CYBER READINESS
INSTITUTE

FAQ sur les clouds :

Améliorer la cybersécurité pour le télétravail

En réponse à la pandémie COVID-19, la main-d'œuvre de la plupart des entreprises s'est éloignée. Le travail à distance introduit de nouveaux risques en matière de cybersécurité, d'autant plus que les employés accèdent à l'information par de nouvelles voies, notamment par le biais du cloud.

Le moment est venu d'évaluer comment votre organisation utilise le cloud. Le cloud a de multiples atouts qui peuvent contribuer à rendre le télétravail plus pratique, plus efficace et plus sûr. Cette FAQ est conçue pour aider les cadres supérieurs des petites et moyennes entreprises (PME) à se familiariser avec la terminologie du cloud et à comprendre les bases de la contribution du cloud à la cybersécurité de votre personnel distant.

J'entends beaucoup parler du "Cloud", mais quelles sont les bases que je dois connaître ?

Le "cloud" désigne un groupe d'ordinateurs (appelés communément "serveurs") appartenant à une entreprise et exploités par celle-ci (généralement dénommée fournisseur de service cloud ou "CSP") qui vous fournit des logiciels ou de l'espace de stockage. Un client ou une entreprise accorde une licence pour l'utilisation du logiciel et/ou de la capacité de stockage, généralement sur une base mensuelle, les coûts variant en fonction de l'utilisation, comme les coûts mensuels des services publics.

Le fournisseur du cloud est responsable du fonctionnement, la maintenance et la mise à jour du matériel informatique (par exemple, l'espace de stockage, les serveurs), qui est physiquement situé dans un centre de données et non dans les locaux du client. En tant que client, vous payez pour l'utilisation de leurs services.

guide@cyberreadinessinstitute.com

Quels sont les termes courants que je vais entendre au sujet du cloud ?

CENTRES DE DONNÉES (Data centers)

Pensez à de grands entrepôts remplis d'ordinateurs connectés à Internet et appelés communément "serveurs". Lorsque vous utilisez un service (par exemple Outlook) en tant que client vous louez essentiellement un espace (de la mémoire informatique) et des services (courrier électronique) pour écrire, lire et envoyer des courriers électroniques.

SERVEURS

Une collection d'ordinateurs et de matériel informatique connectés à l'internet qui fournissent un service qui peut être du stockage informatique ou une autre fonction.

FOURNISSEURS DE SERVICES CLOUD (CSPs, CLOUD SERVICE PROVIDER")

Les entreprises qui vous fournissent des services. Certaines entreprises bien connues sont par exemple Microsoft, Google ou Amazon Web Services (AWS).

LOGICIELS COMME SERVICE (SOFTWARE AS A SERVICE, **SAAS**) (prononcé "sass")

Un fournisseur de services cloud héberge sur ses serveurs les logiciels auxquels votre entreprise a accès par Internet. Il est courant que les entreprises accordent des licences pour l'utilisation de nombreux types de logiciels tels que les courriers électroniques (Google Mail), le traitement de texte (Microsoft Word), les tableurs (Google Sheets), la comptabilité (QuickBooks), ou la gestion des ventes (Salesforce). Il s'agit de la façon la plus commune pour les petites entreprises d'utiliser le cloud et nécessite le moins d'entretien possible pour le client.

PLATEFORME EN TANT QUE SERVICE (PLATFORM AS A SERVICE, **PAAS**) (prononcé "paz")

Un fournisseur de cloud fournit l'infrastructure (ex. un système d'exploitation comme Windows) et les logiciels qui vous permettent de développer, de gérer et d'utiliser des applications personnalisées (par exemple, des services de gestion des stocks ou de commandes mobiles de clients).

INFRASTRUCTURE EN TANT QUE SERVICE (INFRASTRUCTURE AS A SERVICE, **IAAS**) (prononcé "iyazz")

Un fournisseur de services cloud héberge physiquement des composants qui étaient traditionnellement dans un centre de données sur site, comprenant les serveurs, l'espace de stockage, les équipements d'interconnexion du réseau informatique et les logiciels du serveur.

Quels sont les avantages en matière de sécurité à déplacer les opérations et les informations dans le cloud ?

