



Axel Buecker
Loïc Guézo
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Computing : guide de la sécurité

Recommandations d'IBM pour la sécurisation de l'informatique en nuage

Ce « Redpaper » présente les recommandations d'IBM pour la sécurisation de l'informatique en nuage (cloud computing). Nous commencerons par des considérations générales sur le Cloud Computing et sur la sécurité associée.

Introduction au Cloud Computing

Le Cloud Computing – ou « informatique en nuage » – est une plateforme souple, rentable et fiable permettant la fourniture de services informatiques aux entreprises et aux particuliers via Internet. Les ressources Cloud sont rapides à mettre en œuvre et offrent une grande évolutivité, l'ensemble des processus, applications et services étant fournis à la demande, indépendamment de l'emplacement des utilisateurs ou des équipements.

Le Cloud Computing permet ainsi aux organisations d'être plus efficaces dans la fourniture de services, de rationaliser leur gestion informatique et de mieux aligner leurs services informatiques sur des besoins métier en constante évolution. Il offre à la fois un solide support pour les fonctions métier stratégiques, et la capacité de développer des services nouveaux et innovants.

Remarque : Le Cloud Computing améliore en outre l'expérience des utilisateurs en masquant la complexité. Les utilisateurs n'ont pas besoin de savoir quoi que ce soit des technologies qui sous-tendent « l'informatique en nuage ».

Aujourd'hui, il existe des modèles de Cloud Computing publics et privés. Les modèles publics, accessibles à quiconque dispose d'un accès Internet, recouvrent plusieurs types de nuages : les nuages SaaS (*Software as a Service* – logiciel en tant que service), comme IBM LotusLive ; les nuages PaaS (*Platform as a Service* – plateforme en tant que service), comme Amazon Web Services ; et les nuages SDPaaS (*Security and Data Protection as a Service* – sécurité et protection des données en tant que service), comme IBM Security Event and Log Management Services.

Les clouds – ou nuages – privés sont détenus et exploités par une seule entité. Globalement, ils offrent les avantages des clouds publics tout en conférant davantage de souplesse et de contrôle à leur propriétaire.

Les clouds privés peuvent en outre présenter un temps de latence inférieur dans les périodes de pointe, où le trafic ou l'utilisation sont plus denses. De nombreuses organisations combinent les modèles privé et public dans des clouds hybrides. Conçus pour répondre à des besoins métier et techniques spécifiques, les clouds hybrides renforcent la sécurité et la protection des données personnelles moyennant un investissement minimum en coûts informatiques fixes.

Si les avantages du Cloud Computing sont évidents, il n'en est pas moins impératif de sécuriser efficacement les solutions Cloud. Dans la suite de ce document, nous allons passer en revue les principaux problèmes de sécurité qui peuvent se présenter dans les environnements de Cloud Computing. Pour finir, nous exposerons les recommandations d'IBM pour la sécurisation de l'informatique en nuage, recommandations fondées sur un ensemble de frameworks et de bonnes pratiques dans le domaine de la sécurité de l'information.

Sécurisation de l'informatique en nuage : le grand défi

En complément des problèmes habituels de sécurisation des systèmes informatiques, le Cloud Computing présente un facteur de risque supplémentaire du fait de l'externalisation de services stratégiques auprès d'un fournisseur externe. Il est en effet plus difficile, avec cette dimension d'externalisation, d'assurer l'intégrité et la confidentialité des informations, la disponibilité des données et des services, et l'établissement de la conformité à une politique ou réglementation.

De fait, le Cloud Computing transfère une grande part du contrôle sur les données et sur les opérations de l'entreprise cliente au fournisseur de services Cloud – de la même façon que les entreprises sous-traitent certaines de leurs activités informatiques à des prestataires externes. Même des activités élémentaires comme la mise en œuvre de correctifs et la configuration des pare-feux peuvent devenir de la responsabilité du fournisseur de services Cloud, et non plus de l'entreprise cliente. Ces clients doivent donc développer une relation de confiance avec leur fournisseur et bien cerner les risques liés à la façon dont ce fournisseur met en œuvre, déploie et gère leur sécurité. Cette relation de confiance entre fournisseurs et consommateurs de services Cloud est cruciale, car l'utilisateur reste le responsable ultime du respect de la réglementation et de la protection de ses informations critiques, même si ses activités ont été transférées dans l'informatique en nuage. Les risques liés à l'externalisation amènent de fait certaines organisations à préférer les clouds privés ou hybrides aux clouds publics.

D'autres aspects du Cloud Computing requièrent également une sérieuse réévaluation de la sécurité et des risques. Il est plus difficile de localiser l'emplacement physique des données stockées à l'intérieur d'un nuage. Des procédures de sécurité normalement visibles sont désormais masquées par plusieurs couches d'abstraction. Ce manque de visibilité peut entraîner des problèmes de sécurité et de conformité.

De plus, la mutualisation de l'infrastructure opérée à grande échelle dans le cadre du Cloud Computing instaure une nette disparité entre la sécurité au sein du nuage et la sécurité des environnements informatiques plus classiques. Bien souvent, des utilisateurs de différentes entreprises et de niveaux de confiance variables interagissent avec les mêmes ressources informatiques. En même temps, l'équilibrage des charges, la variété des engagements de qualité de service (SLA) et d'autres aspects des environnements informatiques dynamiques modernes accroissent les risques de mauvaise configuration, d'altération des données et de conduite malveillante.

La mutualisation de l'infrastructure nécessite une standardisation et une automatisation très poussées des processus afin d'améliorer la sécurité en éliminant les risques d'erreur et de négligence des opérateurs. Toutefois, du fait des risques inhérents à une infrastructure mutualisée à grande échelle, les modèles de Cloud Computing doivent accorder la plus grande importance aux notions de ségrégation, d'identité et de respect des règles.

Le Cloud Computing est disponible sous la forme de différents modèles de services – y compris des modèles hybrides – présentant des niveaux de responsabilité variables en matière de gestion de la sécurité. La Figure 1 décrit ces différents modèles.

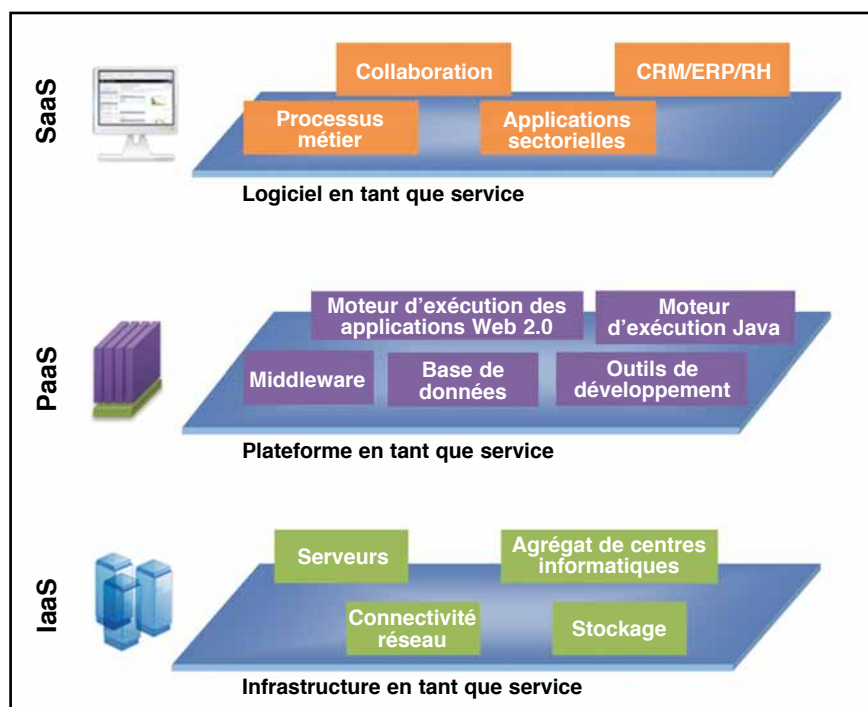


Figure 1 : Les modèles de Cloud Computing

Évaluer les différents modèles de Cloud Computing

La visibilité de l'infrastructure sous-jacente pour l'utilisateur est variable selon le modèle de Cloud Computing. Or cela conditionne le niveau de contrôle direct sur la gestion de l'infrastructure informatique ainsi que la répartition des responsabilités en termes de gestion de la sécurité.

