Clouds et sécurité informatique

Camille Bednarek

2023-02-08

L'arrivée de l'Internet a eu un impact considérable sur le monde informatique. Ce qui a commencé comme un projet pour l'armée américaine par des étudiants s'est rapidement transformé en une innovation qui continue à évoluer pour être toujours plus performante. Aujourd'hui, les utilisateurs peuvent accéder à Internet à partir de différents appareils, tels que les téléphones portables, les ordinateurs et les clouds, qui offrent des applications et des services de stockage en ligne.

Qu'est ce qu'un cloud ?

Un cloud est un service de stockage de données en ligne qui permet aux utilisateurs de stocker, accéder et partager leurs données à partir d'internet. Au lieu de stocker des données sur le disque dur local d'un ordinateur, les données sont stockées sur des serveurs distants, gérés par un fournisseur de services de cloud. Les utilisateurs peuvent accéder à leurs données à partir de n'importe où et de n'importe quel appareil connecté à internet. Les clouds peuvent également offrir des services supplémentaires tels que le traitement du traitement des données, l'analyse, la gestion des applications, etc.

Pourquoi utiliser un cloud ?

Les clouds sont devenus un élément clé de l'infrastructure informatique pour de nombreuses entreprises et particuliers. Les avantages de l'utilisation des clouds incluent une flexibilité accrue, une accessibilité à distance, une collaboration en temps réel, une réduction des coûts informatiques, une scalabilité plus facile et une maintenance simplifiée. Les services de cloud computing peuvent être utilisés pour stocker des données, exécuter des applications et des programmes, et fournir un accès à des ressources informatiques telles que le calcul et le stockage. Il existe différents types de clouds, tels que les clouds publics, les clouds privés, les clouds hybrides et les clouds communautaires, qui répondent à différents besoins en matière de confidentialité, de performance, de coûts, de gestion et de sécurité. Cependant, l'utilisation des clouds comporte également des risques tels que la perte de données, la violation de la vie privée, les cyberattaques et les interruptions de service. Il est donc important de choisir un fournisseur de cloud fiable et de mettre en place des mesures de sécurité appropriées pour protéger les données et les informations sensibles.

Quels risques liés au cloud ?

Les risques liés aux clouds sont nombreux et peuvent porter sur la sécurité des données, la confidentialité, la disponibilité et la conformité réglementaire. Tout d'abord, les clouds étant accessibles en ligne, les données y étant stockées peuvent être vulnérables aux cyberattaques, telles que les pirates informatiques, les hacks et les ransomwares. De plus, les clouds sont souvent gérés par des tierces parties, ce qui peut entraîner des problèmes de confidentialité si les données sont partagées avec des parties non autorisées. Les clouds peuvent également être affectés par des perturbations telles que les pannes de serveur, ce qui peut rendre les données inaccessible à l'utilisateur. Enfin, l'utilisation de clouds peut entraîner des problèmes de conformité réglementaire, telles que les réglementations en matière de protection des données personnelles. Il est donc important pour les utilisateurs de se familiariser avec les risques liés aux clouds et de prendre les mesures nécessaires pour minimiser ces risques.

(El Alloussi, Fetjah, and Sekkaki 2012)

Quelles mesures préventives ?

Pour protéger son cloud, il est recommandé de suivre les mesures suivantes: 1. Former les employés aux risques de sécurité et à la protection des données. 2. Identifier les données et les traitements qui seront transmis via le cloud. 3. Définir les exigences de sécurité pour chaque utilisateur (personnel ou professionnel). 4. Choisir un prestataire de confiance qui offre des garanties de sécurité. 5. Réaliser une analyse des risques de cyberattaques régulièrement. 6. Mettre en place une stratégie de sauvegarde et de restauration des données en cas d'incident. 7. Établir des contrats formels avec les éditeurs pour définir les obligations en matière de protection des données. 8. Mettre à jour régulièrement les systèmes de sécurité pour garantir leur efficacité.

Existe-t-il des protections?

Afin de palier à ces risques, il existe le Règlement général sur la protection des données (RGPD). Il s'agit d'une réglementation de l'Union européenne entrée en vigueur en mai 2018. Il a pour objectif de renforcer les droits des citoyens en matière de protection de leurs données personnelles et de responsabiliser les entreprises qui collectent, traitent et utilisent ces données. Le RGPD s'applique à toutes les entreprises et organisations situées dans l'Union européenne, ainsi qu'à celles qui collectent et traitent des données de citoyens de l'UE, même si elles ne sont pas situées sur le territoire de l'UE. Il impose de nouvelles obligations en matière de protection des données personnelles, telles que la notification obligatoire des violations de données, l'obligation d'obtenir le consentement explicite des personnes concernées pour le traitement de leurs données, la mise en place de mesures de sécurité appropriées pour protéger les données et la nomination d'un délégué à la protection des données pour les entreprises de certaine taille. Le RGPD prévoit également des sanctions importantes en cas de non-conformité, allant jusqu'à 4% du chiffre d'affaires annuel mondial de l'entreprise ou 20 millions d'euros, ce qui incitera les entreprises à prendre la protection de la vie privée de leurs clients très au sérieux. En somme, le RGPD vise à renforcer la confiance des citoyens dans le traitement de leurs données personnelles par les entreprises et à instaurer un cadre juridique plus robuste pour protéger la vie privée en ligne.

(DE TERWANGNE 2018)

Ainsi, la sécurité des données dans le cloud est cruciale en raison de la nature de ces dernières, souvent confidentielles et sensibles. Si elles sont compromises, cela peut avoir de graves conséquences pour les individus et les entreprises. Il est donc important de mettre en place des mesures pour protéger les données stockées dans le cloud, telles que l'utilisation de mots de passe forts, la mise en place de contrôles d'accès stricts et la mise en œuvre de politiques de sauvegarde régulières. Le RGPD offre également une protection supplémentaire en matière de protection des données personnelles, en exigeant que les entreprises traitant ces données les protègent adéquatement. Sécuriser son cloud et ses données personnelles est une responsabilité partagée entre les entreprises et les individus. Il est important de rester informé et conscient des risques pour prendre les mesures nécessaires pour protéger les informations sensibles.

Bibliographie

Bibliographie

« Cloud : quelles sont les principales menaces et comment s'en protéger ». Consulté le 10 février 2023. https://www.lebigdata.fr/cloud-menaces.

« Le RGPD pour les nuls | Définition, application et obligations ». Consulté le 10 février 2023. https://donnees-rgpd.fr/definitions/rgpd-pour-les-nuls/.

Koban. « [RGPD] Où sont stockées vos données ? Le Cloud pour les nuls », 11 décembre 2017. https://www.koban.cloud/rgpd-stockees-vos-donnees-cloud-nuls/.

DE TERWANGNE, Cécile. 2018. "TITRE 2 définitions Clés Et Champ d'application Du RGPD." *Le règlement général Sur La Protection Des Données (RGPD/GDPR): Analyse Approfondie*, 59–84.

El Alloussi, Hassan, Laila Fetjah, and Abderrahim Sekkaki. 2012. "L'état de l'art de La sécurité Dans Le Cloud Computing." *INTIS 2012*, 3.