∞drive

DSI-RSSI : La sécurité, un critère de sélection capital dans la mise en œuvre de votre cloud privé

Sommaire

01

Le cloud computing : état des lieux

Le cloud computing : état des lieux

Après deux années de pandémie et d'évolution des modèles collaboratifs, la plupart des organisations ont désormais intégré le cloud à leur fonctionnement afin de répondre aux impératifs de continuité d'activité, même à distance.

Après cette période de migration rapide, associée à la mise en place d'outils d'analyse et de détection des cyberattaques, se posent désormais, pour les DSI, plusieurs questions en résonance avec l'actualité.

Comment gérer ses SI dans le cloud tout en assurant la sécurité des données sensibles, en rationalisant le stockage des données, en se protégeant des cyberattaques et en optimisant les fonctionnalités métier ?

Le respect du RGPD, les enjeux écologiques et les nécessités économiques demeurent également au cœur des nouvelles approches des SI.

1.1 Tendances 2023 : vers un cloud agile, optimisé et cyber-résilient

En 2023, certaines tendances émergent clairement pour répondre à ces nouvelles problématiques. La question n'est plus tant d'intégrer le cloud à ses SI mais d'affiner au maximum son besoin pour adopter une solution parfaitement adaptée avec :

- **De nouvelles stratégies de stockage agiles afin d'éviter des réplications de données inutiles et limiter les coûts**
- **Une vision protectrice de la cybersécurité au-delà de la prévention et de la détection des menaces, pour mettre en place des schémas réactifs de type protection – sauvegarde – restauration en cas d'attaque.**
- **Des offres cloud qui s'adaptent mieux à l'agilité et aux exigences de sécurité comme : la réplication décentralisée, le verrouillage d'objets, et l'immuabilité des données**
- **L'application de pratiques de cyber-résilience en écho avec les directives européennes. La stratégie de cybersécurité de l'entreprise devient un système global de gestion des risques, à même d'assurer la continuité des opérations en cas de sinistre ou d'attaque.**
- **Une approche toujours plus sectorielle du cloud par type d'activité afin de fournir les réponses appropriées en termes de sécurité et d'optimisation des coûts**

1.2 Public ou privé, hybride ou multicloud : des solutions différentes selon les usages

En France comme ailleurs, la majeure partie des entreprises a entamé une migration vers le cloud pour rester compétitives et harmoniser l'environnement technologique des collaborateurs, qu'ils soient nomades ou sédentaires.

Mais il est important de bien différencier chaque type de cloud en fonction de ses besoins réels. Le choix va dépendre du niveau de plusieurs paramètres : la criticité des données, les besoins collaboratifs, la structuration de l'entreprise, les applications métier etc.

Cloud public : un attrait économique et une grande souplesse

Le cloud public demeure le choix de la facilité et de la disponibilité : les ressources sont détenues et exploitées par un prestataire tiers, les serveurs et applicatifs sont mutualisés.

Il permet de faire face aux pics d'activités et ne nécessite aucun frais d'infrastructure ou de maintenance.

Les plateformes de cloud public, évolutives et économiques, présentent toutefois des limites en termes de sécurité des données, de personnalisation, de support et de maîtrise globale de l'environnement. On ne saurait les privilégier si l'on souhaite être en conformité avec les normes internationales de sécurité ou que l'on évolue dans un secteur d'activité critique.

Cloud privé : le cloud sécurisé

La conformité réglementaire et le souci de la protection des données poussent donc souvent les entreprises à faire le choix du cloud privé.

Avec des serveurs et des boîtiers de chiffrement HSM dé-

diés, les entreprises bénéficient d'une totale confidentialité des données et d'un système individualisé, isolé des autres entreprises.

Le cloisonnement physique et la qualité de service en font le cloud de référence pour toutes les organisations manipulant des données sensibles et très confidentielles.

Une infrastructure dédiée et un haut niveau de service pour une tranquillité d'esprit et une sécurité optimale.

Cloud hybride, un compromis intéressant, une mise en oeuvre complexe

De plus en plus plébiscitée par les entreprises, la solution hybride qui consiste à utiliser les deux types de cloud, l'un public et mutualisé, l'autre privé et dédié, présente clairement des avantages.

L'organisation bénéficie de la souplesse de l'un et des aspects sécuritaires de l'autre en fonction du caractère confidentiel des activités, des applicatifs et des données échangées.

Parvenir à une gestion cohérente de l'ensemble n'est pas évidente pour les DSI qui doivent clarifier au maximum leur stratégie et savoir la faire évoluer au gré des innovations technologiques, des nouveaux usages et des besoins collaboratifs.

Multicloud : une approche multiservices

Contrairement au cloud hybride, le multi-cloud se base sur un seul choix, cloud privé ou cloud public, mais sur une variété de services et prestataires et sur un déploiement de solutions différenciées, sans interconnexion.