Avec le modèle SaaS (Software as a Service – logiciel en tant que service), cette responsabilité est principalement dévolue au fournisseur des services Cloud. Le modèle SaaS fournit plusieurs méthodes pour contrôler l'accès au portail Web – gestion de l'identité des utilisateurs, configuration au niveau des applications, possibilité de restreindre l'accès à des plages d'adresses IP ou à des régions spécifiques.

Les modèles de type PaaS (Platform as a Service – plateforme en tant que service) permettent aux clients d'assumer une plus grande part de responsabilité dans la gestion de la configuration et de la sécurité des logiciels d'infrastructure (middleware), des bases de données et des environnements d'exécution des applications. Le modèle IaaS (Infrastructure as a Service – infrastructure en tant que service) concède encore plus de contrôle et de responsabilité au client, avec un accès au système d'exploitation qui prend en charge les images virtuelles, la connectivité réseau et le stockage.

Les entreprises sont intéressées par ces modèles de Cloud Computing du fait de leur flexibilité et de leur rentabilité, mais elles sont en même temps préoccupées par les questions de sécurité. Des études et des articles de presse récents sur l'adoption du Cloud Computing ont confirmé cette inquiétude devant le manque de visibilité et de contrôle, le problème de la protection des informations sensibles et le stockage d'informations réglementées dans un environnement mutualisé et géré à l'extérieur.

Remarque : L'adoption de plateformes de Cloud Computing externes mutualisées à grande échelle et totalement ouvertes pour des services informatiques critiques n'est toujours pas considérée comme une éventualité à court terme.

À court terme, la plupart des entreprises cherchent les moyens de recourir à des fournisseurs de services Cloud externes. Ces nuages serviraient avant tout pour les charges applicatives à faible risque métier, pouvant ainsi se contenter d'une approche standardisée de la sécurité offrant des garanties minimales ; le prix étant ici le critère numéro un. Pour les charges de travail à risque moyen ou élevé, concernant des informations sensibles réglementées ou propriétaires, les entreprises choisissent des nuages privés et hybrides offrant un réel niveau de contrôle et des assurances tangibles. Ces applications pourront être transférées dans des nuages externes dès lors que ces derniers commenceront à offrir une sécurité plus stricte et plus modulable.

IBM propose un cadre de référence complet qui permet de mieux appréhender la sécurité de l'entreprise (voir Figure 2). Dans le chapitre suivant, nous allons examiner ce cadre de plus près pour comprendre les différents aspects d'une architecture de sécurité globale.



Figure 2 : IBM Security Framework

IBM Security Framework

Développé pour décrire la sécurité du point de vue des ressources opérationnelles à protéger, l'IBM Security Framework couvre les différents domaines de ressources dans une perspective métier.

En nous appuyant sur ce cadre de référence de la sécurité ainsi que sur nos échanges approfondis avec nos clients, nous pouvons aujourd'hui répondre aux grands problèmes de sécurisation dans les environnements Cloud Computing d'entreprise. (Pour plus de détails, voir le document « Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security », IBM Redguide, REDP-4528.)

Gouvernance de la sécurité, gestion des risques et mise en conformité

Les entreprises ont besoin de visibilité sur la situation sécuritaire de leur informatique en nuage – et notamment sur la gestion des changements, des images et des incidents, ainsi que sur la signalisation des incidents pour les différents acteurs et pour leurs données de journalisation et d'audit.

La visibilité peut être particulièrement importante dans le contexte du respect de la réglementation. La loi Sarbanes-Oxley, la loi HIPAA (Health Insurance Portability and Accountability), les directives et lois européennes sur la protection des données personnelles et quantité d'autres réglementations exigent des fonctionnalités d'audit très complètes. Un cloud public étant par définition une boîte noire pour les utilisateurs, ces derniers peuvent ne pas être en mesure de faire état de leur conformité. Un cloud privé ou hybride, en revanche, peut être configuré pour satisfaire ces exigences.

De plus, les fournisseurs sont parfois tenus de permettre les audits par des tiers, et leurs clients peuvent être amenés à se soumettre à des recherches de preuves électroniques (e-discovery) et à des expertises légales quand une infraction est suspectée, ce qui renforce encore l'importance d'une visibilité du nuage.

De façon générale, fortes de leur expérience de l'externalisation et des services gérés classiques, les entreprises évoquent le besoin d'engagements de qualité de service (SLA) souples qui puissent s'adapter à leur situation spécifique.

Sécurité des personnes et des identités

Les entreprises doivent avoir la certitude que, d'une part, les utilisateurs autorisés au sein de l'entreprise et de la chaîne logistique ont accès aux informations nécessaires et aux outils dont ils ont besoin, quand ils en ont besoin, et que, d'autre part, les accès non autorisés sont bloqués. Ces contrôles sont d'autant plus indispensables que les environnements Cloud servent généralement à une communauté d'utilisateurs élargie très diversifiée. En outre, l'informatique en nuage introduit en outre une nouvelle catégorie d'utilisateurs privilégiés : les administrateurs qui travaillent pour le fournisseur de services Cloud. La surveillance de ces utilisateurs particuliers, et notamment la journalisation de leurs activités, revêt une grande importance. Elle doit couvrir la surveillance physique et des vérifications d'antécédents et de références.

Des capacités de fédération des identités et de connexion rapide doivent assurer la coordination des authentifications et des autorisations avec les systèmes dorsaux de l'entreprise ou les systèmes tiers. Une procédure de signature unique (SSO) fondée sur des standards simplifiera la connexion des utilisateurs aux applications internes et au cloud pour leur permettre de profiter facilement et rapidement des services Cloud.

Sécurité des données et des informations

La plupart des entreprises mentionnent la protection des données comme leur problème de sécurité majeur. Les préoccupations concernent les modalités d'accès aux données et leur stockage, les besoins de conformité et d'audit, et les problèmes liés aux intrusions éventuelles – coût, obligations déclaratives et préjudice en termes d'image. Toutes les informations sensibles ou régulées, y compris les données archivées, doivent être nettement séparées sur l'infrastructure de stockage Cloud.

Le chiffrement et la gestion des clés de chiffrement des données en transit dans le cloud ou des données qui séjournent dans le centre informatique du fournisseur de services sont essentiels pour la protection des données personnelles et le respect de la réglementation. Le chiffrement des supports de stockage mobiles et la possibilité d'un partage de ces clés de chiffrement en toute sécurité entre le fournisseur de services Cloud et le consommateur sont des nécessités importantes, mais souvent négligées. Le transfert rapide et économique de gros volumes de données via Internet n'étant toujours pas viable dans bien des cas, les entreprises doivent souvent envoyer des supports de stockage mobiles, comme des bandes magnétiques, au fournisseur de services Cloud. Il est impératif que les données soient chiffrées, et que seuls le fournisseur et le consommateur des services Cloud aient accès aux clés de chiffrement.

Le Cloud Computing peut être soumis à d'importantes restrictions quant à la colocalisation des données, selon le lieu d'implantation d'une organisation, le type de données qu'elle manipule et la nature de son activité. Plusieurs États membres de l'Union Européenne, par exemple, ont expressément réglementé le transfert à l'étranger d'informations personnelles non publiques concernant leurs ressortissants.

Remarque : Aux États-Unis, les administrations de plusieurs États n'autorisent pas la communication extraterritoriale d'informations personnelles non publiques relatives à leurs employés.

Le déploiement d'une informatique en nuage peut en outre poser des problèmes de violation des lois d'exportation en ce qui concerne les informations chiffrées et la propriété intellectuelle. L'organisation doit conduire une étude préalable approfondie de tous ces aspects juridiques et veiller à conserver le contrôle sur la localisation géographique de ses données dans l'infrastructure du prestataire.

Dans les domaines impliquant des utilisateurs et des données présentant différentes classes de risques explicitement identifiés – comme dans les services publics et financiers –, les organisations doivent entretenir une classification des données à l'échelle du cloud. Cette classification déterminera les droits d'accès, le mode de chiffrement et d'archivage des données, et les modalités de mise en œuvre des technologies pour prévenir les pertes de données.

Sécurité des applications et des processus

Les clients abordent généralement les besoins de sécurisation des applications Cloud à travers la sécurité des images. Tous les impératifs de sécurité des applications classiques restent valables pour les applications dans l'informatique en nuage, mais ils doivent également s'appliquer aux images qui hébergent ces applications. Le fournisseur de services Cloud doit suivre et prendre en charge un processus de développement sécurisé. Les utilisateurs du cloud veulent en outre des assurances sur la provenance des images et un contrôle des droits de licence et d'utilisation. La suspension et la destruction d'images doivent être effectuées avec le plus grand soin, dans le respect de la confidentialité des données sensibles contenues dans ces images.

