ADVICE ON INDUSTRIAL SECURITY

Measures for enhanced component security

TABLE OF CONTENTS

1. INTRODUCTION

To protect your assets from external attacks, it is not enough to just select secure components, you also need to configure them correctly. According to the shift-left principle of security, you should therefore pay attention to the correct use of your E-T-A components during the planning and deploying of your system.

This document provides you with general information on the secure use of E-T-A components. The user documentation for the individual products provides more detailed information on how to apply these instructions in practice and which additional measures should be taken to increase security. Apply the instructions in this document to maintain the confidentiality, integrity and availability of your data and systems.

In addition to applying these guidelines, we also recommend introducing processes in your organization to enforce information security measures. This includes, for example, the introduction of an information security management system (ISMS) in accordance with ISO/IEC 27001.

2. SECURITY MEASURES FOR COMPONENTS

The purpose of the following instructions is to increase the security of your components during installation, operation and disposal. However, to ensure the security of your system, it is not enough to apply the individual instructions in isolation. Rather, a holistic defense-in-depth approach is required, in which you coordinate the security measures across all components and set up several layers of protection.

2.1 Securing communication channels

- Do not connect your components to public networks.
- Prevent unauthorized access to your networks and components by setting up a firewall.
- Isolate your systems from the rest of the company infrastructure as far as possible.
- Disable unused communication channels in your components.
- If you need to access your systems and components remotely, set up secure channels such as VPN or HTTPS.

2.2 Protection against unauthorized access

- If your E-T-A component has a user management system, only assign the least required privileges to each user.
- Change the default login password after deploying a component.
- Only use passwords for your components that comply with the security guidelines of your organization.
- Change the login data to your components regularly, as required by your organization's security guidelines.
- Restrict physical access to your components, e.g. by using lockable control cabinets.
- Make use of tamper detection measures, e.g. by sealing devices that support this.

2.3 Maintaining security

- Use the latest firmware for your components. You can find software updates on the respective product pages at www.e-t-a.de.
- Regularly check for updates for your components.
- Pay attention to the associated release notes when applying a software update.
- Regularly check the E-T-A PSIRT security advisories to see how you can work around potential vulnerabilities. Details on the PSIRT can be found in section 3.
- Do not store sensitive data like passwords in plain text and consider using a password manager.
- Utilize event logging features and evaluate these logs regularly and/or automatically.
- Perform regular backups of your component configuration.
- Perform a threat risk analysis on a regular basis. Update your threat model using the vulnerabilities published for your components.

2.4 Secure disposal

- Delete sensitive data from the components after decommissioning.
- Reset your components after decommissioning using the commands provided for this purpose.

3. REPORTING SECURITY VULNERABILITIES

The E-T-A Product Security Incidence Response Team (PSIRT) is the central point of contact for reporting and publishing security vulnerabilities and security advisories. The team handles reports of security incidents in our components and works closely with you to develop mitigation measures as quickly as possible.

Vulnerabilities in E-T-A components and workarounds are published on the PSIRT homepage in the form of security advisories. Stay up to date by regularly checking the website for news.

Further information on the work of the PSIRT, contact details and reports on security vulnerabilities can be found at www.e-t-a.de/psirt.