Le multicloud peut être un choix délibéré des DSI quand elle n'est pas une résultante du shadow IT qu'il leur faut parvenir à entériner et maîtriser.

1.3 IaaS, PaaS, SaaS, les différents modèles de services

Au cœur du cloud computing, plusieurs modèles de services existent selon les besoins. Petit rappel de leurs caractéristiques et des responsabilités prestataire - client.

IaaS ou Infrastructure as a Service pour externaliser l'infrastructure matérielle

Comme son nom l'indique, l'IaaS permet d'externaliser serveurs, réseaux et stockage des données. Le client loue les aspects matériels et n'a pas besoin d'investir dans ces équipements, en revanche il reste responsable de ses applications, ses données et du système d'exploitation.Une solution IaaS couplée à un cloud privé s'avère idéale pour héberger les applicatifs cœur de métier.

PaaS ou Platform as a Service pour faciliter le développement

Avec le mode PaaS, en plus de l'infrastructure, le prestataire fournit l'ensemble des applications middleware : système d'exploitation, base de données, serveur web etc.

Le PaaS permet surtout de développer, d'exécuter et de gérer des applications sans avoir à construire et à maintenir l'infrastructure.

Le modèle de sécurité du PaaS est donc partagé. Le fournisseur sécurise l'infrastructure tandis que le client conserve la responsabilité de protéger comptes, applications et données hébergées sur la plate-forme

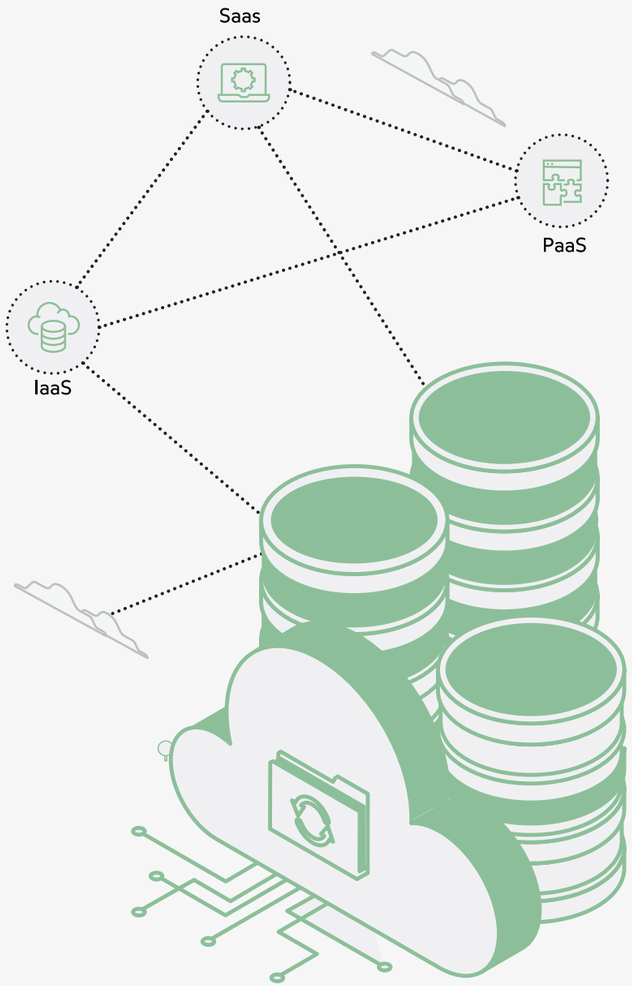
Saas ou Software as a Service : le All-in-One sécurisé

Contrairement aux autres modèles, le SaaS suppose une prise en charge totale des logiciels, de la maintenance et de l'infrastructure. C'est le fournisseur qui gère les serveurs, le réseau, le stockage, le système d'exploitation, les bases de données et les applications client. Les collaborateurs peuvent accéder aux logiciels à distance 24h/24, grâce à une connexion Internet.

Adossé à un cloud privé sécurisé et souverain, le SaaS apparaît comme le modèle le plus robuste et sécurisé pour le traitement et le stockage des données sensibles.

Pour les DSI, c'est également un vrai gage de tranquillité car il permet notamment :

- La reprise d'activité rapide en cas de faille du système
- La récupération des données en cas de sinistre
- L'externalisation de la maintenance et des mises à jour
- Une meilleure sécurisation des données pour les travailleurs nomades



02

Cloud Computing : profitez du meilleur du cloud en tenant compte de ses limites

Cloud Computing : profitez du meilleur du cloud en tenant compte de ses limites

Lorsqu'on parle de migration des SI dans le cloud, la question qui revient systématiquement est celle de la sécurisation.