La définition, la vérification et le maintien du niveau de sécurisation des images par rapport aux règles de sécurité spécifiques du client sont des exigences importantes, surtout dans les secteurs très réglementés. Les organisations doivent veiller à ce que les services Web qu'elles publient dans le cloud soient sûrs, et conformes à la législation et à leurs propres règles de gestion : ils doivent impérativement s'appuyer sur les bonnes pratiques du développement sécurisé.

Sécurité des réseaux, des serveurs, des postes de travail et autre point de terminaison

Dans un environnement Cloud mutualisé, les clients veulent être certains que les domaines des différents acteurs sont parfaitement étanches et qu'il n'existe aucun risque de « fuite » de données ou de transactions d'un domaine à l'autre. Ils doivent pour cela avoir la possibilité de configurer des domaines virtuels de confiance ou des zones de sécurité régies par des règles.

Dès lors que les données échappent au contrôle du client, ce dernier veut un environnement doté de systèmes de détection et de prévention des intrusions. Cet aspect ne concerne pas seulement les intrusions dans le domaine de confiance virtuel d'un client, mais aussi les risques de vol d'informations et d'extrusion – l'utilisation frauduleuse d'un domaine pour monter des attaques contre des tiers. Le transfert de données chez des fournisseurs de services augmente également les risques d'attaques par saturation (DoS) ou d'attaques par saturation distribuées (DDoS) – en interne ou via Internet.

Remarque : La sécurité de l'information étant une « cible mobile », l'environnement doit faire l'objet d'inspections régulières visant à identifier les menaces et les failles nouvellement apparues.

Dans un environnement mutualisé, toutes les parties doivent définir leurs responsabilités respectives quant au contrôle des données et effectuer de façon régulière les contrôles qui leur incombent. L'organisation doit prendre l'initiative dans la gestion du contrat pour l'évaluation des risques et le contrôle des déploiements qu'elle ne conduit pas elle-même.

Dans le cas où le fournisseur de services Cloud fournit des catalogues d'images, les clients veulent que ces images soient sécurisées et protégées efficacement contre l'altération et les fraudes. Nombre d'entre eux voudraient que ces images soient certifiées et protégées par des moyens cryptographiques.

Sécurité des infrastructures physiques

L'infrastructure du nuage informatique – serveurs, routeurs, équipements de stockage, alimentation et autres composantes qui assurent son fonctionnement – doit être sécurisée physiquement. Les dispositifs de protection peuvent comprendre le contrôle et la surveillance des accès physiques à l'aide de moyens biométriques et un système de vidéosurveillance. Les fournisseurs doivent expliquer clairement comment ils gèrent l'accès physique aux serveurs qui hébergent les applications et les données du client.

Comment mettre en œuvre un cloud sécurisé ?

Les recommandations ci-après reflètent les bonnes pratiques générales en matière de sécurisation des clouds. Toutefois, elles ne doivent pas être vues comme une garantie de réussite. Pour déterminer la meilleure approche par rapport aux besoins spécifiques de votre environnement, veuillez consulter le représentant IBM local pour les services de sécurité.

- ▶ Mettre en place et maintenir un programme de sécurisation
- ▶ Construire et maintenir une infrastructure Cloud sécurisée
- ▶ Assurer la protection des données confidentielles
- ▶ Mettre en œuvre une gestion solide des accès et des identités
- ▶ Assurer le provisionnement des applications et de l'environnement
- ▶ Mettre en place un programme de gouvernance et de gestion des audits
- ▶ Mettre en place un programme de gestion des vulnérabilités informatiques et des intrusions
- ▶ Tester et valider régulièrement l'environnement.

Mettre en place un programme de sécurisation

Un programme de sécurisation apporte la structure nécessaire pour gérer la sécurité des informations et faire face aux risques et aux menaces qui pèsent sur l'environnement cible. En cas de violation de la sécurité, ce programme fournit des informations cruciales sur la protection de l'informatique en nuage, la réponse aux menaces et détermine les responsabilités pour la gestion des événements.

1. Considérations sur la mise en place d'un programme de sécurisation

Voici des recommandations à prendre en compte dans l'élaboration d'un programme de sécurisation :

- 1.1. Évaluez et documentez la culture de l'organisation en matière de sécurité en général :
 - a. Évaluez les besoins actuels spécifiques du secteur et de l'organisation dans l'établissement de bonnes pratiques de sécurisation d'infrastructure. Aux États-Unis, par exemple, les organisations du secteur de la santé peuvent être considérées comme des « entités concernées » (covered entities) au titre de la loi HIPAA (Health Insurance Portability and Accountability Act).
 - b. Si la compétitivité de l'entreprise repose sur des secrets commerciaux, le programme de sécurisation de l'entreprise doit spécifier les règles à observer.
 - c. Si le contrôle des exportations est applicable aux données de l'entreprise, il est important de déterminer une méthodologie spécifique de mise en conformité des données.

- d. Évaluez la pertinence d'un déploiement en nuage pour chaque application envisagée. Des échanges détaillés sur les besoins de l'entreprise avec le fournisseur de services Cloud ou avec le prestataire chargé de mettre en place l'infrastructure sécurisée permettront de déterminer l'intérêt de telle ou telle offre Cloud.
- 1.2. Hiérarchisez par ordre d'importance les attributs de sécurité de votre solution Cloud.
- 1.3. Définissez et maintenez des règles et des procédures sur l'approche de l'organisation concernant les différents aspects de la sécurité des nuages :
 - a. Ces règles doivent identifier les menaces qui pèsent sur l'environnement Cloud et sur ses contenus ; elles doivent être constamment actualisées pour couvrir les nouvelles menaces.
 - b. Elles doivent identifier les principaux indicateurs à surveiller et leur fréquence d'évaluation ; ces indicateurs et ces mesures pourront être déterminés en fonction de la réglementation ou des bonnes pratiques du secteur.
 - c. Elles doivent spécifier une structure de responsabilité.
 - d. Elles doivent fournir des recommandations sur la réponse à apporter en cas de survenue d'un événement.
 - e. Les réponses recommandées doivent déterminer les actions à mener, le personnel concerné et les procédures d'escalade à suivre selon un calendrier précis.
- 1.4. Impliquez l'équipe d'encadrement chargée de la solution Cloud pour vous assurer que le projet est bien compris et qu'il reçoit le soutien nécessaire.
- 1.5. Instituez un programme de formation à l'échelle de l'organisation pour communiquer les règles de sécurité et faire en sorte qu'elles soient globalement bien comprises.
 - a. Veillez à ce que toutes les personnes ayant un rôle administratif reçoivent la formation requise.
 - b. Assurez-vous que les règles sont aisément accessibles à tous ceux qui sont responsables de leur mise en œuvre et de leur gestion.
- 1.6. Mettez en place un système indiquant de façon transparente l'état de la sécurité et la survenue d'événements anormaux.
- 1.7. Instaurez un programme d'audit.
- 1.8. Définissez un modèle d'application des règles afin d'assurer la communication des événements et la responsabilisation.
- 1.9. Établissez un programme de notification assurant la communication au personnel compétent de tout événement anormal dans des délais aussi proches que possible du temps réel.

Déployer une infrastructure Cloud sécurisée

Une infrastructure sécurisée contribue à la résilience du nuage avec l'assurance que les informations qui y sont stockées bénéficient d'une protection adéquate. Dans le cadre des préparatifs du projet, l'organisation doit veiller à ce que le fournisseur soit en mesure de répondre à toutes les spécifications opérationnelles, fasse preuve d'une parfaite compréhension des problématiques juridiques, réglementaires et sectorielles, ainsi que des besoins spécifiques du client, et qu'il ait la capacité de répondre à ces exigences de manière satisfaisante.

2. Configurez des pare-feux

La configuration des pare-feux doit suivre les recommandations ci-après :

2.1. La configuration des pare-feux doit comprendre les éléments suivants :

- a. Un processus formel de gestion des modifications des pare-feu formalisant l'approbation et la recette des changements apportés à la configuration.

