Rapport - Analyse de sécurité
2Tl2 - Groupe 3

Louis Arys Brogniet Geoffrey Martin Perdaens
Jean-Michael Tang

1er juin 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 VPS :** Les plus grands risques ou failles qui puissent survenir sur nos VPS sont l'accès à **Root en ssh** qui est vivement déconseillé, le **brute force** qui permettra de découvrir nos mots de passe et les **droits trop présents pour les utilisateurs**

— **Le DNS :** Le **cache-poisonning** est un grand risque sur nos DNS, c'est à dire une corruption d'envoi de données via une adresse ip falsifiée. Mais il y a également les **attaques DDos**, qui, sont but, est de bloquer le fonctionnement de la ressource. Et enfin les messages non authentifié comme les attaques de type **Man in the Middle**

— **Le mail : Les spams et les fishings** sont les dangers majeurs pour nos mails. Envoyer un grand nombre de mail en peu de temps peut bloquer une boite mail et envoyer des emails avec le domaine de la société pour tromper les clients et non clients en les dirigeants vers un formulaire dans le but de leurs soutirer des informations. Les abus de scripts automatisés peuvent atteindre n'importe quel service qui est connecté à internet.
Le service mail est donc exposé à des risques, si la configuration est mal faite, il y a des risques qu'un envoi de mail n'est pas envoyé à une seule personne, mais à tout le monde, c'est ce qu'on appelle plus communément un relais ouvert. Le système se retrouvera sur plusieurs listes noires : si c'est le cas, il y a peu de chance que des mails importants arrivent à leur destination, cela posera problème pour les clients.

— **La confidentialité des mails :** Étant donné que des protocoles comme SMTP n'ont aucune priorité en matière de sécurité et/ou de confidentialité, ils peuvent partager des données avec n'importe quel autre système sans protection. De ce fait, les informations privées peuvent être divulgué sans consentement aux administrateurs locaux, la CIA, la NSA ou même, des hackers.

  Le Service d'information et de recherche Sociale (SIRS) recueillent les données personnelles et les protègent (en Belgique en tout cas). Cela ne veut pas spécialement dire que nos données ne seront jamais lue : il suffit qu'on soit désigné comme étant suspect pour qu'ils aient une raison justifiable de fouiller dans nos données personnelles. Un hacker professionnel

qui aurait réussi à outre-passer la sécurité du SIRS peut également fouiner dans nos données personnelles : ce scénario est peu probable certes, mais reste plausible. "Les données à caractère personnel ne peuvent être recueillies et traitées que dans les limites prévues par la législation, et ne seront pas communiquées à des tiers sans autorisation légale ni utilisées à des fins commerciales ;
La loi Only Once du 5 mai 2014 rend obligatoire le principe de la collecte unique de données par les instances publiques auprès des citoyens et des entreprises : réutilisation obligatoire des données disponibles dans des sources authentiques auxquelles le SIRS a accès ou qui sont mises à disposition via des services d'intégration comme Fedict et la Banque carrefour de sécurité sociale (BCSS)." Selon ces lois, nous sommes protégés des divulgations de données personnelles, mais il y aura tout de même des personnes qui y aurons accès comme les inspecteurs et les services de sécurité, même si d'autres loi les obligent à garder le silence professionnel.

— **VOIP :** Pour cette partie, les risques sont nombreux comme par exemple la **découverte du mot de passe par brute force** (courant sur SIP), **usurpation d'identité, l'écoute, les spams, les abus d'utilisation** et encore plus. C'est pour cela qu'une bonne sécurisation est nécessaire.

— **La base de données :** Le risque sur la base de données est le changement d'une donnée ou d'une table à cause d'une mauvaise sécurité de cette base de données. Un autre risque sur notre base de données est le vol ou la corruption de nos données ainsi que les attaques DDos.

3 Les solutions aux risques

— **Les VPS :** Nous avons enlevé l'accès à ROOT et nous avons supprimé une connexion via mot de passe et remplacé par une passphrase et clé ssh via keygen. Nous avons aussi installé Fail2ban qui va exclure après 5 tentatives de connexion l'adresse ip qui essaye de se connecter.

— **Le DNS :** Nous avons différencier le DNS externe et interne afin d'avoir une architecture sécurisée.

— **Le mail :** Nous avons mis en place une sécurité StartTLS, une mise en place d'un outil anti-spam et d'un mot de passe crypté et non plein est en construction. Nous avons également mis en place un service Fail2ban. Fail2ban n'est pas un outil de sécurité, mais un outil qui aide à réduire les risques qu'un intrus s'introduise dans le système. Si la sécurité est mauvaise, fail2ban ne pourra pas empêcher des hackers de s'introduire, en revanche, si la sécurité est bonne, les tentatives de brute force, ddos et autres approche lourdes seront moins fréquente, puisque fail2ban permettra de les réduire en bannissant les adresses IP source venant de ces

derniers. Cela permettra d'alléger les logs du système, ou en tout, d'éviter une surcharge.

— **VOIP :** Nous avons mis en place deux sécurité pour notre service, UFW qui est un pare-feu et qui va interdire toutes connexions venant de port non autorisés, et Fail2ban qui va bannir les adresses IP après 5 tentatives et pour une durée déterminée de 1 jour.

— **La base de données :** Un mot de passe sécurisé est mis en place.

— **Web :** Une mise en place d'HTTPS en cours sur les sites.