Or, les avancées technologiques en matière de cybersécurité, les connaissances et l'expérimentation ont permis une vraie révolution : il apparaît de plus en plus qu'en mettant en place des stratégies adaptées et en adoptant de bonnes pratiques, le cloud s'avère plus sécurisé que les installations on-premise.

La raison ? Une professionnalisation des métiers du cloud, des prestataires et des clients mieux au fait de leurs besoins et des dangers, des stratégies plus efficaces, une législation nationale et européenne protectrice des données… Entre autres.

En 2023 le cloud est le meilleur allié des DSI à condition d'en connaître les limites et d'adopter les bonnes pratiques.

2.1 Profiter du meilleur du cloud en entreprise…

Pour les utilisateurs finaux comme pour les DSI, le cloud computing possède des atouts indiscutables :

Agilité, collaboration, mobilité, fiabilité : le cloud au service des utilisateurs finaux

Le 1er objectif du cloud computing reste de permettre à l'entreprise et aux collaborateurs de fonctionner le mieux possible et au même rythme que la concurrence. Cela passe aujourd'hui par :

- l'agilité, qui favorise flexibilité et mobilité des collaborateurs ;
- la collaboration, pour accéder aux documents, les modifier et les partager en temps réel et depuis n'importe quel support ;
- l'évolutivité, avec des produits et services disponibles à la demande, sans qu'il soit nécessaire de posséder les ressources et les compétences en interne ;
- la fiabilité grâce à la sauvegarde et la récupération des données en urgence, permettant ainsi la continuité des activités dans une situation de crise.

Les atouts du cloud pour les DSI : souplesse, fiabilité des modèles et maîtrise des coûts

Pour les DSI, les atouts du cloud tiennent à la flexibilité des solutions, la simplification et l'optimisation des processus mais aussi et surtout à une plus grande maîtrise des coûts d'implémentation, d'hébergement, de maintenance et de sécurisation.

Passer par un SaaS cloud sécurisé permet entre autres :

- la réduction des délais de déploiement et une intégration technique facilitée par la mise à disposition des ressources matérielles et humaines ;
- des mises en place progressives, par module fonctionnel ;
- une simplification de la sauvegarde et de la récupération des données en urgence appuyée par une implication forte et permanente du prestataire cloud ;
- une allocation dynamique de capacité pour une plus grande flexibilité

L'impact financier et la maîtrise des coûts, l'atout majeur d'un cloud Saas pour les SI

Les solutions cloud, particulièrement en mode SaaS, ont un impact direct sur les coûts à tous les niveaux.

L'investissement initial est réduit, libéré des frais d'infrastructure ou de mobilisation des ressources : il n'y a pas de serveur ni de logiciel à installer, pas de réseau à étendre, pas de formation exploitant à acquérir.

Les coûts sont mieux maîtrisés avec des frais de maintenance déjà intégrés au modèle locatif, une facturation à la demande, des mises à jour de version transparentes car déjà incluses dans l'abonnement et un support optimisé pour permettre d'accéder en ligne à l'application défectueuse.

L'impact financier se joue aussi plus strictement au niveau comptable :
le Cloud Computing est considéré comme une charge de fonctionnement, donc immédiatement déductible pour la totalité de son montant parce que « consommée » immédiatement, au contraire de l'immobilisation.

2.2 ...tout en prenant en compte de ses limites en termes de sécurité

La sécurité des SI dans un environnement de travail hybride fait partie des grandes problématiques du Cloud Computing en 2023.

A quelles attaques variées doit-on faire face ? Quelles sont les dernières tendances chiffrées en matière de cybersécurité ? Que risque-t-on en cas d'attaque non maîtrisée ou de non-conformité aux lois en vigueur ? Le point sur une problématique qui touche tous les métiers à responsabilité des SI.

2.2.a Panorama des types d'attaques les plus courants en 2022

Le phishing et le spear fishing

Les attaques d'hameçonnage et hameçonnage ciblé demeurent les plus courantes. Elles consistent à envoyer des e-mails qui semblent provenir de sources fiables dans le but d'obtenir des informations personnelles ou d'inciter les utilisateurs à une action.

Cette technique implique souvent une pièce jointe à un e-mail, qui charge un logiciel malveillant sur l'ordinateur, ou un lien pointant vers un site web illégitime qui incite à télécharger des logiciels malveillants ou à transmettre des données personnelles.

Les attaques par déni de service (DoS) et par déni de service distribué (DDoS)

L'attaque DoS ou déni de service submerge les ressources d'un système afin que ce dernier ne puisse pas répondre aux demandes de service. L'attaque DDoS est lancée à partir d'un grand nombre d'autres machines hôtes infectées par un logiciel malveillant contrôlé par l'attaquant.

