D1.10
Cyber-security guidelines for SMEs 2.0
version 1.0

PUBLIC

Anne Immonen
VTT Technical Research Centre of Finland Ltd
Kaitoväylä 1, 90571 Oulu
anne.immonen@vtt.fi

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 951813.

Project acronym Better Factory	**Project title** Grow your manufacturing business		**Grant agreement No.** 951813
Deliverable No. D1.10	**Deliverable title** Cyber-security guidelines for SMEs 2.0		**Version** 1.0
Type REPORT	**Dissemination level** PUBLIC		**Due date** 31.3.2024
Lead beneficiary VTT			**WP No.** 1
Main author Anne Immonen		**Reviewed by** Konstantinos Grevenitis	
Accepted by Project Coordinator Magnus Simons		**Accepted by Technical Coordinator** Anastasia Garbi	
Contributing author(s) Sami Lehtonen			**Pages** 18
VTT archive code VTT-R-01405-20		**Lead beneficiary archive code**	

Abstract

This deliverable describes the security guidelines required to run a testbed successfully and securely with a RAMP IoT or other Better Factory software installations for SMEs.

Project Coordinator contact	**Technical Coordinator contact**
Magnus Simons VTT Technical Research Centre of Finland Ltd Tekniikantie 21 Espoo, Finland E-mail: Magnus.simons@vtt.fi Tel: +358 40 820 6139	Anastasia Garbi European Dynamics SA E-mail: anastasia.garbi@eurodyn.com Tel: +30 6947566672

Notification

The use of the name of any authors or organization in advertising or publication in part of this report is only permissible with written authorisation from the VTT Technical Research Centre of Finland Ltd.

Acknowledgement

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 951813

HISTORY OF CHANGES

Date	Version	Author	Comments
4.12.2023	0.1	Anne Immonen (VTT)	Document draft
5.12.2023	0.2	Anne Immonen (VTT)	Poll summary and analysis
18.12.2023	0.3	Anne Immonen (VTT)	Security guidelines
18.3.2024	0.4	Anne Immonen (VTT)	Minor modifications
19.3.2024	1.0		Final version

TABLE OF CONTENT

HISTORY OF CHANGES 4

EXECUTIVE SUMMARY 6

ACRONYMS 7

1 INTRODUCTION 8

2 SECURITY POLL 9

2.1 Questionnaire 9

2.2 Results analysis 9

3 SECURITY GUIDELINES 11

3.1 Authentication 11

3.2 Certificates 11

3.3 Security certification 11

3.4 Guidelines in relation to company policies 12

3.5 GDPR 12

3.6 Backups 12

3.7 Network topology 12

3.8 Intrusion Detection and Prevention Systems 12

4 CONCLUSIONS 14

APPENDIX A 15

EXECUTIVE SUMMARY

This deliverable describes the updated security guidelines for a secure implementation design for a testbed with a RAMP IoT for SMEs. More thorough and comprehensive guides exist for SMEs to implement security in their organization and services. Deliverable D1.1 covered the cyber security features of a RAMP IoT system and D1.4 actual configuration and hardening of RAMP IoT platform services. Deliverable D1.5 covered the first version of security guideline considerations of the platform. This document is a continuation of the guidelines.

Two small polls on security issues were carried out within Better Factory project. The results of the polls were taken into account in creating these security guidelines. The number of the responses of the polls was low, so any statistical analysis of the results was not considered meaningful. However, the status, trends and deficiencies in security issues in the involved organizations could be discovered. There were no significant differences between the answers.

In the context of Better Factory project, it is necessary to provide guidance on how the produced components or the Better Factory platform can be taken into use in SME organizations. The purpose of this deliverable is to provide such information.

ACRONYMS

EEA	European Economic Area
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
TLS	Transport Layer Security

1 Introduction

All companies must take care of information security. Especially in the case when personal information is handled within the company, the requirements of data privacy are strict and regulated with an EU law. In the context of this project, it is necessary to deliver guidance on how the produced components or the Better Factory platform can be taken into temporary and test use in a SME organization. This deliverable aims at providing such needed information.

A small poll on security issues was carried out within Better Factory project earlier, and the second, follow-up, poll was implemented in November 2023. The number of answers was low in the first poll (only three returned questionnaires), but the second poll received 10 responses. The results provided a small view of the status of security issues in organizations. The results of these polls were considered in creating these security guidelines.

