# Partie 2.4 : Rôle et responsabilité de l’ingénieur.

## Responsabilité Juridique :

Le groupe doit expliquer comment il a géré la confidentialité des données utilisateur

Incontestablement, Docker s’adresse à trois grands profils de clients : les early adopters, les utilisateurs qui découvrent cet environnement et ceux qui ne l’ont pas encore utilisé. Pour autant, quel que soit son niveau de maturité, la sécurité reste toujours un obstacle à franchir.

Concrètement, lorsque l’on utilise des « containers », la sécurité traditionnelle ne suffit pas. On ne sécurise pas une infrastructure « containérisée » comme on sécurise son infrastructure virtualisée. Il est donc important de bien comprendre les enjeux de la sécurité dans une infrastructure « containérisée », ainsi que les risques associés pour les intégrer efficacement dans sa politique de sécurité.

Evaluation de l’infrastructure containerisée afin de déterminer les différences de sécurisation de la solution.

* Plus de composants

Dans une infrastructure virtualisée, les flux sont plus au moins maitrisés. Dans une infrastructure « containérisée », cela se complique au regard des architectures complexes type « microservices », où le code est éclaté sur différents composants. Pour les équipes sécurité, il faut donc s’adapter à cette multitude de flux.

* Durée de vie courte des containers

En comparaison avec les machines virtuelles, un container a une durée de vie plus courte. Les équipes de développement vont donc constamment recréer des containers.

* Quels changements au niveau des risques ?

Les risques sont pratiquement identiques à ceux des infrastructures virtualisées ou classiques. Cependant, certains points sont intéressants à préciser :

* + Risques sur les configurations par défaut

Garder les configurations par défaut amène un risque important dans une infrastructure conteneurisée. Nous avons donc personnalisé chacune de nos configuration afin de fournir un service unique et sécurisé répondant à chacun des besoins de votre entreprise.

* + Le top ten owasp reste valable

Avec les containers, on utilise toujours les mêmes protocoles de communication : les attaques applicatives classiques sont donc courantes. Nous avons donc créé notre infrastructure en prenant en compte les dix attaques les plus fréquentes de cette années.

* + Attaque réseau

Si un pirate prend la main sur un container, il pourra lancer un scan réseau et faire des déplacements latéraux. Comme il y a un manque de visibilité, les équipements de sécurité ne vont pas détecter ce scan, et le pirate pourra facilement passer d’un container à l’autre.

Sécurisation des opérations sur Docker :

Voici les quelques bonnes pratiques que nous avons mis en place :

* Créer une partition physique séparée pour Docker
* Maintenir le système et les images à jour
* Éviter le stockage de secrets au sein d’une image
* Ne pas utiliser n’importe quel registre, nous n’utilisons que le hub docker.
* Contrôler les communications entre containers : nous avons mis en place des réseaux spécifiques pour chaque liaison. De cette manière, vos services peuvent uniquement communiquer avec leurs propres applications.
* Vérifier les sources de construction des images utilisées par les conteneurs et assurer un suivi de leurs évolutions.

Sécurisation des communications :

Nous proposons la mise en place du protocole de communication HTTPS afin de sécuriser les échanges entre nos serveurs et le client. Grâce à cette technologie nous pouvons garantir au client que celui-ci communique uniquement avec nos serveurs lors de l’échange de données confidentielles. L'HyperText Transfer Protocol Secure : HTTPS, est la combinaison du HTTP avec une couche de chiffrement TLS. HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité de certification : une autorité tierce, réputée fiable et faisant généralement partie de la liste blanche des navigateurs internet. Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur et reçues du serveur.

Sécurisation des données personnelles : RGPD

La protection des données personnelles nécessite de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

* SENSIBILISER LES UTILISATEURS

Faire prendre conscience à chaque utilisateur des enjeux en matière de sécurité et de vie privée.

* AUTHENTIFIER LES UTILISATEURS

Reconnaître ses utilisateurs pour pouvoir ensuite leur donner les accès nécessaires. Par exemple dans le cas de notre solution nous utilisons LDAP qui est un protocole permettant l’interrogation et la modification de notre service d’annuaire.

* GÉRER LES HABILITATIONS

Limiter les accès aux seules données dont un utilisateur a besoin.

* TRACER LES ACCÈS ET GÉRER LES INCIDENTS

Journaliser les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).

* PROTÉGER LE RÉSEAU INFORMATIQUE INTERNE

Autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place.

* SÉCURISER LES SERVEURS

Renforcer les mesures de sécurité appliquées aux serveurs.

* SAUVEGARDER ET PRÉVOIR LA CONTINUITÉ D'ACTIVITÉ

Effectuer des sauvegardes régulières pour limiter l’impact d’une disparition non désirée de données.

* ARCHIVER DE MANIÈRE SÉCURISÉE

Archiver les données qui ne sont plus utilisées au quotidien mais qui n’ont pas encore atteint leur durée limite de conservation, par exemple parce qu’elles sont conservées afin d’être utilisées en cas de contentieux.

* ENCADRER LA MAINTENANCE ET LA DESTRUCTION DES DONNÉES

Garantir la sécurité des données à tout moment du cycle de vie des matériels et des logiciels.

* GÉRER LA SOUS-TRAITANCE

Encadrer la sécurité des données avec les sous-traitants.

* SÉCURISER LES ÉCHANGES AVEC D'AUTRES ORGANISMES

Renforcer la sécurité de toute transmission de données à caractère personnel.

* PROTÉGER LES LOCAUX

Renforcer la sécurité des locaux hébergeant les serveurs informatiques et les matériels réseaux.

* CHIFFRER, GARANTIR L’INTÉGRITÉ OU SIGNER

Assurer l’intégrité, la confidentialité et l’authenticité d’une information.

## L’impact sur l’environnement :

Le groupe doit analyser l'impact de la solution sur la société et l'environnement en s’appuyant par exemple sur une politique Green IT ou de développement durable

* Les matériels qui ne demandent pas un fonctionnement permanent sont systématiquement éteints et non mis en veille. Grâce à la containerisation il est possible lors de perte de charge de limiter l’utilisation des machines afin de réduire la consommation d’énergie.
  + Objectifs :
    - Permettre une réduction de la consommation énergétique supérieure à celle relevée lorsque les appareils sont en veille
    - Adopter un comportement responsable
* Les calculs et les tâches sont répartis sur différents serveurs dédiés en fonction de la nature de leurs tâches (données, mails, vidéos etc.)
  + Objectifs :
    - Maîtriser l'impact sur la consommation énergétique
    - Réduire l'impact écologique des échanges d'information
* Dans le cadre de travaux collectifs, l'usage d'outils collaboratifs en ligne est privilégié à l'échange de courriels.
  + Objectifs :
    - Réduire l'impact écologique des échanges d'information
    - Sensibiliser les personnels
    - Responsabiliser les personnels
    - Maîtriser la politique GreenIT de l'entreprise
* Anti-SPAM : Tous les spams sont supprimés
  + Objectifs :
    - Limiter l'impact écologique du stockage de l'information
    - Induire des comportements responsables

## Argumentation :

Dans l’ensemble du document, le groupe a expliqué et argumenté les choix réalisés

## Rédaction :

Le document est rédigé (phrases, paragraphes) et sans faute d’orthographe