Les Malwares ou logiciels malveillants

Ils sont légion et protéiformes, on peut citer : les macro-virus, les infecteurs de fichiers, les infecteurs de système ou de secteur d'amorçage, les virus polymorphes qui se cachent dans des cycles de chiffrement et de déchiffrement, les virus furtifs qui prennent le contrôle de certaines fonctions du système pour se dissimuler, les Chevaux de Troie, les Bombes logiques, les vers, les fichiers en .exe. En 2022, ce sont les rançongiciels et les logiciels espions qui créent le plus de dégâts.

L'Attaque de l'homme du milieu (MitM)

Une attaque de l'homme du milieu est un pirate qui s'insère dans les communications entre un client et un serveur. Voici quelques types courants d'attaques de l'homme du milieu :

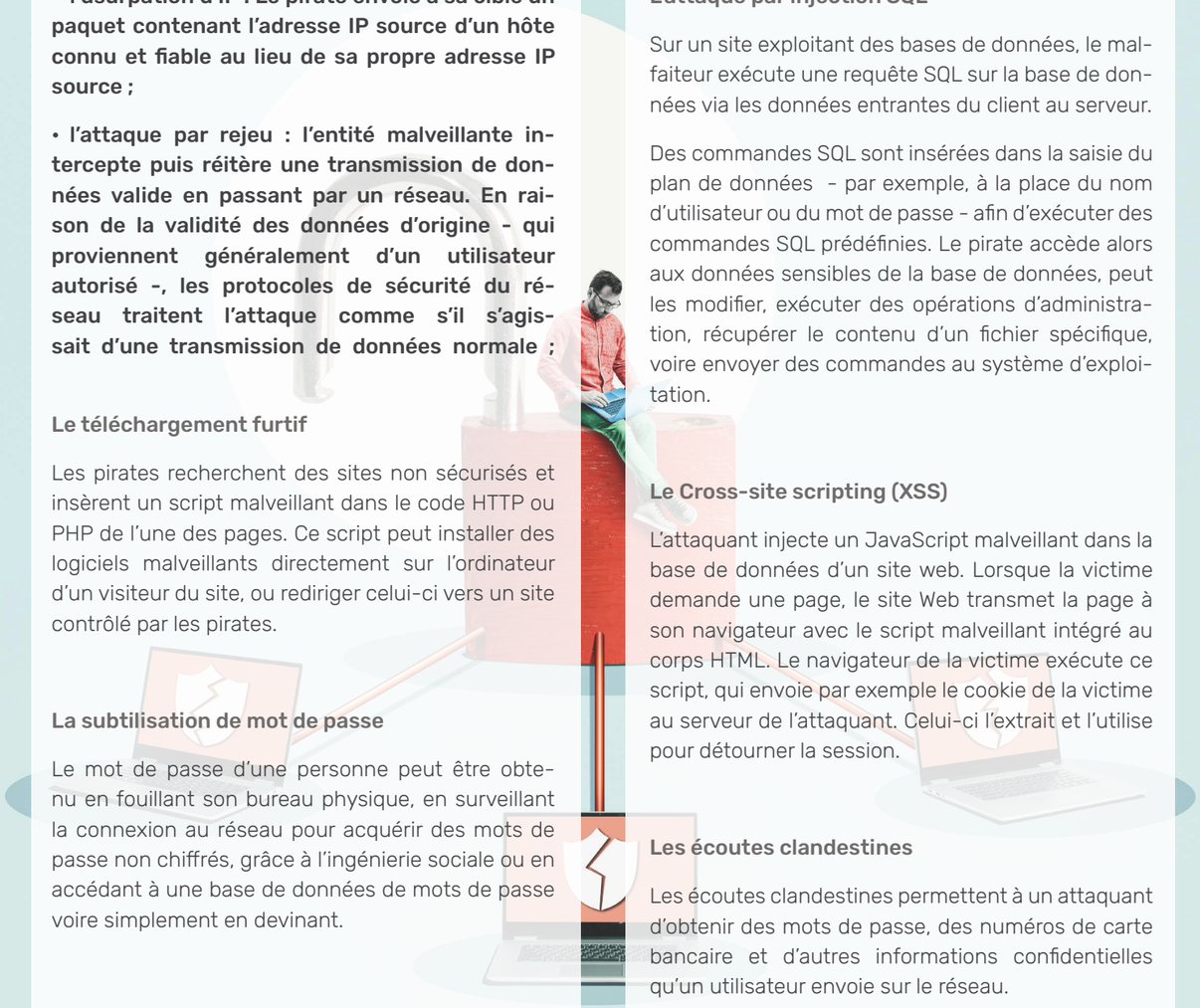
- **le Détournement de session qui permet à l'ordinateur attaquant de substituer son adresse IP au client de confiance pendant que le serveur poursuit la session, croyant qu'il communique avec le client ;**
- **l'usurpation d'IP : Le pirate envoie à sa cible un paquet contenant l'adresse IP source d'un hôte connu et fiable au lieu de sa propre adresse IP source ;**
- **l'attaque par rejeu : l'entité malveillante intercepte puis réitère une transmission de données valide en passant par un réseau. En raison de la validité des données d'origine - qui proviennent généralement d'un utilisateur autorisé -, les protocoles de sécurité du réseau traitent l'attaque comme s'il s'agissait d'une transmission de données normale ;**