Les fournisseurs de cloud considèrent la sécurité comme une fonction commerciale essentielle et reconnaissent que la confiance est un élément fondamental de leur modèle économique. Ils se concentrent sur la mise à jour continue des services et de l'infrastructure fournis pour mettre en place des solutions sécurisées pour leurs clients. Vous bénéficiez de leur expertise et de leur souci permanent de la sécurité.

L'infrastructure physique (par exemple les serveurs, les routeurs, les dispositifs du réseau) est hébergée dans des centres de données appartenant au fournisseur et gérés par celui-ci. Cela permet généralement a.) de réduire les coûts associés à l'entretien, y compris les frais de construction et de maintenance, mais aussi b.) de disposer de ressources dédiées afin de protéger le site de dangers physiques.

Les fournisseurs de cloud permettent de réaliser des ***économies d'échelle en*** vous donnant accès à des ressources et des services qui dépassant les capacités de tout utilisateur individuel. Par exemple, les fournisseurs mettent en commun leurs ressources pour mieux comprendre les dernières cyber-attaques que les pirates informatiques utilisent afin de déployer des solutions visant à protéger leurs services et vos données.

La plupart des fournisseurs de services en cloud réputés définiront clairement les contrôles de sécurité qu'ils ont mis en place et quelles sont vos responsabilités lorsqu'il s'agit d'utiliser leur service. Si ce n'est pas le cas, ou si cette information ne provient pas du fournisseur de services cloud que vous envisagez de joindre, vous devriez vous adresser à un autre fournisseur.

Alors que nous nous dirigeons vers le cloud, quelles sont nos responsabilités en matière de cybersécurité ?

Votre responsabilité première est le comportement de vos employés. Vous êtes responsable de la formation vos collaborateurs en matière de prévention de problèmes et sur ce qu'il faut faire en cas de problème. Vous devez vous assurer qu'ils comprennent qu'être prêt pour la transition en ligne est une priorité pour votre entreprise.

Il y a des principes fondamentaux à comprendre lorsqu'il s'agit des responsabilités en matière de sécurité pour votre organisation lors de l'utilisation d'un fournisseur de services cloud :

- Premièrement, externaliser des services, des fonctionnalités ou des infrastructures à un fournisseur de cloud ne signifie pas que vous externalisez votre responsabilité en matière de sécurité. Un exemple simple qui s'applique à presque tout le monde est celui la sensibilisation et l'accès des employés. Vos employés savent-ils comment détecter les courriers électroniques suspects ? Votre organisation limite-t-elle ou restreint-elle l'accès des employés aux logiciels (par exemple, les applications comptables) en fonction des besoins et de leurs responsabilités) ?
- Deuxièmement, les agresseurs se concentrent sur la tromperie (connue sous le nom d'hameçonnage ou "phishing" en anglais) pour gagner des accès non autorisés. Plus de 90 % des piratages réussis commencent par un clic sur un lien de courrier électronique suspect. La formation des employés à la cybersécurité est large, comprenant une bonne "cyber hygiène", comme ne pas cliquer sur des liens provenant d'expéditeurs inconnus ou valider avec des cadres des courriels demandant des informations sensibles.
- Troisièmement, ce qui arrive aux données est presque toujours de la responsabilité du client. Par exemple, la fuite de données financières sensibles des clients mal protégées (pensez aux informations sur les cartes de crédit) qui est téléchargé vers un fournisseur de cloud relève de la responsabilité du client, et non du fournisseur. De plus, les conséquences en termes de réputation, de droit, de finances et de conformité, pour n'en citer que quelques-unes, relèvent également de la responsabilité du client.

Comment le passage au “cloud” améliore-t-il la sécurité liée à la gestion de l’identité des utilisateurs (par exemple, les mots de passe et l’authentification) ?

De nombreux fournisseurs de services cloud disposent d’équipes dédiées à la cybersécurité et peuvent répondre aux incidents en temps réel, en identifiant le moment où les problèmes commencent et en prenant des mesures pour atténuer l’ampleur des dommages. Un grand fournisseur de services cloud reçoit plus de 200 millions de tentatives de connexion **par jour.**

Ce fournisseur peut apprendre rapidement lorsqu’un nouveau type d’attaque menace vos mots de passe et prendre des mesures pour éviter qu’elle n’ait de répercussions sur vous ou vos utilisateurs.