- b. Installation d'un pare-feu sur chaque interface externe du réseau, et entre chaque zone de sécurité au sein du nuage.
 - c. Un schéma des interfaces réseau et des emplacements corrélé aux flux d'informations et à l'emplacement des pare-feu, et prévoyant l'activation d'environnements virtualisés et de solutions logicielles de pare-feu.
 - d. Une liste documentée et actualisée des ports et des services nécessaires à la conduite et à la continuité de l'activité. Par défaut, les ports du pare-feu seront paramétrés pour interdire les accès.
 - e. Justification et évaluation des risques pour toute exception de protocole des pare-feux ou toute définition de conception anormale.
 - f. Description des groupes, des rôles et des définitions pour la gestion logique du réseau.
 - g. Évaluation trimestrielle des configurations des pare-feux et des routeurs, et des règles en vigueur.
 - h. Standards de configuration des pare-feux et des routeurs.
- 2.2. Le pare-feu doit refuser les accès par des sources ou des applications « non fiables », et journaliser ces événements.
- 2.3. Le pare-feu doit restreindre les accès par des systèmes dotés d'une connexion externe directe et par ceux qui contiennent des données confidentielles ou des données de configuration. La configuration doit comprendre les éléments suivants :
- a. Restriction spécifique du trafic entre les ports et adresses de filtrage spécifiés.
 - b. Interdiction de l'accès direct aux zones à accès réservé du réseau à partir d'interfaces externes.
 - c. Mise en œuvre d'un filtrage dynamique des paquets.
 - d. Restriction de tout trafic entrant et sortant relatif aux informations spécifiées dans la liste des ports et des services documentée et actualisée.
 - e. Interdiction des accès sans fil directs à l'infrastructure Cloud.
 - f. Interdiction de l'accès direct à des interfaces externes par des adresses internes.
- 2.4. Dans la mesure des possibilités offertes par l'hébergeur Cloud, installez des pare-feux périmétriques entre les données confidentielles, de configuration et les interfaces externes.
- 2.5. Dans la mesure des possibilités offertes par l'hébergeur Cloud, installez des pare-feux logiciels personnels sur les équipements externes comme les ordinateurs, les équipements mobiles, etc., qui sont en interface avec l'environnement Cloud.
- 2.6. Installez des masques IP pour empêcher la présentation et l'identification des systèmes internes par des entités externes.
- 2.7. Installez un pare-feu pour isoler les informations confidentielles, et assurez-vous que toutes les informations confidentielles sont stockées en deçà du pare-feu.

3. N'utilisez pas les paramètres de sécurité par défaut (mots de passe et autres) fournis par le prestataire.

Les valeurs par défaut fournies par le prestataire pour les paramètres de sécurité tels que les mots de passe ne doivent pas être employées.

- 3.1. Changez toujours les mots de passe et les autres paramètres de sécurité fournis par le prestataire avant d'activer un serveur ou de créer des images de machines virtuelles.
- 3.2. Élaborez des standards et des recommandations de configuration Cloud pour votre organisation. Documentez ces standards et assurez-vous que votre environnement Cloud s'y conforme. Veillez à ce que ces standards soient cohérents avec les recommandations de votre secteur en matière de sécurisation.
- 3.3. Assurez-vous que chaque machine virtuelle n'implémente qu'une seule fonction primaire.
- 3.4. Aucune fonction ni aucun processus non nécessaire ne doit être actif.
- 3.5. Éliminez du système virtuel toutes les applications, tous les scripts et tous les modules non nécessaires.

4. Protégez les accès administratifs.

Tous les accès administratifs doivent être protégés par des contrôles d'accès et par une connectivité réseau sécurisée.

- 4.1. Employez des protocoles de connectivité sécurisés (SSH, SSL, IPSEC et VPN) pour toutes les activités administratives, avec une authentification bidirectionnelle.
- 4.2. Exigez un double contrôle pour tous les accès du fournisseur aux ressources du consommateur (authentification et autorisation du fournisseur et du consommateur pour les opérations).
- 4.3. Conservez une piste d'audit des activités administratives.
- 4.4. L'hébergeur Cloud doit développer et publier des recommandations pour la gestion des configurations.
- 4.5. Mettez en place un mécanisme de découverte des actifs pour identifier les ressources exploitées dans l'environnement cible.
- 4.6. Examinez régulièrement la cartographie des actifs pour cerner les ressources présentes dans l'environnement Cloud.
- 4.7. Maintenez un référentiel des données de configuration pour faciliter les audits et bien cerner la sécurité dans son ensemble.

5. Pensez à la gestion des correctifs.

Il est nécessaire de mettre en œuvre un programme de gestion des correctifs.

- 5.1. L'hébergeur Cloud doit développer et publier un programme de gestion des correctifs et des modifications.
- 5.2. Développez un système de gestion des correctifs en préproduction pour assurer la résilience de l'activité.
- 5.3. Veillez à ce que la journalisation soit activée pour tous les processus liés aux correctifs et produisez la documentation adéquate.
- 5.4. Assurez-vous que tous les systèmes et applications exécutent les plus récents correctifs fournis par le prestataire et que les mises à jour sont appliquées dans les délais spécifiés par le programme de gestion des correctifs et des modifications. Un calendrier doit être défini.
- 5.5. Instituez un processus ou faites appel à un fournisseur pour rester informé sur les failles les plus récentes.

6. Définissez un plan de sécurité pour l'environnement physique.

Il est nécessaire de mettre en place un plan de sécurité pour l'environnement physique.

- 6.1. Les locaux doivent disposer de contrôles de sécurité physique adéquats pour prévenir les accès non autorisés aux zones sensibles et l'accès aux ressources et aux systèmes physiques par des intrus ou par des utilisateurs non habilités.
- 6.2. Les références et les antécédents de tous les employés bénéficiant d'un accès direct aux systèmes doivent être vérifiés.
- 6.3. Les fournisseurs externes doivent avoir défini des règles et des procédures distinguant entre les employés et les visiteurs.
- 6.4. Le service d'hébergement doit être correctement protégé contre les catastrophes naturelles.

7. Protégez les communications hybrides.

Les communications entre les infrastructures distantes et celle de l'entreprise doivent être efficacement protégées.

- 7.1. L'infrastructure de l'entreprise ne doit être accessible qu'à travers des communications sécurisées.
- 7.2. Toutes les communications entre les infrastructures distantes et celle de l'entreprise doivent être chiffrées.
- 7.3. Les communications doivent provenir uniquement de l'infrastructure de l'entreprise.

- 7.4. L'infrastructure de l'entreprise doit être protégée par un pare-feu.
- 7.5. Toutes les communications entre les infrastructures distantes et celle de l'entreprise doivent passer par une liaison réseau dédiée.
- 7.6. Limitez le nombre des utilisateurs disposant d'un accès administratif aux infrastructures distantes et à celle de l'entreprise.
- 7.7. Prenez vos dispositions pour pouvoir utiliser des communications hors bande protégées en cas d'urgence.

Assurer la protection des données confidentielles

La protection des données est un principe fondamental de la sécurité des informations. Toutes les normes et réglementations dans ce domaine, comme la plupart des bonnes pratiques, exigent une protection adéquate des informations sensibles en vue d'en préserver la confidentialité. Et cette confidentialité est requise quel que soit l'emplacement où résident les données dans la chaîne de contrôle (chain of custody), y compris l'environnement Cloud.

8. Protégez les données personnelles.

Les données personnelles (Personally Identifiable Information – PII) doivent être gérées et protégées avec le plus grand soin.

- 8.1. Définissez et publiez des règles sur la génération, la capture, la gestion, la transmission, le stockage et la suppression des données personnelles.
- 8.2. Consultez votre service juridique sur les obligations spécifiques de votre organisation et de votre secteur.
- 8.3. Définissez une stratégie et des règles de notification et de communication d'informations sur toute faille susceptible de compromettre la confidentialité des données personnelles, dans le respect de la législation en vigueur et conformément aux réglementations et aux bonnes pratiques de votre secteur.
- 8.4. Préparez un inventaire et un schéma de classification des données personnelles.
- 8.5. Ne stockez que le minimum indispensable de données personnelles en adoptant les règles suivantes :
 - a. Définissez et appliquez une politique de conservation des données.
 - b. Détruisez de façon sécurisée toutes les données personnelles non indispensables (sous réserve des obligations légales).

9. Détruisez de façon sécurisée toutes les données personnelles non indispensables.

Les données personnelles non indispensables à l'activité doivent être détruites de façon sécurisée.

