Étapes à suivre pour prévenir les violations de la sécurité 4

En 2015, plus de **25 MILLIONS D'ENREGISTREMENTS PERSONNELS,** contenant des informations allant de la couleur des yeux aux numéros de sécurité sociale, ont été dérobés au bureau gouvernemental de gestion du personnel américain. Et rien qu'au premier semestre 2016, plus de **12,8 MILLIONS D'ENREGISTREMENTS** ont été divulgués aux États-Unis.[1] Tous les points d'accès peuvent être la cible d'une cyberattaque, mais avec les bons outils, une attaque peut être bloquée avant même d'être lancée.

Les pare-feu et les programmes antivirus sont indispensables pour protéger vos données, mais pour garantir votre cybersécurité, vous devez garder une longueur d'avance sur les intrus à l'aide des quatre verrous suivants.

Confidentialité | **Conformité** | **Transparence** | **Sécurité intégrée**

Tous les secteurs sont menacés.

82 %

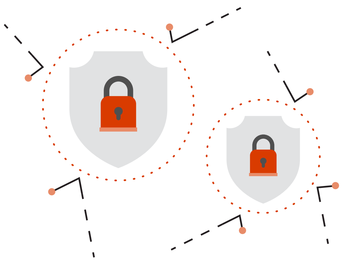
des entreprises américaines s'attendent à être la cible d'une cyberattaque dans le courant de cette année.[2]

Confidentialité 1

Les réglementations strictes du secteur d'industrie permettent aux clients des services cloud de contrôler la façon dont leurs données sont utilisées. Veillez à informer et former vos employés sur les normes les plus récentes afin de minimiser les risques de violation de la sécurité.

Dans 8 entreprises américaines sur 10,

les employés ne respectent pas les politiques de protection des données personnelles.[3]



Conformité 2

Le respect des exigences juridiques et sectorielles (telle que l'HIPAA aux États-Unis) et la gestion des risques liés à la conformité peuvent prendre du temps. Pour avoir l'esprit tranquille, n'hésitez donc pas à déléguer ces tâches à un tiers, tel que votre fournisseur de cloud.

Plus d'un tiers

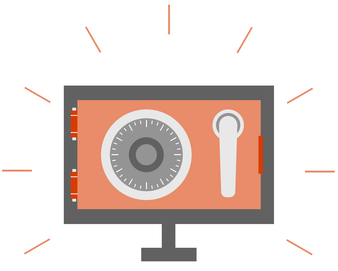
des entreprises américaines consacrent **au moins une journée par semaine** au suivi et à l'analyse des évolutions réglementaires.[4]

Transparence 3

Un contrôle total de vos données est essentiel à une bonne gestion de la sécurité. Veillez à bien contrôler vos accès afin de décider qui peut consulter vos données.

39 %

des violations de données mondiales impliquent des tiers : sous-traitants, prestataires extérieurs, consultants ou partenaires commerciaux.[5]



Sécurité intégrée 4

Les menaces accidentelles internes à votre entreprise constituent un véritable problème et peuvent vous coûter cher. Afin d'éviter les accidents, votre fournisseur de cloud doit vous fournir une technologie de protection contre la perte de données (DLP, Data Leak Protection) minimisant les risques de fuites.

575 milliards de dollars

Coût annuel de la cybercriminalité pour les particuliers et les entreprises aux États-Unis.[6]

Quels que soient les efforts déployés, la sécurité n'est jamais totalement garantie. Des cyberattaques aux accidents internes, il est très difficile de prévoir avec exactitude quelles menaces peuvent peser sur vous. Vous devez donc impérativement mettre en place les outils et systèmes adéquats pour pouvoir vous concentrer sur vos priorités.

Choisissez les fonctionnalités et les offres Microsoft Office 365 qui vous intéressent, et comparez les tarifs :

https://products.office.com/business/compare-more-office-365-for-business-plans

SOURCES :

« Hackers Dominate Big 2015 Breaches », McGee, M., 2015 [1]
« Data Breach Reports: 2016 », Identity Theft Resource Center, 2016 [2]
« Managing data security and privacy risk of third-party vendors. (n.d.). », Hertzberg, J. and Henselin, A., 2013 [3]
« Thomson Reuters 2016 Cost of Compliance Survey », Thomson Reuters, 2016 [4]
« Net Losses: Estimating the Global Cost of Cybercrime », McAfee, 2014 [5]
« The State of Data Privacy in 2015: A Survey of IT Professionals », Druva, 2015 [6]

Office 365

Microsoft