Le téléchargement furtif

Les pirates recherchent des sites non sécurisés et insèrent un script malveillant dans le code HTTP ou PHP de l'une des pages. Ce script peut installer des logiciels malveillants directement sur l'ordinateur d'un visiteur du site, ou rediriger celui-ci vers un site contrôlé par les pirates.

La subtilisation de mot de passe

Le mot de passe d'une personne peut être obtenu en fouillant son bureau physique, en surveillant la connexion au réseau pour acquérir des mots de passe non chiffrés, grâce à l'ingénierie sociale ou en accédant à une base de données de mots de passe voire simplement en devinant.



L'attaque par injection SQL

Sur un site exploitant des bases de données, le malfaiteur exécute une requête SQL sur la base de données via les données entrantes du client au serveur.

Des commandes SQL sont insérées dans la saisie du plan de données - par exemple, à la place du nom d'utilisateur ou du mot de passe - afin d'exécuter des commandes SQL prédéfinies. Le pirate accède alors aux données sensibles de la base de données, peut les modifier, exécuter des opérations d'administration, récupérer le contenu d'un fichier spécifique, voire envoyer des commandes au système d'exploitation.

Le Cross-site scripting (XSS)

L'attaquant injecte un JavaScript malveillant dans la base de données d'un site web. Lorsque la victime demande une page, le site Web transmet la page à son navigateur avec le script malveillant intégré au corps HTML. Le navigateur de la victime exécute ce script, qui envoie par exemple le cookie de la victime au serveur de l'attaquant. Celui-ci l'extrait et l'utilise pour détourner la session.

Les écoutes clandestines

Les écoutes clandestines permettent à un attaquant d'obtenir des mots de passe, des numéros de carte bancaire et d'autres informations confidentielles qu'un utilisateur envoie sur le réseau.

2.2.b Les chiffres-clés* de la Cybersécurité en 2022

Cyberattaques réussies : des chiffres en baisse relative par rapport à 2021

Même si le nombre de cyberattaques démontre une tendance à la baisse, **près de la moitié des entreprises ont subi au moins une cyberattaque réussie en 2022**.

La majorité de ces attaques demeurent les attaques de type phishing ou spearfishing à 74%, suivies à 45 % par l'exploitation de failles logiciels et configuration.

L'attaque par rançongiciel touche particulièrement les TPE, PME et ETI. Cette attaque qui consiste à crypter les données d'une entreprise de façon à lui extorquer des sommes d'argent reste au cœur des préoccupations de l'ANSSI, et donne lieu à de nombreuses actions de sensibilisation.

A l'origine des attaques ? Les négligences, erreurs de manipulation ou de configuration par un administrateur interne ou un salarié, ainsi que **le Shadow IT** – soit la mise en place ou l'utilisation d'applications non approuvées – cause de 35 % des cyberattaques.

En effet, malgré les politiques de sensibilisation mises en place, 1/3 des utilisateurs sensibilisés ne suivent pas les recommandations.

Quelles conséquences pour les entreprises ? Le vol de données, l'usurpation d'identité, le chiffrement des données par ransomware et le déni de service sont les principales conséquences de ses attaques.

Une meilleure efficacité des solutions mises en place dans les entreprises

Avec ces chiffres toujours élevés de cyberattaques et des failles liées souvent aux nouveaux modes de travail à distance, **plus de 8 entreprises sur 10 considèrent la sensibilisation des utilisateurs comme le premier facteur de réduction des cyberattaques**.

Outre la sensibilisation, les solutions jugées les plus efficaces aujourd'hui sont les **solutions d'authentification multifacteurs (MFA)** considérées efficaces à 92% et l**es solutions Endpoint Detection and Response (EDR)** à 86%.

