Rapport/Analyse de sécurité
Groupe 3

Louis Arys Brogniet Geoffrey Martin Pardeans
Jean-Michael Tang

March 13, 2020

1 Introduction

Ce rapport est destiné à lister les risques ainsi que les solutions apportées à ces risques de l'entreprise WoodyToys tant au niveau infrastructure de celle-ci mais aussi du prototype que nous fournissons.

2 Risques de l'infrastructure réseau

Les risque les plus important pour WoodyToys sont la confidentialité et l'intégrité au sein de l'entreprise mais aussi à l'extérieur. Les exemples les plus clairs sont les interceptions des paquets, c'est-à-dire l'interception de message unique non identifié à cause d'une attaque de type "Man in the middle" par exemple. L'interception des paquets peut aussi mener à du "Fishing", autrement dit, le fait de se faire passer pour le site (ici WoodyToys) et de rediriger vers un site de Fishing qui pourra soit voler vos mots de passe soit agir de manière malveillante envers un client.

Pour éviter ces risques, nous pouvons envisager de sécuriser le site et d'utiliser un https qui, dans tout les cas, sera de rigueur.

Un des risques aussi de WoodyToys peut être la disponibilité du site mais aussi de ses infrastructures interne. Le site de l'entreprise doit être tout le temps opérationnel et pour cela plusieurs sécurité peuvent être mises comme par exemple ne pas tout mettre au "même endroit" ou encore bien choisir ses serveurs grâce au VPS

3 Risques du prototype

Le prototype peut conduire à plusieurs gros risques tant au niveau du VPS qu'au niveau des Dockers utilisés et empruntés sur le WEB.

Les risques du VPS sont les suivants :

- Les performances d'un VPS n'atteignent pas celles d'un véritable serveur. Généralement, les fournisseurs des VPS limitent les performances des serveurs afin de maximiser le nombre d'unité qu'un serveur physique peut contenir. Ce qui rejoint le risque de la disponibilité expliqué ci-dessus.

- Les VPS sont généralement des virtualisation du serveur, ce qui permet de créer un isolation entre chaque serveur. Mais le risque zéro n'existe pas et il est conseillé d'éviter les environnements partagés.

Les risques au niveau du Docker sont simplement l'exécution de code, la confiance des Docker mis à disposition ainsi que le déni de service. Afin de contrer ces risques, il faut prévenir tout cela en utilisant des sources de confiance ou alors utiliser des outils qui pourront analyser notre Docker.

Et enfin nous pourrons aussi privilégier l'utilisation d'un Fail2ban qui va analyser le nombre de tentative d'accès et bloquer l'utilisateur après 3 tentatives par exemple grâce à son adresse IP. Cela veut dire qu'avec l'adresse utilisée pour se connecter, l'utilisateur ne pourra plus essayer de se connecter pendant un moment prédéfinis.