ZVEI: Die Elektroindustrie

Discussion Paper

Horizontal Process Requirements for the Security Life-Cycle Management of IoT Products

June 2020

German Electrical and Electronic Manufacturers' Association

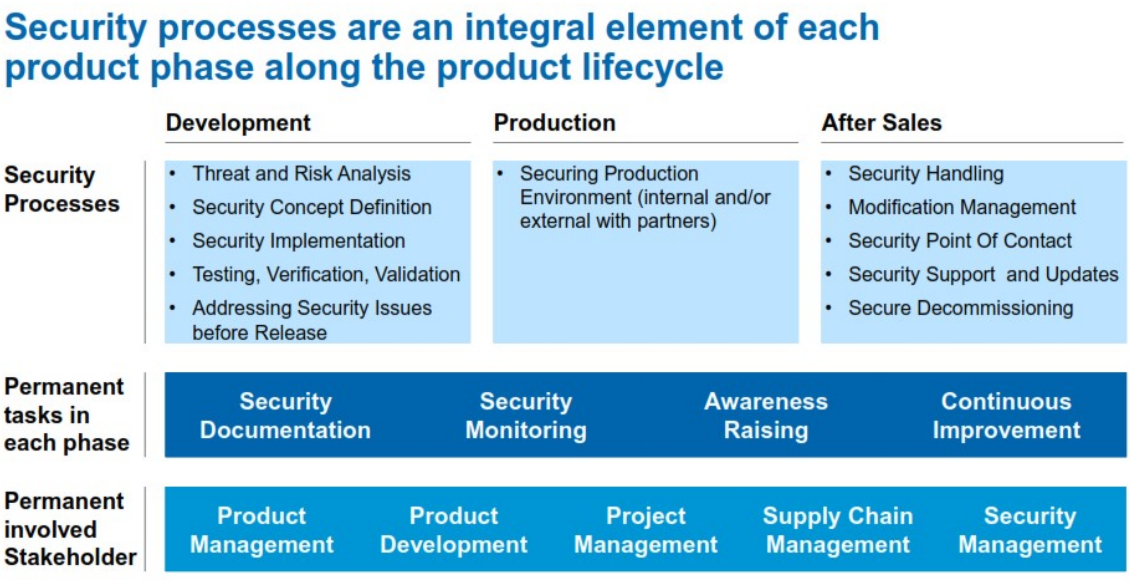
Content

Understanding and Scope of this Paper 3
Overview: 3
1. Product Development 4
1.1 Threat and Risk Analysis 4
1.2 Security Concept Definition 4
1.3 Security Implementation Concept 4
1.4 Security Concept Verification and Validation 4
1.5 Addressing Security Issues before Release 4
2. Product Production 5
Securing Production Environment 5
3. After Sales 6
3.1 Vulnerability and Incident Handling 6
3.2 Modification Management 6
3.3 Point of Contact for Security Issues 6
3.4 Security of Updates and Security Updates 6
3.5 Secure Decommissioning 6

Understanding and Scope of this Paper

This paper outlines cross-domain security process requirements for IoT manufacturers at a meta-level with an international focus. Its purpose is to identify fundamental processes for the three core security competences: prevention, detection and reaction. By implementing these processes manufacturers may achieve basic security hygiene for their IoT products and organization. The requirements outlined here are in accordance to international standards addressing security. However, the paper is solely voluntary in its nature and does not determine the implementation of specific norms and standards. Manufacturers can choose how to fulfill these requirements. As such, this paper represents a common understanding and industry opinion of ZVEI members. If there is need for new (sectoral) process standards, we strongly recommend this document for the minimum requirements, which should be included in an aforementioned standard.

Overview:



1. Product Development

1.1 Threat and Risk Analysis

A process should be implemented to

- analyze the intended environment and context of the product (e.g. user, scope, intended use, 3rd party components, network to be integrated in etc.),
- identify assets to be protected,
- perform threat modelling and
- assess identified risks.

Threat and Risk Analysis of the product should be aligned with the manufacturer‘s overall risk management processes.

1.2 Security Concept Definition

A process should be implemented to derive the security requirements from the threat and risk analysis for the whole product lifecycle (development, installation, operation, maintenance and decommissioning). Determined requirements should be transferred to specific security measures for the product and its environment.

1.3 Security Implementation Concept

A process should be implemented to ensure a secure product implementation for the derived security measures. This could be supported by following good security implementation practices.

Note: An implementation concept could include (example):

- Technologies used in the product (especially those of external interfaces),
- Good practices to safeguard the listed technologies, recommendations for implementation such as Unit Tests, Static Code Analysis, Vulnerability Scans and Testing,
- Security Guidelines for the programming languages used
- Measures that safeguard against known weaknesses, e.g. the prevention of SQL-injection

1.4 Security Concept Verification and Validation

A process should be implemented to ensure that the implementation of the security measures fulfill the security concept.

1.5 Addressing Security Issues before Release

A process should be implemented to ensure that all security related issues are addressed before release.

2. Product Production

Securing Production Environment

A process should be implemented to assess and secure the operational environment of the product's production. This should include internal organizational and technical measures and/or contractual/legal provisions and guidelines when dealing with external production partners.

Note: This process is of particular importance if sensitive data such as certificates, keys or other credentials are used or installed on the product during production.

3. After Sales

3.1 Vulnerability and Incident Handling

3.1.1 A process should be implemented to ensure, that all products and their environments are continually monitored over the whole product lifecycle in order to identify security vulnerabilities and changes in the product or its environment. For all identified vulnerabilities the vulnerability management process should be started.

3.1.2 The vulnerability management process should detect, evaluate, and, where necessary, remediate vulnerabilities in products in a timely fashion. Remediation measures should be provided for a defined period of time. They include but are not limited to patches and updates.

3.1.3 An incident handling process should be implemented, that enables the coordination and the management of a cybersecurity incident including assigning responsibility for completion of all necessary activities for the incident.

3.1.4 A process should be implemented to inform affected parties about reportable security-related issues in a timely manner.

3.2 Modification Management

A process should be implemented to analyze, before launching a new product release (including 3rd party components), if there are security-related consequences. Regarding these changes the process steps for product development defined in chapter 1. should be performed.

3.3 Point of Contact for Security Issues

The manufacturer should provide a point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues.

3.4 Security of Updates and Security Updates

A process should be implemented that ensures integrity of all distributed software releases, updates and patches. For non-constrained devices authenticity should also be ensured. Those should be published according to the potential risk in a timely fashion.

3.5 Secure Decommissioning

A process should be implemented that ensures that for every product a user documentation is provided with guidelines for removing the product securely from use, e.g. secure removal of user data.

Horizontal Process Requirements for the Security Life-Cycle Management of IoT Products

Published by:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

ZVEI - German Electrical and Electronic Manufacturers' Association

Innovation Policy Department

Lyoner Str. 9
60528 Frankfurt am Main

Germany

Responsible: Marcel Hug

Telephone: +49 69 6302-432

E-Mail: Marcel.Hug@zvei.org

Editorial: ZVEI Project Team
Horizontal Security Requirements

www.zvei.org

June 2020