Une confiance encore fragile, malgré des stratégies plus efficaces

Malgré un meilleur bilan de 2022, 50% des entreprises victimes de cyberattaques estiment toujours que les menaces de cyberespionnage sont élevées. **La menace d'espionnage informatique est d'ailleurs celle qui a le plus mobilisé les équipes de l'ANSSI en 2022.**

Enfin, si les entreprises sont plus de 70% à considérer avoir les moyens de prévention et de détection des cyberattaques de grande ampleur. En revanche, près de la moitié doutent de leur capacité de réponse e**t reconstruction après une cyberattaque.**

2.2.c De graves conséquences financières et juridiques

Pour l'entreprise, une cyberattaque peut avoir des conséquences graves à différents niveaux avec :

• **D'importantes pertes financières comme le paiement d'une rançon aux hackers, le remplacement des serveurs et du parc informatique, des jours voire des semaines de fonctionnement perdus, la chute des actions en bourse liées à la perte de confiance des actionnaires et du public.**

• **Des amendes infligées par l'administration compétente ou sanctions pénales très impactantes. La sécurisation des données est aujourd'hui encadrée par des réglementations nationales et européennes.**

A savoir : En 2022, 21 sanctions ont ainsi été prononcées par la CNIL, pour un montant de 101 277 900 euros. Ces sanctions comportent 19 amendes et 2 décisions de liquidation d'astreinte, c'est-à-dire le paiement d'une somme en raison du non-respect d'un ordre donné par la CNIL dans sa décision de sanction.

Parmi les manquements les plus fréquents figurent **le défaut d'information des personnes, le non-respect de leurs droits et le défaut de coopération avec la CNIL.**

Sur ces 21 sanctions, un tiers comporte également **un manquement en lien avec la sécurité des données personnelles.**

Près de la moitié des entreprises ont subi au moins une cyberattaque réussie en 2022

Plus de 8 entreprises sur 10 considèrent la sensibilisation des utilisateurs comme le premier facteur de réduction des cyberattaques

50% des entreprises victimes de cyberattaques estiment toujours que les menaces de cyberespionnage sont élevées

21 sanctions ont ainsi été prononcées par la CNIL, pour un montant de 101 277 900€

** Chiffres issus du Baromètre Cesin 2022 et du panorama de la Cybermenace 2022 de l'ANSSI*

03

Législation, certifications et souveraineté : des gardes-fous pour un cloud sain et sécurisé

Législation, certifications et souveraineté : des gardes-fous pour un cloud sain et sécurisé

Si l'on sait mieux aujourd'hui détecter les menaces et identifier les types d'attaques, l'amélioration de la sécurité du cloud doit beaucoup à l'encadrement des institutions nationales et européennes.

Du RGPD à la qualification SecNumCloud, la création de certifications toujours plus pointues pour les prestataires cloud français et européens leur permet de garantir aux entreprises une meilleure protection des données.

La souveraineté du cloud se trouve toutefois menacée à l'International, notamment par une politique américaine qui va à l'encontre du RGPD européen.

3.1 Une législation européenne et nationale protectrice

Le RGPD et les axes de travail de la CNIL en 2023

Entré en vigueur en mai 2018, le Règlement Général sur la Protection des Données encadre le stockage et le traitement des données personnelles des citoyens européens par les organismes publics et privés. En France c'est la CNIL - Commission nationale de l'informatique et des libertés – qui est chargée de veiller à son application.

Depuis son entrée en vigueur les entreprises ont dû entre autres :

- **Modifier leurs process de traitement des données et les sécuriser**
- **Désigner un Délégué à la Protection des Données (DPO).**
- **Etablir un registre de traitement des données.**
- **Mettre en conformité leur site internet pour la collecte des cookies**

Pour exemple, toutes les données personnelles RH contenues dans les bulletins de paie, les RIB et autres contrats doivent être consignées dans un registre des traitements. L'entreprise doit connaître leur localisation et maîtriser tous les événements liés à ces données. Certaines devront être obligatoirement supprimées après le départ d'un salarié.

En cas de non-respect du RGPD, l'entreprise peut se voir infliger une amende allant jusqu'à 4% de son CA annuel mondial. Ces amendes relativement rares les premières années d'application sont de plus en plus courantes.

Quelles priorités pour la CNIL en 2023 ?

En raison de l'évolution et de la profusion des outils numériques dans notre quotidien, la CNIL a retenu trois thématiques prioritaires de travail et axes de vigilance pour le futur proche :

- **les caméras augmentées avec notamment un risque de surveillance des personnes à grande échelle**
- **les transferts de données dans le cloud et leur sécurisation dans les pays situés en dehors de l'Union Européenne**
- **la collecte des données dans les applications des smartphones afin de protéger la vie privée des utilisateurs et les sensibiliser sur ces sujets.**

En parallèle de ces actions ciblées, elle continue à développer les outils de certification et à diffuser largement les bonnes pratiques et codes de conduite issus du RGPD.

3.2 FISA, Cloud Act et Executive Order 12333 : les menaces venues d'Outre-Atlantique

Alors que le RGPD européen n'a de cesse de protéger le traitement des données privées des citoyens sur son territoire, les Etats-Unis adoptent une politique très différente qui oblige les entreprises européennes à trouver des solutions contractuelles pour ne pas tomber sous le coup de ces lois.