- 9.1. Masquez les données personnelles affichées quand c'est opportun (par exemple, en n'affichant qu'une partie des numéros de sécurité sociale).
- 9.2. Rendez illisibles les données personnelles où qu'elles soient stockées.
- 9.3. Veillez à ce que les données personnelles en mémoire soient illisibles et inaccessibles par des technologies des clients.
- 9.4. Les données personnelles ne doivent pas être enregistrées dans des fichiers de journalisation ou d'autres fichiers système.
- 9.5. Limitez les risques de divulgation en vous assurant que toutes les extractions de données personnelles sont journalisées.

10. Protégez les données confidentielles et stratégiques.

Définissez et appliquez une politique de protection des données confidentielles et stratégiques.

- 10.1. Définissez et publiez des règles sur la génération, la capture, la gestion, la transmission, le stockage et la suppression des données confidentielles.

- 10.2. Définissez une stratégie et des règles de notification et de communication d'informations sur toute faille susceptible de compromettre la confidentialité des données personnelles, conformément à la législation en vigueur et aux réglementations et aux bonnes pratiques de votre secteur.
- 10.3. Préparez un inventaire et un schéma de classification des données confidentielles que vous actualiserez régulièrement.
- 10.4. Ne stockez que le minimum indispensable d'informations confidentielles en adoptant les règles suivantes :
 - a. Définissez et appliquez une politique de conservation des données.
 - b. Détruisez de façon sécurisée toutes les informations confidentielles non indispensables (sous réserve des obligations légales).
- 10.5. Conduisez une étude d'impact avant de déployer des données dans le nuage en documentant et en évaluant la tolérance aux risques.
- 10.6. Interdisez tout stockage d'informations sensibles avant que l'utilisateur ne soit identifié.

11. Protégez la propriété intellectuelle.

Définissez et appliquez une politique de protection de la propriété intellectuelle.

- 11.1. Avant le déploiement d'un nuage public, l'évaluation des risques encourus par l'organisation doit inclure la propriété intellectuelle.
- 11.2. Dans le cas d'un cloud public, le service juridique de l'organisation doit veiller à ce que les engagements de qualité de service (SLA) couvrent la protection de la propriété intellectuelle.
- 11.3. Dans le cas d'un cloud public, l'organisation doit s'efforcer dans toute la mesure du possible d'opacifier la propriété intellectuelle par le chiffrement ou d'autres mécanismes afin de compliquer la tâche d'utilisateurs malintentionnés qui essaieraient de reconstituer les informations.

12. Protégez les clés de chiffrement contre toute divulgation ou utilisation frauduleuse.

Les clés de chiffrement doivent être gérées de façon sécurisée afin de prévenir toute divulgation ou utilisation frauduleuse.

- 12.1. Documentez et déployez un programme de gestion du stockage des clés couvrant les éléments suivants :
 - a. Production d'un minimum de recommandations sur le type et la longueur des clés et sur les règles applicables.
 - b. Méthode de diffusion et de gestion sécurisées des clés.
 - c. Recyclage périodique des clés (au moins tous les ans).
 - d. Méthode de destruction des clés périmées ou inactives.
 - e. Mécanisme assurant la suppression et le remplacement rapides des clés perdues ou volées.
 - f. Processus de signalisation des événements susceptibles de compromettre le secret des clés.
 - g. Prévention des remplacements de clés non autorisés.
 - h. Connaissance répartie et double contrôle des clés.
 - i. Documentation de règles relatives à l'enregistrement des informations et mise en place de mécanismes d'archivage adéquats.
- 12.2. Mettez en place un programme de gestion des clés :
 - a. Appliquez le principe du droit d'accès minimal quand vous définissez des droits d'accès à des clés.
 - b. Révissez régulièrement les droits d'accès utilisateur aux clés.
 - c. Stockez les clés dans un nombre d'emplacements aussi réduit que possible.
 - d. Enregistrez tous les accès aux clés.

13.Sécurisez les communications de données.

Instituez des règles de sécurisation pour la communication de données.

- 13.1. Définissez et publiez des recommandations sur les moyens à employer pour communiquer des données et sur les contraintes applicables.
- 13.2. Employez de solides protocoles de chiffrement et de sécurisation (tels que SSL/TLS et IPSEC) pour protéger les informations sensibles.
- 13.3. N'envoyez jamais par courrier électronique des données personnelles ou des informations confidentielles non chiffrées.
- 13.4. Utilisez un protocole réseau sécurisé pour vous connecter à un référentiel d'informations sécurisé.
- 13.5. Lors de la constitution d'archives, assurez-vous que des moyens de transport sécurisés sont employés.

14.Prévenez les pertes de données.

Mettez en place un mécanisme de prévention des fuites de données (Data Loss Prevention – DLP).

- 14.1. Mettez en place un mécanisme DLP pour prévenir les fuites d'informations accidentelles ou intentionnelles.
- 14.2. Le mécanisme DLP doit fournir des fonctions de reporting adéquates.
- 14.3. Votre solution DLP doit s'intégrer avec les règles de sécurité.

15.Protégez les informations traitées par les applications.

Assurez-vous que les applications protègent les informations qu'elles traitent.

- 15.1. Mettez en place un contrôle de la totalité du code client qui manipule des données personnelles ou sensibles, et documentez les types d'informations stockés.
- 15.2. Toutes les données personnelles et confidentielles doivent être stockées dans un format non lisible.
- 15.3. Les données personnelles et les informations sensibles stockées dans des cookies doivent être chiffrées et dans un format non lisible.
- 15.4. Interdisez le stockage de routine des clés de chiffrement sur les systèmes locaux.
- 15.5. Interdisez la mise en cache de données personnelles ou sensibles.
- 15.6. En cas d'affichage de données personnelles ou d'informations sensibles, veillez au masquage des champs présentant des données.
- 15.7. Interdisez le stockage de données sensibles sous la forme de variables constantes au sein de l'application.
- 15.8. Recherchez régulièrement les failles éventuelles des applications Internet.

Mettre en œuvre une solide gestion des accès et des identités

La gestion des accès et des identités est cruciale pour la sécurité du cloud. Elle permet de limiter l'accès aux données et aux applications aux seuls utilisateurs autorisés.

16.Adoptez le principe du droit d'accès minimal.

Veillez à ce que les utilisateurs aient des droits d'accès adéquats, avec des mécanismes d'accès sécurisés.

- 16.1. Évaluez régulièrement la liste des droits d'accès utilisateurs pour vérifier que seuls les niveaux appropriés sont accordés et que seul le personnel autorisé a accès aux systèmes.
- 16.2. Définissez des règles pour les systèmes multi-utilisateurs en restreignant les accès selon les compétences et le rôle de chacun.
- 16.3. Avant d'accorder un accès, les systèmes doivent vérifier l'identité de tous les utilisateurs par rapport à une liste de droits d'accès validée.

- 16.4. Installez un mécanisme d'identification validé.
- 16.5. Définissez un accès avec authentification multi-facteur pour tous les systèmes, y compris les systèmes administratifs.
- 16.6. Pour l'accès aux fonctions administratives, faites appel à des technologies VPN (réseau privé virtuel) assurant l'identification du numéro appelant ou l'identification des utilisateurs distants (SSL/TLS et IPSEC), avec des certificats individuels.
- 16.7. Chiffrez tous les mots de passe lors des transmissions et des activités de stockage.
- 16.8. Suivez les recommandations ci-après pour vous assurer qu'il existe des fonctions efficaces de gestion des authentifications et des mots de passe sur tous les composants des systèmes :
 - a. Contrôlez la gestion des informations relatives aux identifiants utilisateurs.
 - b. Vérifiez l'identité de l'utilisateur avant toute modification ou réinitialisation d'un mot de passe.
 - c. Exigez des utilisateurs qu'ils changent de mot de passe dès leur premier accès à l'application.
 - d. Révoquez rapidement les droits d'accès des utilisateurs radiés.
 - e. Supprimez régulièrement les comptes inactifs (au moins tous les 30 jours).
 - f. Documentez les règles relatives aux mots de passe et aux identifiants, et formez les employés sur les recommandations à suivre.
 - g. Les mots de passe des fournisseurs et de l'hébergeur doivent être activés uniquement pendant les périodes de maintenance.
 - h. Proscrivez les comptes ou mots de passe collectifs, partagés ou génériques.
 - i. Les utilisateurs doivent changer leur mot de passe à des intervalles prédéfinis (30, 60 ou 90 jours).
 - j. Exigez des mots de passe utilisateurs complexes contenant des caractères alphabétiques et numériques.
 - k. Limitez la réutilisation des mots de passe (par exemple, pas de réutilisation des trois derniers mots de passe).
 - l. Limitez le nombre d'erreurs de mot de passe auquel a droit l'utilisateur avant d'être rejeté par le système.
 - m. Définissez un délai d'expiration après inactivité pour tous les systèmes quand l'accès à des données confidentielles exige qu'un utilisateur s'identifie une seconde fois auprès du système.
 - n. Mettez en œuvre une règle de verrouillage soit temporelle, soit requérant une réactivation (sous la forme d'une fonction de service).

