Security at RAKwireless

Introduction

RAKwireless delivers innovative Internet-of-Things (IoT) products to our global community. We are your all-in-one IoT solutions provider that ranges from end node sensors to cloud computing. While focusing on hardware production, the company also delivers software solutions to manage and maintain the networks of IoT devices it provides to the customers. Our growing number of distributors and partners help us to get closer to developers around the world. RAK is committed to delivering practical and effective IoT solutions to people. We continually improve our products to safeguard user data. We follow the principles of the ISO/IEC 27001:2022 for Information Security Management System (ISMS). As for the Privacy of Users' personal information, RAKwireless strives for maintaining ongoing compliance with the General Data Protection Regulation (the "GDPR") as a leading data protection and privacy legislation. We are committed to the principles inherent in the GDPR and particularly to the concepts of privacy by design and privacy by default. RAKwireless takes comprehensive measures to ensure effective data protection and privacy of its users. In this document, we aim to explain our approach to security.

Compliance and data protection

Compliance

RAKwireless follows the principles of the ISO/IEC 27001:2022 for Information Security Management System (ISMS), and is ISO/IEC 27001:2022 certified. The ISO/IEC 27001:2022 is a widely known international standard that is aimed at implementing, maintaining, and continually enhancing information security within the context of the organization and its products.

As for the Privacy of Users' personal information, RAKwireless strives for maintaining ongoing compliance with the General Data Protection Regulation (the "GDPR") as a leading data protection and privacy legislation. We are committed to the principles inherent in the GDPR and particularly to the concepts of privacy by design and privacy by default. Our goal is to ensure:

- transparency with regard to the use of personal data;
- that any processing activity is lawful, fair, transparent, and necessary for a specific purpose;
- that the personal data is accurate, kept up to date, and erased when no longer necessary;
- that data is processed securely and safely.

Customer data privacy

RAKwireless takes comprehensive measures to ensure effective data protection and privacy of its users. Inter alia, such measures include purpose limitation, data minimization, and storage limitation. We process as minimum data as feasible and according to the appropriate legal grounds.

The access to personal data is strictly limited to the dedicated team members and processors who reasonably need such access.

Organizational security

Security policies and training

The hiring process at RAKwireless includes screening for candidates and additionally criminal, credit, immigration, and security checks where it's required and local labor law or statutory regulations permit.

At the very beginning, employees have to get acquainted with the RAKwireless policies and procedures (e.g., Information Security Policy, Acceptable Use Policy) and agree with the "Terms and Conditions", before being provided with access to internal systems.

All RAKwireless's employees receive education, awareness, and training, which covers topics like social engineering, malware protection, password security, classification and handling of information, etc., and some specific, as relevant for their job function.

Security program and team

RAKwireless security program is aimed to define the high-level security requirements and information security strategy. Its goal is to protect the company and users to the maximum extent possible against security threats that could jeopardize their integrity, privacy, reputation, and business outcomes.

The security program is based on the ISO/IEC 27001:2022 standard, where the specialists are focused on the implementation and enhancement of security controls for each of the following domains:

- Security Policy
- Risk Management
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- Information Systems Acquisition, Development and Maintenance

- Supplier Relationships Management
- Information Security Incident Management
- Business Continuity Management
- Compliance

Our security specialists are professionals and enthusiasts of Cyber/Information Security, with well-known certifications in the Information/Cyber Security and Security Testing domains.

Incident management

Our company follows an incident management process for the security events that may affect our product, systems, endpoints, etc. The process defines how the incidents are identified, investigated, classified by type and severity, contained and minimized, and how the affected services and systems are restored, and mitigated to prevent new cases.

Information security incidents are handled by the dedicated Incident Response Team (IRT). In cases where an incident may relate to personal data, the Data Protection Officer (DPO) is involved in the IRT.

Supplier management

RAKwireless cooperates with third-party organizations that supply goods and/or services (e.g., solution hosting, SaaS vendors, etc.) to the company to maximize the value. Before starting cooperation with a 3rd party vendor, RAKwireless conducts the Security Assessment, Risk Assessment, and evaluates Legal and Regulatory requirements. Chosen 3rd party vendors are assessed from the security/risks point of view on an annual basis.

User access management

Access to the information, services, and resources of RAKwireless is provided according to the least privilege principle on a need-to-know basis and only for authenticated users. All requests for additional/non-standard access rights are granted only after a formal request and approval from the System/Process Owner and Management team. Owners of the systems and services or other authorized persons periodically review current access rights and when needed adapt or revoke them.

User endpoint protection

RAKwireless endpoint security controls are defined based on best-in-class security practices. RAKwireless endpoints are required to be protected by using an anti-malware solution that continuously monitors for malicious software, a host-based firewall to prevent malicious activity, a strong password policy, a lock-when-idle mechanism, host encryption, and OS patching.

WisGateOS2 product security

We develop and maintain the product in accordance with strict confidentiality, integrity and availability requirements based on the OwASP Application Security Verification Standard.

Software Development Security

In the development process of the WisGateOS2 product, we apply the Secure SDLC approach which significantly increases the level of security of the product. Security is integrated from the early beginning of the development and follows the development process to the release phase.

During all steps of the development, we utilize security principles like separation of duties and least privilege to prevent malicious activity in case of security breaches.

Security of Design

Security engineers are involved in defining the security requirements and reviewing the system design to avoid creating weaknesses in the product architecture. This approach allows the implementation of the latest protection mechanisms.

Before development of a new feature begins, the threat model is created to anticipate serious security issues that may arise in the product design. It allows us to 'fix' the problem before it arises, and apply the most effective mitigations to the product design.

Security of Development

Security is always a component of the development process and has a significant influence on it. Security review and testing are part of the feature development workflow without exceptions.

As soon as code is deemed feature-complete, it has to pass through different security testing methodologies, which include:

- Static application security testing (SAST): To check source code for known vulnerabilities.
- Software composition analysis (SCA): To identify all the open-source integrated into the product and check if it is vulnerable to known vulnerabilities.
- Security code review: To check the implementation of security mechanisms and identify weaknesses that can be missed by the automation approach (SAST).
- Manual security testing: To validate if all specified on design phase security requirements are in place. Also, by utilizing this approach the product is tested in an individual way, which is not provided by the automation.

No product's features can be released without security team approval because the early identification of issues is a key to product quality.