Le FISA - Foreign Intelligence Surveillance Act

Loi de 1978 amendée en 2008, le FISA Amendments Act of 2008 autorise l'administration américaine à collecter, utiliser et partager des données personnelles étrangères, stockées sur des serveurs américains. Seule restriction : les personnes ciblées ne doivent pas être américaines. Les Etats-Unis peuvent ainsi récupérer des données en Europe et les partager avec d'autres pays étrangers

Le Cloud Act - Clarifying Lawful Overseas Use of Data Act

En 2018 sous la présidence de Donald Trump, le Cloud Act est adopté : il permet la récupération de manière légale et sans procédure, des données localisées dans les datacenters d'entreprises américaines, situés aux États-Unis et à l'étranger, sans que l'utilisateur concerné n'en soit informé.

Le fournisseur de cloud qui officie en Europe doit être une entreprise américaine, en totalité ou en partie (consortium, joint venture, filiale) ou être en affaires avec une entreprise américaine.

L'Executive Order 12333

Ce décret exécutif du Président des Etats-Unis, permet aux services de renseignement d'intercepter et d'analyser toute donnée entrant aux Etats-Unis. Cette collecte se fait par « interception », notamment via les câbles sous-marins qui permettent le transfert de données de l'Europe vers les Etats-Unis. Heureusement, le chiffrement de bout en bout des données transférées permet la confidentialité des informations.

Face à cette menace américaine et conformément au RGPD, l'Etat Français montre l'exemple à travers sa « doctrine du Cloud au centre » en imposant un hébergement des données sensibles détenues par ses administrations chez des prestataires certifiés SecNumCloud.

Il exclut de fait l'accès à ces données par les géants américains du cloud que sont Microsoft, Amazon et Google.

3.3 Panorama des certifications et qualifications pour un cloud hautement sécurisé

La sécurisation du cloud, capitale pour les acteurs européens et français passe donc par un certain nombre de qualifications et certifications parmi lesquelles :

• **La qualification SecNumCloud délivrée par l'ANSSI - Agence Nationale de la Sécurité des Systèmes Informatique – qui atteste du plus haut niveau en matière de sécurité informatique dans le cloud. Un prestataire qualifié SecNumCloud peut prouver que son système respecte les bonnes pratiques listées dans le référentiel et que cette conformité a été vérifiée par des prestataires d'audit également approuvés par l'Anssi - les PASSI**

En janvier 2019, Oodrive est devenu **le premier acteur qualifié SecNumCloud** pour l'ensemble de ses offres de cloud privé. Ce visa, d'une durée de trois ans, a été renouvelé en 2022.

• **La qualification eIDAS, norme européenne relative aux moyens d'identification électronique et aux transactions des différents Etats-membres de l'UE. Elle encadre l'usage de la signature électronique pour les échanges entre les organismes du secteur public et leurs usagers. Le règlement eIDAS traite aussi des documents électroniques en leur accordant un effet juridique.**

• **La certification ISO 27001, norme internationale qui régit la mise en place de systèmes de management de la sécurité de l'information (SMSI). Elle définit une méthodologie pour identifier les cyber-menaces, maîtriser les risques associés aux informations critiques de son organisation, mettre en place les mesures de protection appropriées afin d'assurer la confidentialité, la disponibilité et l'intégrité de l'information.**

• **Son extension, la certification ISO 27701 permet de faire reconnaître un système de management de la protection de la vie privée, dans le cadre de la gestion des risques liés à la protection des données personnelles. Elle atteste de la mise en œuvre d'une politique des données maîtrisée et d'un haut niveau de confidentialité et de protection de la vie privée.**

• **La certification HDS - Hébergeur de Données de Santé - est obligatoire pour justifier de l'hébergement et l'infogérance des services et applications contenant des données de santé identifiables et personnelles. Cette certification a pour objectif de garantir une qualité de service des hébergeurs de données de santé.**

04

Mise en place du cloud dans votre entreprise : Les grandes étapes

Mise en place du cloud dans votre entreprise : Les grandes étapes

On l'a vu, la mise en place du SaaS dans un cloud sécurisé représente un atout majeur pour les DSI à condition d'en connaître les limites et de choisir des partenaires qualifiés, parfaitement au fait des dernières technologies de cybersécurité et de la réglementation en vigueur.

Plus concrètement, un passage au cloud réussi en 2023 passe par quatre étapes à ne surtout pas négliger : la définition du projet initial, la détermination des besoins concrets qui en découlent, la migration des données dans le cloud et l'accompagnement du changement.

4.1 Bien définir son projet initial

Pour qu'une stratégie cloud fonctionne de façon optimale et avec une pleine maîtrise des coûts, il faut d'abord savoir déterminer ses besoins réels. Cela passe par une parfaite connaissance de ses systèmes informatiques, de ses réseaux et des spécificités métier.

• Cherche-t-on à héberger ses données confidentielles dans un environnement sécurisé et souverain ?