17. Mettez en place une gestion fédérée des identités.

La fédération des identités permettra de sécuriser les échanges d'informations sur les identités.

- 17.1. Instituez une gestion fédérée des identités dans le cadre de l'interconnexion des environnements Cloud.
- 17.2. La fédération des identités doit s'accompagner de la mise en place d'un système de confiance pour les identités afin de prévenir toute usurpation d'identité.

Assurer le provisionnement des applications et de l'environnement

Dans un environnement Cloud dont la gestion est centralisée, il est essentiel de mettre en œuvre une fonctionnalité de provisionnement automatisée.

18. Mettez en place un programme de provisionnement des applications.

Développez un programme de provisionnement des images et des applications.

- 18.1. Un processus validé doit assurer le provisionnement des images virtuelles.
- 18.2. Le système de provisionnement doit appliquer des droits d'accès lors du provisionnement.

- 18.3. La gestion du provisionnement doit comporter les contrôles de sécurité et d'autorisation adéquats.
- 18.4. Les activités de dé-provisionnement des applications et des images virtuelles doivent être journalisées.
- 18.5. Toutes les modifications concernant les accès aux applications et aux images virtuelles doivent être journalisées.
- 18.6. Contrôlez régulièrement l'accès au système de gestion du provisionnement pour vérifier qu'aucune règle ne déroge au droit d'accès minimal.
- 18.7. Déployez un mécanisme pour gérer la destruction des images virtuelles obsolètes ou non valides.

Mettre en place un programme de gouvernance et de gestion des audits

Pour vous préparer aux audits réglementaires ou internes, vous devez mettre en œuvre un programme définissant où, quand et comment collecter les informations de journalisation et d'audit.

19. Instituez un programme pour gérer la protection des données personnelles.

- 19.1. Ce programme de gestion de la protection des données personnelles doit répondre à plusieurs caractéristiques :
 - a. Déterminez les données personnelles et les informations confidentielles qui existent et sont gérées.
 - b. Priorisez les données personnelles et les informations confidentielles en termes de risques et d'impact de la réglementation.
 - c. Définissez des règles sur l'utilisation, la conservation, la modification et la suppression des données personnelles et des données confidentielles.
 - d. Impliquez la direction et l'encadrement dans la validation de ce programme.
 - e. Mettez en place un processus pour surveiller le respect des règles et les entorses.
 - f. Établissez un programme de formation sur les règles.
 - g. Instaurez un programme d'audit des règles.
 - h. Définissez des règles pour l'application et le suivi du programme.
 - i. Établissez un programme/processus de notification des parties concernées en cas d'incident.
- 19.2. Ajoutez les données personnelles à la cartographie de référence des données pour permettre aux auditeurs et aux administrateurs d'identifier les menaces qui pèsent sur l'environnement Cloud.

20. Mettez en place des mécanismes de capture et de gestion des audits.

Instituez un programme de gestion des audits et des dossiers.

- 20.1. Avec l'aide de votre service juridique, identifiez et documentez toutes les obligations légales et réglementaires applicables à chaque instance Cloud.
- 20.2. Définissez ensuite des règles de capture et de conservation des documents légaux et réglementaires.
- 20.3. Procédez à une inspection régulière des informations conservées.
- 20.4. Instaurez un programme d'audit pour vérifier la mise en œuvre des règles de capture et de conservation des audits.
- 20.5. Assurez-vous que tous les documents légaux et réglementaires requis sont collectés.

21.Documentez la protection des données et la conformité à l'étranger.

Définissez des règles pour vous assurer que les données sont manipulées et stockées dans le respect des réglementations et des obligations de protection en vigueur à l'étranger.

- 21.1. Avec votre service juridique, passez en revue toutes les lois régionales, nationales et internationales applicables pour déterminer les obligations relatives au transfert et à l'utilisation du stockage par les consommateurs et les hébergeurs du nuage.
- 21.2. Documentez les règles et les procédures relatives aux lois et réglementations régionales, nationales et internationales qui concernent votre activité :
 - a. Où stocker les données, en fonction des contenus et du consommateur de l'information.
 - b. Qui a accès aux données, en fonction des contenus et du consommateur de l'information.
 - c. Quelles protections (chiffrement, ségrégation, etc.) mettre en place pour protéger les données compte tenu des lois et réglementations régionales, nationales et internationales qui concernent votre activité.
- 21.3. Avec votre service juridique, passez régulièrement en revue les lois et réglementations applicables à la création, au stockage, à la transmission et à la destruction de données dans le cadre des protections requises à l'étranger.
- 21.4. Quand l'autorisation de la personne concernée est requise, veillez à conserver une trace de l'obtention de cette autorisation.
- 21.5. Assurez-vous que les personnes chargées de traiter les données ont connaissance des procédures et des contraintes applicables aux informations sensibles.

Mettre en place un programme de gestion des failles et des intrusions

Dans un environnement Cloud de confiance, vous devez mettre en œuvre un programme et des mécanismes rigoureux de gestion des failles, notamment des systèmes de détection et de prévention des intrusions, pour que les ressources informatiques (serveurs, réseau, composants de l'infrastructure et points de terminaison) soient sous surveillance permanente.

22.Installez et actualisez régulièrement des programmes antivirus/anti-logiciel espion et des systèmes de détection/prévention des intrusions.

L'environnement doit être protégé par la recherche des failles, par des antivirus et par des mécanismes de détection et de prévention des intrusions.

- 22.1. Déployez des logiciels antivirus sur tous les systèmes pris en charge qui pourraient être exposés aux attaques de virus ou de logiciels espion.
- 22.2. Les programmes choisis doivent être capables de protéger les systèmes contre les logiciels ou les processus malveillants en identifiant et en isolant ou en éliminant les menaces.
- 22.3. Définissez des règles de classification des machines en fonction des protocoles de gestion antivirus.
- 22.4. Tous les mécanismes de protection doivent être à jour et actifs, et pouvoir générer des journaux.
- 22.5. Recourez à des systèmes de détection/prévention des intrusions sur le réseau et sur le système central pour assurer une surveillance active de l'environnement Cloud et alerter le personnel en cas de tentative d'intrusion.
- 22.6. Tous les moteurs des systèmes de détection/prévention des intrusions doivent être constamment actualisés.
 - a. Vérifiez que des systèmes de détection/prévention des intrusions sont utilisés et que la totalité du trafic de l'environnement Cloud est sous surveillance.
 - b. Vérifiez que les systèmes de détection/prévention des intrusions sont configurés pour alerter le personnel en cas de tentative d'intrusion.

Tester et valider régulièrement l'environnement

Vous devez employer différents mécanismes de test et de validation pour préserver l'intégrité de l'environnement Cloud.

23. Mettez en place un processus de gestion des modifications.

Définissez et mettez en œuvre un processus de gestion des modifications.

- 23.1. Vous devez mettre en place un processus documenté de gestion des modifications des configurations.
- 23.2. Le processus de gestion des modifications des configurations pour les systèmes et les logiciels du nuage doit prévoir :
 - a. La journalisation des demandes de modification.
 - b. Le résultat de l'analyse d'impact.
 - c. Les résultats des tests de préproduction et la validation.
 - d. Le processus de retour à l'état antérieur.

24. Mettez en place un programme de chiffrement des données et d'accès aux informations.

Mettez en place un programme testant la protection des données stockées.

- 24.1. Testez les bases de données et les autres moyens de stockage pour vérifier l'efficacité de leur protection et la mise en œuvre des niveaux de chiffrement adéquats.

25. Mettez en place un programme de développement et de test sécurisés des applications.

Vous devez mettre en place un programme de développement et de test sécurisés des applications.

