Sentimail

Plan de sécurisation

CPE Lyon

Nicola Piemontese, Valentin TOURNIER, Thomas VIOLENT,
Thomas GENIN
25/01/2024

Table des matières

Introduction 1
Mesures de Sécurité 1
Confidentialité 1
Intégrité 1
Disponibilité 2
Sécurité du Code 2
Sécurité de l'Infrastructure 2
Sécurisation des Accès 2
Améliorations futures 3
Analyse de Vulnérabilités avec OpenVAS 3
Tests d'Intrusion avec OWASP ZAP 3
Tests d'intégration 3
Construction automatique d'images 3

Introduction

Ce document présente le plan complet de sécurisation mis en œuvre pour garantir la robustesse et la fiabilité de notre projet SentiMail. Notre approche repose sur les principes de la cybersécurité, en particulier sur les piliers fondamentaux que sont la confidentialité, l'intégrité et la disponibilité. Nous avons également adopté une approche DevSecOps, intégrant la sécurité dès le début du processus de développement.

Mesures de Sécurité

Confidentialité

Chiffrement des données

- Utilisation d'un certificat SSL/TLS 1.3 avec le protocole HTTPS pour garantir la confidentialité des données en transit. Le renouvellement de ce certificat est géré automatiquement par Traefik.
- Traefik se charge de forcer la communication en TLS1.3

Intégrité

Stratégie de sauvegarde

Mise en place d'une sauvegarde automatique quotidienne de la machine virtuelle (VM) pour assurer l'intégrité des données et permettre une récupération efficace en cas de besoin.

Disponibilité

Haute disponibilité avec Kubernetes

Utilisation de Kubernetes pour assurer une haute disponibilité des services, offrant une gestion efficace des conteneurs et une résilience accrue.

Sécurité du Code

GitHub

Tout le code source de l'application et de l'infrastructure sont stockés sur GitHub afin d'avoir un suivi des évolutions et de sauvegarder le code.

Audit de code avec SonarQube

Intégration de SonarQube pour réaliser des audits de code, identifiant les vulnérabilités potentielles et renforçant la sécurité du code dès les premières étapes du développement.

Recherche de vulnérabilités dans les images Docker avec Grype

Utilisation de Grype pour une analyse proactive des images Docker, permettant de détecter et de remédier aux vulnérabilités avant leur déploiement.

Sécurité de l'Infrastructure

Reverse Proxy, Firewall et CrowdSec

- Mise en place d'un reverse proxy pour sécuriser les connexions entrantes.
- Utilisation d'un pare-feu (firewall) pour filtrer le trafic réseau.
    - Celui-ci va filtrer le trafic entrant et sortant, en entrée seul l'api Kubernetes et l'ingress traefik est ouvert. En sortie HTTP, HTTPS, DNS et NTP sont autorisés si ceux-ci vont sur internet (Une connection vers un autre sous-réseau est bloquée)
- Intégration de CrowdSec en tant que solution IPS/IDS pour détecter et répondre aux menaces de manière proactive.

Sécurisation des Accès

Système d'authentification et d'autorisations des utilisateurs

Mise en place d'un système robuste pour gérer l'authentification et les autorisations des utilisateurs, assurant la confidentialité des données sensibles.

Authentification par clé d'API

Intégration d'un système d'authentification par clé d'API pour sécuriser l'accès à l'API, renforçant ainsi la sécurité des accès.

Améliorations futures

Nous envisageons d'intégrer plusieurs initiatives pour renforcer davantage la sécurité de notre projet :

Analyse de Vulnérabilités avec OpenVAS

Intégration de l'outil OpenVAS pour des analyses régulières des vulnérabilités. OpenVAS fournira des rapports détaillés identifiant les points faibles potentiels dans notre infrastructure, permettant ainsi une action préventive pour remédier aux vulnérabilités avant qu'elles ne puissent être exploitées.

Tests d'Intrusion avec OWASP ZAP

L'intégration de tests d'intrusion, notamment avec l'utilisation d'OWASP ZAP (Zed Attack Proxy). Ces tests permettront de simuler des attaques potentielles, et effectuer des tests d'intrusion automatisés, identifiant les éventuelles vulnérabilités au niveau de l'application.

Tests d’intégration

Lors du développement d’une nouvelle version, il n’y a pas de tests d’intégration qui sont fait. On risque donc une régression. L’idée des tests d’intégration est d’envoyer des mails « de référence » et de comparer les différents résultats renvoyés par l’application

Construction automatique d’images

Grype vérifie à la construction des images si de potentielles vulnérabilités sont présentes dedans. Cependant pour devoir les détecter, une image doit être construite. L’idée ici est de construire des images à intervalle régulier (par exemple tous les jours) et de juste les scanner. Si celles-ci contiennent des vulnérabilités, celles-ci doivent être remontées avec une notification (envoie de mail ou autre)