Comment le passage au “cloud” améliore-t-il la préparation informatique liée à la mise à jour des logiciels ?

La mise à jour des logiciels est un avantage considérable pour les clients et constitue souvent un argument de vente clé pour les fournisseurs de services cloud, notamment lorsqu’ils proposent des logiciels ou des plateformes informatiques. Lorsque vous passez à un service cloud, le fournisseur est responsable de la maintenance des mises à jour du logiciel sans que vous ayez à faire quoi que ce soit.

Cependant, cette fonction peut avoir un inconvénient, car les utilisateurs peuvent ne pas s’adapter aux nouvelles fonctions aussi rapidement que les entreprises du cloud les déploient. Si cela s’applique à votre entreprise, vous devez demander s’il existe une **option de mise à jour différée pour v** votre licence de logiciel cloud. N’oubliez pas que les employés peuvent toujours être responsables de la mise à jour d’un logiciel qui se trouve sur leur ordinateur, tablette ou téléphone individuel.

Comment le passage au cloud améliore-t-il notre prévention face aux courriers électroniques d’hameçonnage ?

Le “phishing”(hameçonnage) est difficile à combattre car il fait appel à du piratage psychologique (parfois, spécifiquement adaptés à l’individu, appelé ***“spear-phishing” (harponnage***)) pour entrer dans une application ou accéder à des données sensibles (par exemple, les identifiants et les mots de passe).

Cela dit, les fournisseurs de messagerie électronique cloud peuvent apprendre et répondre rapidement aux attaques d’hameçonnage **une fois qu’ils sont connus**. Les fournisseurs de messagerie électronique cloud peuvent fournir des services pour aider à signaler et à empêcher les e-mails d’hameçonnage d’atteindre vos employés. En fin de compte, la meilleure ligne de défense est un ***utilisateur bien formé*** qui sait à quoi ressemblent les e-mails d’hameçonnage et ce qu’il faut faire (et ne pas faire !) lorsqu’il en voit un.

En faisant appel à un fournisseur de services en ligne, vous améliorez la capacité de votre entreprise à gérer l’identité de l’utilisateur, la mise à jour des logiciels et la prévention des courriers électroniques d’hameçonnage.

Comment le passage au cloud améliore-t-il notre sécurité face à l'utilisation de clés USB et de supports amovibles ?

Le passage au "cloud" représente une amélioration considérable, car il n'y a pas de dispositifs amovibles nécessaires pour utiliser les logiciels basés sur le cloud. Tout ce dont le cloud a besoin est un utilisateur avec un identifiant, un navigateur et une connexion internet. Les clés USB et les supports amovibles perdent toute pertinence lorsque vous formez vos utilisateurs à l'utilisation du cloud pour le stockage, le transfert et l'accès aux informations dont ils ont besoin.

Vous serez toujours responsable du maintien de la sécurité sur les dispositifs physiques, qui permettent des dispositifs amovibles et pourrait empêcher le client d'accéder à certains services. Un avantage, cependant, est que si un dispositif individuel (par exemple un ordinateur de bureau) peut être compromis par une attaque USB, les services "en direct" dans le cloud sont accessibles à partir d'un appareil non infecté. Il s'agit d'un atout du cloud puissant qui contribue à protéger la continuité de vos activités.

Comment le cloud peut-il m'aider si nous avons un incident informatique ?

Les fournisseurs de services en cloud dépensent beaucoup de temps et d'argent pour s'assurer que leurs services ne peuvent pas être détruits par un incident informatique. Les fournisseurs de cloud proposent des logiciels qui peuvent vous aider à isoler la cause première (ex. enregistrement des évènements, activités suspectes) d'un incident afin de réduire le risque qu'il se reproduise. Les centres de données disposent également d'une sécurité physique, d'une protection électrique et de contrôles de prévention des incendies solides, ce qui vous permet de vous assurer que l'infrastructure informatique physique réelle est bien protégée.

