Plan d’assurance Sécurité

Annexe Microsoft Azure

cegid

SOMMAIRE

Table des matières

1. ÉVOLUTIONS DU DOCUMENT

Version	Date de publication
PAS_CEGID_SAAS_ANNEXE_AZURE_V201711	03 novembre 2017
PAS_CEGID_SAAS_ANNEXE_AZURE_V201802	02 février 2018
PAS_CEGID_SAAS_ANNEXE_AZURE_V201905	23 Mai 2018

2. INTRODUCTION

2.1 Objet

Ce document annexe au PAS décrit les engagements pris par Cegid en termes de sécurité de l'information sur les services opérés sur la plateforme Microsoft Azure.

2.2 Domaine d'application

Cette annexe s'applique uniquement aux éléments cloud de la plateforme Microsoft Azure intégrés par Cegid pour délivrer de manière optimisée et opérés par Cegid Cloud Factory.

Microsoft Azure est considéré par Cegid Cloud Factory comme un fournisseur critique.

2.3 Définitions

ISO : International Organisation for Standardization-Organisation Internationale de Normalisation qui a pour but de produire des normes internationales dans les domaines industriels et commerciaux.

CSA STAR Certification : Certification de la « Cloud Security Alliance » combinant la certification ISO 27001 et la Cloud Control Matrix.

Microsoft Azure : La plate-forme Microsoft Azure correspond aux offres d'informatique en nuage **publics** de type PaaS et IaaS de Microsoft

SAN : Storage Area Network

2.4 Documents de références

P.A.S : Plan Assurance Sécurité – Document de base décrivant la politique de sécurité mise en place par Cegid sur la délivrance des services applicatifs à destination de ses clients

Livrets Service : Documents décrivant les conditions particulières liées à chaque offre SaaS de Cegid. Ils sont disponibles sur www.cegid.com, site web de Cegid

3. CERTIFICATIONS DE LA PLATEFORME MICROSOFT AZURE

Microsoft Azure détient un large éventail de certifications ISO et CSA afin d'avoir une couverture de conformités des plus complète.

Une combinaison de ces certifications sur la plateforme Azure est effective et assure le respect d'un large panel d'obligations réglementaires.

Les enregistrements de certification CSA STAR sont consultables ici :
https://cloudsecurityalliance.org/star-registrant/microsoft/

Les rapports ISO et les certificats associés sont téléchargeables ici :
https://servicetrust.microsoft.com/Documents/ComplianceReports

4. PRESENTATION DE LA SECURITE AZURE

Pour opérer les services à destination de ses clients sur la plateforme Microsoft Azure, Cegid se réfère à l'expérience et l'expertise de Microsoft.

Azure propose divers mécanismes de sécurité pour favoriser la gestion et surveillance des services cloud et des machines virtuelles Azure.

La sécurité des services Microsoft Cloud est une collaboration et une responsabilité partagée entre Cegid et Microsoft. Une responsabilité partagée signifie que Microsoft est responsable de Microsoft Azure et de l'intégrité physique de ses centres de données (grâce à l'utilisation de mesures de protection telles que des portes sécurisées au moyen de badges, des clôtures et des gardes). En outre, Azure fournit des niveaux élevés de sécurité du cloud sur la couche logicielle, répondant aux attentes exigeantes de Cegid en matière de sécurité, de confidentialité et de conformité.

Microsoft s'appuie sur 10 grands principes de sécurité qui font appel au meilleur des technologies en matière de sécurité.

Ces 10 principes sont détaillés sur : https://docs.microsoft.com/fr-fr/azure/security/azure-security

Cegid applique ce référentiel au périmètre concerné par son activité à savoir :

- ✓ Sécurité du réseau
- ✓ Sécurité de la base de données

- ✓ Sécurité du stockage
- ✓ Sécurité opérationnelle

Ces principes sont appliqués afin de garantir la disponibilité, l'intégrité et la confidentialité des données et des applications clients mais aussi la conformité aux bonnes pratiques des équipes Cegid en charge de l'exploitation et de la mise en production de ces applications.

