utile et impartial pour garantir que vos efforts de sécurité placent votre organisation dans de bonnes conditions.
- **Assurez-vous que tous vos fournisseurs de Cloud respectent les dernières normes de sécurité**. La technologie Cloud facilite l'adoption par une entreprise de nombreux services déployés dans le Cloud pour différentes fonctions : automatisation des ventes, ERP, gestion des équipements, paie, etc. Il est essentiel que tous les fournisseurs Cloud prennent en charge les normes de sécurité qui couvrent votre secteur et comprennent les exigences de sécurité spécifiques de votre entreprise.

En cherchant, dans la mesure du possible, à respecter les normes acceptées, vous pouvez réduire l'exposition de votre organisation aux risques et être prêt à résoudre les problèmes rapidement et au coût le plus bas possible.

En bref

Examiner les normes

En restant conformes aux normes de sécurité telles que ISO/IEC 27001:2013 et NIST 800-53, et en vous tenant au courant des dernières recommandations de ces normes, vous réduisez le risque d'une cyberattaque néfaste.

En savoir plus sur le Cloud d'Infor via infor.com/cloud

Suivez-nous :

Infor France (SAS), Immeuble Cristalia, 6ème étage, 3 Rue Joseph Monier, 92500, Rueil-Malmaison

INF-1475040-fr-FR-0919-1