Android Security Guideline

Introduction

Due to the large success of Android operating system and a rising number of installations worldwide (nearly 75% in Europe) there is also an increasing number of threats based on Malware and Spyware.

One example for such a Spyware is the Remote Administration Tool (RAT) "Dendroid" which was identified in March 2014. This software was embedded into a normal App and was offered inside the Googe Play Store.After installation of Dendroid the program was able to take over the control about Camera, Microphone and so on.

In order to prevent such a misuse of Gigaset Android phones it's the goal of this document to provide a guideline for information security procedures. According to this the document defines the most important measures for Android hardening.

Security Guidelines

1. Update firmware and operating system to the latest version

Gigaset is always working to improve the reliability and security of the complete product portfolio.

This means that the phone firmware is permanently enhanced to face threats like malicious software.

Thus it's absolutely recommend to keep the device firmware always up to date.

For the same reason it's best practise to keep also the operating system up to date.

2. Installation of a Virus and Trojan scanner

Despite all security procedures the likelihood is quite high to get malware or spyware. To detect these threats it's crucial to install a Virus and Trojan scanner. By means of these programs the system has got the ability to find and remove malicious software.

3. Don't root the device

The shipped Gigaset Android devices has got no "root" administrator permissions. However, the internet offers a lot of software to obtain these rights and to adjust the own device in a deep level.

Please be aware that these changes incorporates a lot of risks.

Due to this it's not permitted to conduct such changes. Rooting administration of a device affects the loss of all Gigaset warranty.

4. Usage of Google Playstore

It's recommend to use only Google Playstore and to disclaim for the usage of third party App stores. Nevertheless it's necessary to respect certain security rules for the Google Playstore download.

It's a best practice to check the trustworthy of each software . This can be done by a App rating check. Negative ratings and comments should be considered. If ratings or comments are missing the customer should balance the benefits and risks in terms of the new software.

5. Restriction of permissions

The selection of permissions has got a large impact for the operation of a Android device. Thus it should be strictly considered which permissions are really necessary and which not.

So the level of permissions should be respected for each App installation. Not every application needs the access to the internet or to special hardware components like cameras or other service resources.