Nos employés utilisent leurs smartphones pour travailler. Comment l'utilisation de Les services en cloud m'aident à réduire le risque lié à la cybersécurité ?

Vous devez être conscient de la manière dont vos utilisateurs accèdent à vos applications, systèmes et informations. Vous devez créer une politique de sécurité mobile qui s'applique à tous les utilisateurs, quel que soit l'appareil qu'ils utilisent. Le cloud offre les mêmes avantages globaux en matière de sécurité aux employés, qu'ils utilisent leur smartphone ou un autre appareil. Il est important de rappeler que les smartphones offrent la plus grande menace et que chaque entreprise doit faire preuve de diligence dans sa politique de sécurité mobile.

À propos du Cyber Readiness Institute

Le Cyber Readiness Institute est une initiative à but non lucratif qui réunit des chefs d'entreprise de tous les secteurs et de toutes les régions géographiques afin de partager des ressources et des connaissances au sujet du développement d'outils de cybersécurité gratuits pour les petites et moyennes entreprises (PME). Le programme autodidacte Cyber Readiness est disponible en ligne en chinois, anglais, français, espagnol, portugais, arabe et japonais. N'hésitez pas à nous contacter pour toute question, commentaire ou exemple de réussite (**guides@cyberreadinessinstitute.org**).

Comment déterminer les priorités en matière de transition au cloud ?

Il n'y a pas de réponse "unique". La plupart des organisations ont ce qu'on appelle un environnement "hybride" qui utilise un mélange de services en cloud et de solutions autogérées sur site (par exemple, une entreprise peut utiliser leur réseau pour un petit bureau et un service de courrier électronique fourni par le fournisseur de service cloud). Voici quelques considérations :

- Le logiciel ou le service a-t-il une interface directe avec l'Internet ? Beaucoup d'entreprises déplacent leur courrier électronique et leurs applications de gestion de la relation client (CRM) vers le cloud, car il s'agit d'applications critiques dont les serveurs nécessitent traditionnellement beaucoup d'entretien et de maintenance. Aujourd'hui, la plupart des entreprises se procurent également leurs logiciels commerciaux de base (traitement de texte, tableurs, comptabilité) par le biais d'un abonnement de logiciel.
- A quel point cela serait-il difficile ou perturbant ? Certaines fonctions sont beaucoup plus faciles à migrer que d'autres. Par exemple, le déplacement de votre courrier électronique ou du stockage de vos fichiers vers le cloud est simple. Cependant, déplacer des systèmes comme la paie ou la comptabilité qui impliquent beaucoup de données historiques peuvent être beaucoup plus complexes.
- Quels sont les coûts relatifs ? En comparant les coûts entre l'utilisation du cloud et le fait de le faire soi-même, assurez-vous de compter également le temps et les frais de réalisation sur place. Il ne s'agit pas seulement du coût du matériel et des logiciels, mais aussi du temps nécessaire pour installer, mettre à jour, entretenir et dépanner votre système.
- Évaluer en détail les aspects de sécurité liés à utilisation du cloud. Pensez aux éventuelles perturbations pour votre entreprise ainsi qu'à la perte de vos informations - en particulier les plus précieuses.

Quel sera l'impact du passage au "cloud" sur notre flux de travail actuel et ce que nos employés doivent faire ?

La réponse à cette question dépendra de ce que vous faites dans le cloud. Le déplacement du courrier électronique vers le cloud n'entraîne généralement que très peu de changements, alors que le déplacement de votre logiciel de comptabilité vers le cloud pourrait représenter une perturbation considérable nécessitant une gestion du changement pour vos utilisateurs et votre organisation.

Quel est l'impact de l'utilisation du cloud, le cas échéant, sur la façon dont j'interagis avec mes fournisseurs et mes clients ?

La réponse est simple : cela dépend. Les entreprises utilisent le cloud pour atteindre différents objectifs à travers de projets divers. Cependant, le passage au cloud permet souvent de libérer du temps et de l'argent que vous dépenseriez en ressources informatiques (serveurs, réseaux, etc.). Dans la plupart des cas, l'utilisation du cloud rendra plus facile et plus sûr le transfert ou le partage d'informations avec vos clients et fournisseurs.