

## Décision d'homologation de sécurité

### Super Service

Type : API

Objet : Super Service est un service numérique qui donne un accès dématérialisé à ses usagers.

Développé par : Superdev

Hébergement et localisation des données : Scalingo, France

### Principaux risques de sécurité identifiés

Suggestions de l'ANSSI, détails en annexe



L'indisponibilité du service



La divulgation de données  
d'utilisateurs



La surveillance



La défiguration d'un site web



Logiciels malveillants



Arnaques

### Mesures de sécurité retenues

Recommandées par l'ANSSI, détails en annexe

 Mises en œuvre  Planifiées à 3 mois

5 mesures de  
**Gouvernance**

13 mesures de  
**Protection**

4 mesures de  
**Défense**

4 mesures de  
**Résilience**

### Niveau de protection indicatif

Calculé à partir du pourcentage de mesures recommandées par l'ANSSI mises en œuvre

**Bon**

**100%**

des mesures indispensables selon l'ANSSI mises en œuvre

**60%**

des autres mesures suggérées mises en œuvre

## Avis de l'expert cyber

sur le maintien ou la mise en service



Favorable

Expert cybersécurité : Pierre Dubois (RSSI)

Recommandations additionnelles : Rien à signaler.

## Équipe

Décision d'homologation préparée par : Jean Dupont (Responsable métier), Pierre Dubois (RSSI)

## Calendrier

Échéance de mise en œuvre des mesures planifiées : 3 mois

Date d'expiration de l'homologation : Deux ans après signature de la présente homologation

## Décision d'homologation

Autorité d'homologation : Sylvie Martin (Maire)

Lu et approuvé | date | signature



Conformité au  
référentiel général  
de sécurité (RGS)



Contribue à la mise en conformité avec les obligations du règlement  
européen pour la protection des données à caractère personnel (RGPD) en  
matière de « sécurité du traitement des données »

Par la signature de cette décision, vous attestez avoir pris connaissance des risques principaux pour le service numérique et des mesures de sécurité retenues, sur la base des informations fournies dans le présent dossier et ses pièces jointes. Vous validez son maintien ou sa mise en service, dont la sécurité devra être maintenue dans la durée. Une fois signée, la décision d'homologation pourra être publiée sur MonServiceSécurisé et sur « Super Service ». MonServiceSécurisé et l'ANSSI ne peuvent en aucun cas être tenus responsables d'incidents de sécurité susceptibles d'affeter le service numérique homologué et des conséquences qui pourraient en découler.

## Pièces jointes



Visuel du service



Compte-rendu de test de pénétration ou de bugbounty

## Annexe 1 – Détail des risques principaux



### L'indisponibilité du service

Ce risque peut notamment découler d'une attaque par déni de service. Elle peut consister à exploiter, par exemple, une vulnérabilité logicielle ou matérielle ou à saturer la bande passante du réseau. Une telle attaque peut rendre inaccessible tout ou partie du service, empêchant son utilisation pendant une durée de quelques heures à plusieurs jours. L'indisponibilité peut être aussi consécutive d'un problème technique chez l'hébergeur n'ayant pas pris des dispositions nécessaires pour assurer sa résilience.



### La divulgation de données d'utilisateurs

Le vol de données peut être recherché à des fins d'usurpation d'identité. La diffusion de données afin de discréditer des personnes, organisations ou bien l'entité propriétaire du service elle-même. Cette menace peut être permise par un contrôle d'accès insuffisant ou le piratage de comptes d'utilisateurs (vol d'identifiant / mot de passe) ou plus grave d'administrateurs permettant la prise de contrôle du service. Ou encore par la surveillance d'un trafic non chiffré. Les impacts pour le propriétaire du service peuvent être graves en termes de responsabilité juridique et d'image.



### La surveillance

La menace d'accès illégitime à un échange, à des données à des fins d'information, de renseignement peut viser les services permettant les échanges entre personnes, des données sensibles stockées susceptibles d'intéresser des concurrents ou entités malveillantes souhaitant exploiter ses données à des fins de renseignement. Cette menace peut être permise par un contrôle d'accès insuffisant ou le piratage de comptes d'utilisateurs (vol d'identifiant / mot de passe) ou plus grave d'administrateurs permettant la prise de contrôle du service et l'accès à de nombreuses données. Ou encore par la surveillance d'un trafic non chiffré.



### La défiguration d'un site web

Une défiguration est une attaque par laquelle une personne malveillante modifie le site pour remplacer le contenu légitime par un contenu qu'il choisit, par exemple pour relayer un message revendicatif, pour dénigrer le propriétaire du site ou simplement. L'attaque peut avoir des conséquences négatives en termes d'image pour le propriétaire du service.



### Logiciels malveillants


Votre service peut être attaqué en vue de devenir un véhicule pour la diffusion de logiciels malveillants aux utilisateurs de votre service. Cela est rendu possible par l'exploitation de vulnérabilités techniques de votre service, par exemple, si votre service n'a pas été développé avec précaution, si votre service repose sur des logiciels ou équipements n'ayant pas fait l'objet de correctifs de sécurité de vulnérabilités connues. Une telle attaque peut n'avoir aucun impact visible pour le propriétaire du site mais susciter des impacts forts pour les utilisateurs. L'usurpation d'accès d'administrateurs peut également permettre l'envoi de messages malveillants paraissant légitimes aux utilisateurs du service.



### Arnaques

Votre service peut être utilisé à des fins d'arnaques, par exemple, par la création d'un service imitant le vôtre ou envoyant des mails ou SMS ayant l'apparence de messages légitimes, en vue de subtiliser des données, extorquer de l'argent. L'inclusion de code malveillant dans un service numérique peut permettre d'afficher du contenu illicite comme des arnaques au faux support technique.

## Annexe 2 – Détail des mesures de sécurité

☒ Mesures mises en œuvre    ☐ Planifiées à 3 mois    ☐ Non retenues  
 Mesure indispensable (ANSSI)

### Mesures de gouvernance

S'organiser pour gérer la sécurité du service

Identifier les interconnexions avec d'autres systèmes essentiels