4.1 Sécurité du réseau

La sécurité du réseau se concentre sur les points suivants :

- Mise en réseau et architecture
  - Cegid construit différentes architectures flexibles et adaptées aux applications de ces client. Ces architectures s'appuient sur le subnetting du réseau virtuel Azure et la mise en place de DMZ.
  - En complément de la sécurité native de Microsoft, Cegid Implémente une brique de pare-feu de niveau 7 avec option IDS/IPS
- Contrôle des accès réseau
  - La mise en place de NSG (Network Security Group) permet un contrôle total des différents accès aux divers composants du réseau
- Accès à distance et connectivité
  - Le service Azure Express Route est utilisé pour relier les différentes souscriptions.
  - Les services UDR (User Defined Routes), Load Balancer et Application Gateway permettent de rediriger les flux entrants vers les briques de sécurité (Virtual Security Appliance)
  - Les équipes production SaaS administrent la solution via le service Azure Express Route au travers d'un MPLS opérateur

4.2 Sécurité de la base de données

Cegid utilise les principes standards proposés par Microsoft Azure à savoir :

- le protocole TLS/SSL pour le processus de connexion/authentification et pour la gestion des données en transit
- Deux techniques de chiffrement peuvent être mises en place suivant les offres et les architectures à savoir :

- Offre PaaS : chiffrement transparent de la base de données SQL (TDE) en effectuant le chiffrement et le déchiffrement en temps réel à l'aide d'une clé symétrique appelée clé de chiffrement de base de données. Cette clé est protégée par un certificat de serveur intégré. Ce certificat est unique pour chaque serveur de base SQL. Ces clés sont stockées dans un coffre-fort numérique à accès restrictif.
- Offre IaaS : chiffrement direct de l'enveloppe SAN (aire de stockage) sans besoin de clé de chiffrement

4.3 Sécurité du stockage

Cegid utilise les briques Azure suivantes à des fins d'administration de la plateforme Azure

- File Share et Blob Storage (environnements de stockage et de transports cryptés) pour le stockage de fichiers (logs, script …)
- RBAC (Role-Based Access Control) qui permet de sécuriser la base des comptes utilisateurs des équipes de Cegid production SaaS.
- Chiffrement des disques managés des VM

4.4 Sécurité opérationnelle

Cegid s'appuie sur les services Azure suivants :

- Azure Security Center : Prévention, détection et résolution de menaces
- Azure monitor : Outil de surveillance des services
- Azure Network Watcher : Surveillance et diagnostique du réseau Azure
- NSG : flux et analyse de trafic
- Mise en place de key vault (coffre-fort numérique) pour le stockage des éléments de sécurité opérationnels (mot de passe des scripts…)

5. SPECIFICITES LIEES A L'EXPLOITATION

5.1 Localisation

Cegid s'appuie sur l'infrastructure suivante du Cloud Public Microsoft Azure :
https://azure.microsoft.com/fr-fr/regions/

La localisation des données pourra être définie contractuellement avec le client (assignation d'un POD).

Le descriptif des mécanismes d'accès aux données est accessible à :

https://www.microsoft.com/fr-fr/trustcenter/privacy/who-can-access-your-data-and-on-what-terms

5.2 PCA & Résilience

Dans le cadre des offres Cloud Cegid Azure, la mise en œuvre du plan de continuité d'activité telle qu'évoquée dans le PAS Cegid s'appuie plus particulièrement sur les principes et mécanismes ci-dessous.

D'un point de vue technique, la résilience des solutions Cloud Cegid Azure est basée* sur :

- Des mécanismes d'équilibrage de charge réseau (cf Azure Load Balancer)
- Des mécanismes d'équilibrage de charge applicative (cf Azure Application Gateway)
- Des mécanismes de haute disponibilité et de montée en charge (cf Azure Virtual Machine ScaleSet)
- Des mécanismes de haute disponibilité (cf Azure AvailabilitySet ou Availability Zone suivant les offres proposées)
- Des mécanismes de backup haute disponibilité (cf Azure Recovery Site et DPM)
- Des instances multiples et réparties des serveurs d'applications, des pare-feu / IPDS

** cf documents d'architecture des offres concernées*

La gouvernance de sécurité et de résilience est basée sur les bonnes pratiques édictées par Microsoft Azure.

- https://docs.microsoft.com/en-gb/azure/best-practices-network-security

Les différents SLA relatifs à ces services sont accessibles à :

- https://azure.microsoft.com/en-us/support/legal/sla/?v=17.42