Power Marketing

Robin Assistant

Maintenance Report - V1.0

Summary

1. Introduction: *3*

1.1 Project overview 3

2. General: *4*

2.1. Incidents 4

2.2 Updates and patches 4

2.3 Certificates 4

2.4 Maintenance 4

3. Security *5*

3.1 Data 5

3.2 Malicious activity 5

1. Introduction:

1.1 Project overview

Robin Assistant is a new assistive software solution for people with special needs and their careers in performing everyday activities. It is used for different types of brain conditions: autism spectrum, Down syndrome, Alzheimer's disease various forms of dementia, and other sorts of brain injuries.

This document will show all information about the web-app dashboard project plan for the caretakers and the activity-app for the clients.

2. General:

2.1. Incidents

The Robin Assistant application will contain an automatic backup system which stores daily backups on the local server and weekly backups on a cloud server in case of a hard drive failure.
The applications itself can be downloaded, pulled and merged from the GitHub repository which can be rebuild like a regular Laravel application.

2.2 Updates and patches

It's important to keep the system always up to date. The server is running on a Ubuntu 20.04 OS which can be updated with the following commands:

- Sudo apt-get update
- Sudo apt-get upgrade

The commands above will update the server but not the applications.
In order to update the applications we use Composer and NPM. These can be executed within the application directory be executing:

- Npm update
- Composer update

This will update the application the latest stable releases of the libraries.

2.3 Certificates

A valid certificate is very important to the end-users. Without a valid SSL certificate, the website wont function corrects, and all sent and received data will be publicly visible.

Since SSL certificated expire after around 90 days, we use a tool called "certbot".
Certbot will daily check all your server's certificates and update them automatically when needed.
In order to update certificated manually you'd need to execute: "sudo certbot –cert-only".

2.4 Maintenance

In order to put a website offline in maintenance mode we can use a simple Laravel provided command.
This command is "php artisan down".
This command will put your application in a save locked environment where end-users can't access it.
In this way you can update or patch your application if needed.

3. Security

3.1 Data

The AVG law requires applications to collect as less data from an end-user as possible. All useless and not important data will not be stored on the database to prevent breaking this law.

All secure information such as passwords will be encrypted with the latest hashing algorithms to prevent hackers from easily breaking the code and there will be a minimum password requirement to prevent passwords from being brute forced quickly.

3.2 Malicious activity

1. The application will be on a strictly secure server with a firewall that only allows administrators to access the server from within the local network to prevent hack attacks from the outside.

2. Brute forcing user accounts will be reduced by limiting the amount of password attempts by 5 per minute.

3. Server authentication logging will be set to the maximum log option to be able to view all incoming authentication requests and filter / block malicious attempts.

4. Port scanning probes will be blocked by our firewall and most ports will only be accessible within the local network or with a custom proxy.