- 25.1. Appuyez-vous sur les bonnes pratiques pour le développement des applications logicielles, la sécurité formant une composante importante du projet.
 - a. Tous les correctifs de sécurité doivent être validés avant le déploiement en production.
 - b. Les environnements de test et de production doivent être séparés.
 - c. Veillez à la séparation des tâches pour le personnel chargé des tests, du développement et de l'administration.
 - d. N'utilisez jamais dans un environnement de test des données de production contenant des informations confidentielles ou des données personnelles.
 - e. Toutes les données de test et d'administration doivent être supprimées de l'environnement de test avant le passage en production.
 - f. Tous les comptes de test et les comptes personnalisés doivent avoir été supprimés avant l'activation de la production.
 - g. Vérifiez la sécurité de la totalité du code avant le lancement en production.
- 25.2. Développez toutes les applications Web conformément aux recommandations de sécurité fournies par IBM, l'Open Web Application Security Project, etc. Contrôlez régulièrement le code pour repérer les failles courantes, notamment :
 - a. Entrées non validées.
 - b. Contrôles d'accès défaillants ou inopérants.
 - c. Gestion des identifications et des sessions défailante ou inopérante.
 - d. Failles de type XSS (cross-site scripting).
 - e. Failles de type débordement de tampon (buffer overflow).
 - f. Failles de type injection (SQL, LDAP, etc.).
 - g. Gestion des erreurs inefficace ou inexistante.
 - h. Méthodes ou technologies de stockage non sécurisées.
 - i. Gestion non sécurisée des configurations.
 - j. Exposition aux attaques par saturation.

- 25.3. Éliminez du code de production toutes les instructions de trace et de débogage.
- 25.4. L'application ne doit pas comporter d'erreurs dans l'énumération des noms.
- 25.5. Toutes les applications reliées à Internet doivent être protégées contre les attaques connues par l'un des mécanismes suivants :
 - a. Installation d'un pare-feu pour les applications.
 - b. Recherche des failles de sécurité des applications par un prestataire de confiance.
- 25.6. Mise en œuvre d'un programme de surveillance et de test du réseau.
- 25.7. Vous devez disposer d'un processus associant chaque identifiant unique avec les différentes activités, en particulier les tâches administratives.
- 25.8. Les pistes d'audit doivent couvrir tous les événements, notamment :
 - a. Les tentatives de connexion non valides.
 - b. Les tentatives d'accès au titre d'activités d'administration.
 - c. Tous les événements concernant l'accès à des informations confidentielles ou à des données personnelles.
 - d. Tout accès aux fonctions système ou aux pistes d'audit.
 - e. L'activation ou l'arrêt de fonctions ou de processus système.
 - f. Toutes les activités administratives.
 - g. L'activation ou l'arrêt de systèmes virtuels.
- 25.9. Enregistrez au minimum les informations suivantes :
 - a. Identifiants utilisateurs.
 - b. Heure de l'événement.
 - c. Description de l'événement.
 - d. Origine de l'événement (si l'information est pertinente).
 - e. Succès ou échec de l'événement.
 - f. Entité concernée.
- 25.10. Vérifiez que toutes les pistes d'audit sont sécurisées.
- 25.11. Limitez l'accès aux fonctions administratives.
- 25.12. Si possible, chiffrez les pistes d'audit.
- 25.13. Assurez-vous que les pistes d'audit sont sauvegardées régulièrement.
- 25.14. Mettez en place des mécanismes de surveillance des fichiers et de détection des altérations pour déterminer les modifications de fichiers illicites.
- 25.15. Vérifiez que les horloges sont synchronisées.
- 25.16. Conservez l'historique des pistes d'audit pendant au moins un an, ou pendant la durée requise par la législation en vigueur.
- 25.17. Testez la validité des contrôles de sécurité à l'aide d'outils vérifiant les points de terminaison par rapport aux menaces.
- 25.18. Testez les applications avant leur déploiement à l'aide d'outils de validation des applications et des services disponibles sur le marché.
- 25.19. Conduisez des tests d'intrusion au moins une fois tous les 90 jours pour repérer toute nouvelle faille dans votre environnement Cloud.
- 25.20. Déployez des solutions de surveillance de l'intégrité des fichiers pour identifier l'introduction de code malveillant.

En résumé

Le Cloud Computing offre aujourd'hui aux organisations un moyen efficace, évolutif et économique de fournir des services informatiques aux professionnels ou aux particuliers via Internet. Différents modèles de Cloud Computing peuvent être mis en œuvre pour prendre en charge des fonctions métier stratégiques, avec la souplesse nécessaire pour proposer de nouveaux services.

La flexibilité et l'ouverture des modèles de Cloud Computing font cependant peser une série de risques sur la sécurité. Quantité de ressources informatiques sont partagées par de nombreux utilisateurs, et les procédures de sécurité sont souvent masquées par plusieurs couches d'abstraction. Surtout, le Cloud Computing étant souvent fourni sous la forme d'un service, le contrôle des données et des opérations est confié à des prestataires externes. Par conséquent, les clients doivent instaurer des relations de confiance avec leurs fournisseurs et développer des solutions de sécurisation qui tiennent compte de cette relation.

Ce guide a pour vocation de servir de référence pour la sécurisation de l'informatique en nuage. Nous y avons examiné les principaux problèmes de sécurité qui se posent aux fournisseurs de services Cloud et à leurs clients, et présenté des recommandations concrètes pour la mise en œuvre de contrôles de sécurité fondés sur des cadres de référence (frameworks) et des bonnes pratiques reconnus.

Les auteurs du Redpaper IBM

Ce document est le fruit d'un travail d'équipe entre des experts de plusieurs continents réunis à l'ITSO (International Technical Support Organization) du Centre d'Austin.

Axel Buecker est Certified Consulting Software IT Specialist auprès de l'ITSO de l'Austin Center. Il rédige de nombreuses publications et dispense des formations dans le monde entier sur l'architecture de sécurité logicielle et sur les technologies d'informatique en réseau. Titulaire d'un diplôme en science informatique de l'université de Brême en Allemagne, il possède 23 ans d'expérience dans divers domaines liés à la gestion des postes de travail et des systèmes, à l'informatique en réseau et aux solutions e-business. Avant d'intégrer l'ITSO, en mars 2000, Axel était Senior IT Specialist en architecture de sécurité logicielle chez IBM Allemagne.

Koos Lodewijkx est responsable de portefeuille dans l'équipe IBM Corporate Security Strategy, où il coordonne l'élaboration de la stratégie de sécurité pour les différentes marques IBM. Il est entré chez IBM en février 2007, après le rachat par IBM de Consul Risk Management, un leader dans le secteur du développement et de la mise en œuvre de solutions de gestion de mise en conformité. Chez Consul, Koos a occupé plusieurs postes à responsabilité et dirigé la ligne de produits de reporting d'audit et de conformité.

Harold Moss est Emerging Technologies Architect dans l'équipe IBM Corporate Security Strategy. Sa mission consiste à apporter un éclairage technique sur les nouvelles orientations des technologies de sécurisation et sur les technologies existantes. Il a été chargé de vérifier et de valider l'approche architecturale de plusieurs solutions Cloud et Web 2.0 en vue d'en assurer l'adéquation aux besoins des clients et à d'autres actifs IBM. Harold, qui est aujourd'hui membre de plusieurs comités d'architecture IBM, œuvre activement pour le développement des offres dans le domaine des technologies Cloud et Web 2.0.

Kevin Skapinetz est le responsable du portefeuille Sécurité SaaS chez IBM Internet Security Systems (ISS). Il est à ce titre chargé de définir et de mettre en œuvre les orientations stratégiques des offres « sécurité en tant que service » d'IBM. Avec dix ans d'expérience dans la sécurité de l'information, dont sept chez ISS, Kevin a occupé d'importantes fonctions dans les domaines de la stratégie, de l'ingénierie et du support. Il a récemment joué un rôle central à la Direction technique en tant que stratège chargé d'éclairer la stratégie de l'entreprise à l'égard des technologies émergentes, notamment la sécurité dans les environnements de virtualisation et de Cloud Computing. Il a également été pendant plusieurs années Lead Software Engineer pour RealSecure Server Sensor, un système multiplate-forme de prévention des intrusions hôte. Kevin est titulaire d'un diplôme en science informatique de l'université de Tulane et d'une maîtrise en sécurité de l'information du Georgia Institute of Technology.