• Souhaite-t-on adopter un CRM cloud de type Salesforce pour rebooster ses ventes et améliorer la performance des équipes ?

Si les solutions cloud sont personnalisables, la stratégie initiale doit être la plus claire possible pour tirer tous les bénéfices de cette transformation.

4.2 Détailler ses besoins concrets avec le concours des métiers et de la gouvernance de l'Entreprise

Une fois le projet initial bien clarifié, les responsables SI de l'entreprise vont pouvoir s'affranchir du plus gros de la partie technique pris en charge intégralement par leur prestataire cloud.

Ils doivent cependant être en mesure d'intégrer les couches ayant trait à l'authentification des utilisateurs et au niveau de sécurisation des accès à mettre en place.

• Souhaite-t-on un système d'authentification décorrélé de l'entreprise pour éviter que l'administration de certains comptes soit réalisée par la DSI interne ? Cela peut être souhaitable par exemple pour un Conseil d'Administration manipulant des données hautement confidentielles.

• Souhaite-t-on un système d'authentification décorrélé de l'entreprise pour éviter que l'administration de certains comptes soit réalisée par la DSI interne ? Cela peut être souhaitable par exemple pour un Conseil d'Administration manipulant des données hautement confidentielles.

• Ou préfère-t-on une seule base d'administration des comptes pour tous les collaborateurs, en interne, en SaaS ou ailleurs pour faciliter les onboardings et offboardings ?

Le fournisseur de solutions cloud s'adapte en termes de fonctionnalités et d'implémentation mais c'est bien à l'entreprise de déterminer le niveau de sécurisation et d'authentification requis pour ses accès.

Pour cela, il faut être bien au fait des besoins de la gouvernance et des exigences métier en termes de confidentialité afin de pouvoir procéder à la classification des données en amont.

4.3 Classification, cartographie et migration des données

Avant de migrer ses données d'entreprise dans le cloud, il est nécessaire d'avoir d'abord opéré une classification claire de ces dernières car toutes ne seront pas traitées ou sécurisées de la même manière.

Voici un exemple de classification des données :

- **Données hautement sensibles :** confidentielles, elles peuvent nuire à l'entreprise si elles sont divulguées. Ces données seront sécurisées et surveillées, elles requièrent des contrôles d'accès stricts.
- **Données moyennement sensibles :** il s'agit des données internes qui ne peuvent pas être divulguées au public mais ne représentent pas un risque important en cas de violation. On mettra en place un contrôle des accès mais un plus grand nombre d'utilisateurs pourra y accéder.
- **Données à Faible sensibilité :** ce sont les informations publiques qui ne nécessitent pas beaucoup de sécurité

Cette classification n'est pas normée et peut varier d'une entreprise à. l'autre. Une fois réalisée, elle permet d'affiner le contexte de la migration, de cartographier les points d'entrée et le traitement assigné à chaque catégorie de donnée.

4.4 L'Accompagnement du changement et la sensibilisation des utilisateurs

Primordial pour la réussite et la performance d'une migration dans un cloud privé de type SaaS, l'accompagnement du changement est très important pour les aspects fonctionnels mais aussi sécuritaires.

Si les risques de perte ou vol de données sont amoindris dans le cadre de la protection des données hautement sensibles, il demeure impératif que les utilisateurs suivent les recommandations et comprennent l'utilité des nouveaux applicatifs et environnements mis en place au regard des anciens.

Le changement peut être source de stress et parfois de rejet des collaborateurs habitués aux outils du cloud public, souvent adoptés au mépris des consignes de sécurité afin d'assurer la continuité des activités.

En 2023, on entre dans une nouvelle ère, celle des migrations réfléchies, maîtrisées, sécurisées car adossées à des technologies plus robustes et à des prestataires cloud experts.

Cet ebook vous est offert par Oodrive

Oodrive est leader européen de la gestion des contenus sensibles.
Le groupe propose aux entreprises des solutions de partage de documents, de sauvegarde et de signature électronique répondant aux certifications françaises et internationales les plus exigeantes en termes de sécurité et de confidentialité.

oodrive work
pour collaborer dans un environnement sécurisé

oodrive meet
pour digitaliser les réunions des instances de gouvernance

oodrive sign
pour la gestion des signatures électroniques à pleine valeur probatoire

OODRIVE EN BREF :

1 million
d'utilisateurs
dans 45 pays

3 500
clients

400
Oodriviens

Pour satisfaire aux besoins de souveraineté et de confidentialité, et conformément aux réglementations en vigueur, la sécurité des données des clients d'Oodrive est garantie par les plus hauts niveaux de qualifications :

eIDAS

ISO 27001
ISO 27701
HDS

Plus d'information : oodrive.com

26, rue du Faubourg Poissonnière 75010 Paris - France
oodrive.com