Michael Waidner a obtenu en 1991 un doctorat en science informatique de l'université de Karlsruhe en Allemagne. Après avoir passé quelques années dans cette même université en tant que chercheur et conférencier, il est entré en 1994 au laboratoire d'IBM Research de Rüschlikon en Suisse, où il a constitué et dirigé l'une des meilleures équipes de recherche du monde sur la sécurité industrielle. Sous sa direction, cette équipe a apporté de nombreuses contributions fondamentales à la science et aux offres de produits et de services d'IBM dans des domaines tels que la cryptographie, la tolérance aux pannes dans les systèmes distribués, la gestion fédérée des identités, la protection des données personnelles en entreprise, la gouvernance en matière de sécurité et la gestion des risques. En 2006, Michael a rejoint l'IBM Software Group à New York. En 2007, il a piloté la création de l'IBM Security Architecture Board, chargé de déterminer la stratégie architecturale et technique en matière de sécurité pour l'ensemble de la compagnie IBM. Michael, qui préside ce comité depuis le début, en a fait l'organe central d'IBM dans le domaine des technologies de sécurité virtuelles. Il est l'auteur ou le co-auteur de plus de 110 publications scientifiques. Membre de l'IBM Academy of Technology, il est Fellow de l'IEEE et Distinguished Scientist de l'ACM.

Merci aux personnes suivantes pour leur contribution à ce projet :

Wade Wallace

International Technical Support Organization, Austin Center

Calvin Powers, Steven Bade, Marne Gordan, Latha Maripuri, Mari Heiser, Harriet Pearson, Ellen Dulburger, Stephen Mortinger, Tony Nadalin, Ana Lacovetta, Ayomi Burge, Anna Coffey, Annette Miller, David Boloker, Adi Sharabani, Mary Ellen Zurko, Kristof Klockner, Kristin Lovejoy, Christopher Bauserman, Omkhar Arasaratnam, Heather Hinton, Steve Wojtowecz, **IBM**

Loïc Guézo est diplômé de l'Université Paris XIII (1988) et d'un Mastère spécialisé de l'École Centrale Paris (2001). Il a débuté comme Ingénieur d'étude chez Sagem Sécurité pour l'OTAN avant de fonder une startup Sécurité en 1988. Après son Service National en qualité de Scientifique du Contingent à la DCSEA, il rejoint l'Agence Française de Développement (banque spécialisée) en 1993 comme Responsable Informatique Outre-Mer, puis occupe différentes fonctions (IT Manager dans les secteurs du travail temporaire, industrie pharmaceutique) avant d'obtenir un Mastère Spécialisé «Open Source et Sécurité» à l'ECP en 2001. Il rejoint alors IBM Global Services en qualité d'architecte Sécurité, spécialiste d'infrastructure IT.

En 2004, il est certifié IBM Security Architect ; en 2006, il est Consultant Manager au sein d'IBM Global Services, certifié CISSP et LA 27001.

Depuis le rachat de ISS (Internet Security Systems) en octobre 2006 par IBM, Loïc est directeur technique de l'offre IBM Security Solutions, spécialiste de cybercriminalité, détection et réaction aux attaques informatiques, lutte contre la fuite d'informations et à ce titre, correspondant national de la X Force IBM ISS (service R&D Sécurité d'IBM, CERT IBM).

Professionnel des normes PCI DSS et ISO/IEC 27001:2005 qu'il promeut et pratique régulièrement avec son équipe d'auditeurs, Loïc est, depuis 2009, représentant d'IBM France au sein de l'AFNOR SC27 «Sécurité des Systèmes d'Information». Il est par ailleurs membre du Conseil d'Administration et fondateur du Club27001 France (www.club-27001.fr).

Notices

Ce document a été conçu pour des produits et des services proposés aux États-Unis.

IBM n'offre pas nécessairement dans d'autres pays les produits, les services ou les caractéristiques présentés dans ce document. Veuillez contacter IBM pour connaître les produits et les services disponibles dans votre pays. Une référence à un produit, à un programme ou à un service IBM n'implique pas que seul ce produit, ce programme ou ce service puisse être employé. Tout autre produit, programme ou service aux fonctionnalités équivalentes peut être utilisé à leur place dès lors qu'il n'enfreint pas les droits de propriété intellectuelle d'IBM. Il appartient aux utilisateurs d'évaluer et de contrôler le fonctionnement de tout produit, programme ou service non IBM.

IBM peut avoir déposé des brevets ou des demandes de brevets sur les sujets traités dans ce document. La fourniture de ce document ne vous donne aucun droit de licence en relation avec ces brevets. Pour toute demande d'informations concernant une licence, veuillez contacter par écrit :

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 États-Unis.

Le paragraphe qui suit ne concerne pas le Royaume-Uni ou tout autre pays dans lequel cette disposition n'est pas compatible avec la législation en vigueur : IBM FOURNIT CETTE PUBLICATION « EN L'ÉTAT », SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, Y COMPRIS UNE QUELCONQUE GARANTIE IMPLICITE D'APTITUDE À LA COMMERCIALISATION, D'ADÉQUATION À UN USAGE PARTICULIER OU DE NON-CONTREFAÇON. La présente exclusion de garantie n'est applicable que dans les pays où elle ne contrevient pas à la législation en vigueur.

Cette publication peut contenir des erreurs techniques ou typographiques. Des modifications sont apportées régulièrement aux informations contenues dans cette publication ; ces modifications seront intégrées dans les futures éditions. IBM se réserve le droit d'apporter, à tout moment et sans préavis, des améliorations et/ou des modifications aux caractéristiques des produits et/ou des programmes mentionnés dans cette publication.

Toute référence à des sites Web non IBM n'est fournie qu'à titre informatif et ne constitue en aucune façon une recommandation de ces sites Web. Les éléments présentés sur ces sites Web sont étrangers aux éléments relatifs à ce produit IBM et l'utilisation de ces sites est aux risques du lecteur.

IBM peut utiliser ou diffuser les informations que vous fournissez de la façon qui lui paraîtra appropriée sans aucune obligation à votre égard.

Les informations concernant les produits non IBM ont été obtenues auprès des fournisseurs de ces produits, à travers les annonces qu'ils ont publiées ou par d'autres sources publiquement disponibles. IBM n'a pas testé ces produits et ne peut confirmer leurs performances, leur compatibilité ni aucune autre information les concernant. Les questions sur les caractéristiques des produits non IBM doivent être adressées aux fournisseurs de ces produits.

Cette publication contient des exemples de données et d'états employés dans des opérations courantes. Pour les rendre plus éloquentes, nous avons inclus des noms de personnes, d'entreprises, de marques et de produits. Tous ces noms sont fictifs, et toute ressemblance avec des noms existant dans des entreprises réelles ne serait que pure coïncidence.

DROITS DE COPYRIGHT :

Ce document contient des exemples de programmes d'application en langage source illustrant des techniques de programmation sur différentes plates-formes d'exploitation. Vous avez le droit de copier et de diffuser gratuitement ces exemples sous quelque forme que ce soit à des fins de développement, d'utilisation, de commercialisation ou de diffusion de programmes d'application conformes à l'interface de programmation d'applications conçue pour la plate-forme d'exploitation pour laquelle les exemples ont été rédigés. Ces exemples n'ont pas été totalement testés dans toutes les conditions. IBM ne peut par conséquent fournir aucune garantie quant à la fiabilité, à la maintenabilité ou à la fonctionnalité de ces programmes.

© Copyright International Business Machines Corporation 2009. Tous droits réservés.

Note sur les droits des utilisateurs membres de l'Administration des États-Unis –

Utilisation, reproduction et diffusion régies par le « GSA ADP Schedule Contract » signé avec IBM Corp.

Le document REDP-4614-00 a été créé ou mis à jour le 2 novembre 2009.



Pour nous adresser vos commentaires :

- Utilisez le formulaire en ligne « **Contact us** » présent sur les pages relatives aux Redbooks : ibm.com/redbooks
- Envoyez un e-mail à : redbooks@us.ibm.com
- Envoyez un courrier à :
IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400 États-Unis



Marques

IBM, le logo IBM, ibm.com, Redguide, Redpaper, Redpapers et le logo Redbooks sont des marques d'International Business Machines Corporation aux États-Unis ou dans d'autres pays. Les symboles ® ou ™ attachés à la première occurrence de ces marques et d'autres marques IBM indiquent des marques détenues aux États-Unis par IBM au moment de la publication de ces informations. Ces marques peuvent également être déposées dans d'autres pays. La liste des marques IBM est disponible sur Internet sous la rubrique «Copyright and trademark information», à l'adresse www.ibm.com/legal/copytrade.shtml.

Les marques suivantes sont des marques d'International Business Machines Corporation aux États-Unis et/ou dans certains autres pays :



Les autres noms de société, de produit et de service peuvent appartenir à des tiers.