2 Security poll

2.1 Questionnaire

A small Cyber Security poll was held to gather information on current practices. The poll was implemented as a questionnaire that was sent to members of the Better Factory project in November 2023. The questions are added as an Appendix A. The questionnaire aimed at gathering knowledge on which of the designed KTEs are used in each organization. The same kind of questionnaire was implemented at the beginning of 2023. Here we examine what kind of security practices the organizations implement and what kind of threats and development targets they have identified.

Ten responses were received. The summary of the APPS used can be detected in Table 1.

Table 1 Solutions used in organizations' KTEs.

DOMAIN	Solution (APPS)	Used in organization's KTE
Cognitive HRI	Pose Detection & Tracking	XXXX
	FAMS (Fatigue Monitoring System) + IM (Intervention Manager)	XXX
Logistics Automation	Agent Optimization	X
	Person Detection & Tracking	X
	Heatmap of Human Occupancy	X
Resource Optimization	ProOpt (Process Optimization)	XX
	BPO (Business Process Optimization)	XX
	Superset Dashboard	XXXXXXXXXX
Production Reconfiguration	APM (Advanced Plant Model)	XXXXXXX
	MPMS (Manu Process Mgnt System)	X

2.2 Results analysis

The results show good awareness of security issues, and company policies already exist. About a third had have in-house cyber security experts, a third had outsourced, and the rest (only tree) had neither (see Figure 1). It can be detected that security issues are taken seriously in the organizations. None of the respondents had an ISO 27001 certification. Of the internationally recognized standards, one had ISO standard for environmental management systems (EMS).

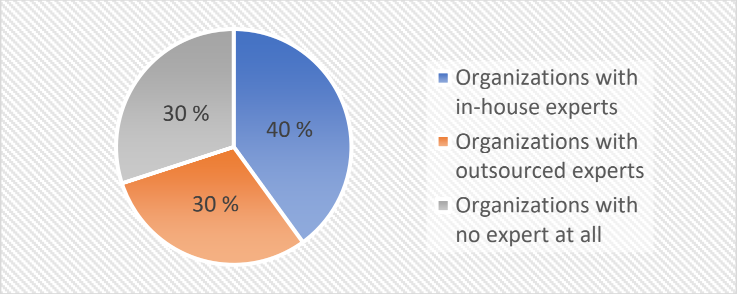

Figure 1 The types of cyber security experts in organizations.

Internal needs for access control in the KTE was recognized by five respondents, as well as five respondents informed that they have a need for access control in external interfaces in the KTE. As an authentication method, nine used username and passwords. Six of the respondents reported that they provide an interface for the customers, partners, or subcontractors in the KTE. Five of them were web apps or web interfaces, and one was a VPN tunnel. Only four used Public Key Infrastructure to encrypt messages. Two of them had own PKI, and two used third-party infrastructure. The fact that so many provided access for parties outside their organization and still didn’t provide rigorous identification may need consideration from the security viewpoint. Rigorous proof to confirm the identity of the parties would be essential especially when handling private, personal information.

Seven of the respondents reported that they manage personal information in their KTE. All of them manage this data according to company GDPR policy. The rest did not manage personal information in KTE. It is important that all the companies have understood the GDPR requirements of personal data. However, it must be noted that there still may be differences between countries of what is classified as personal data, although the rules exist.

Only three of the respondents reported that they use Intrusion Detection System/ Intrusion Prevention System or similar technologies. One of these had built in IDS/IPS and one used honey pot mechanism.

Four of the respondents reported that the backups in their KTE is done according to company GDPR policy. The company guidelines are necessity especially when personal data is processed and stored, as GDPR involves also data storing. Four of the respondents reported that their back-ups are handed by the third-party services or cloud providers. This is a bit risky in the case of personal data, if it is unclear whether these service providers adhere to the GDPR or whether the cloud is located physically outside EU area.

The most valuable assets within the KTEs of the respondents varied from data to designs and products. Five of the respondents reported having security challenges when implementing the KTE. These included security of access and commands from FIWARE, data confidentiality and integrity, access management, protection against attacks, monitoring and auditing, and deploying the security systems.

Moving KTE technology from test to production use requires a new cyber security set up for four of the respondents.

3 Security guidelines

As the results of the questionnaire shows, the security issues are well noticed in the companies. However, the usage of well-known standards is important to protect the company, its environment, and all operations. EU provides clear guides for SMEs on security controls[1] and on implementing information security management system (ISMS) according to ISO27001[2]. None of the companies that responded the poll utilized security standards.

3.1 Authentication

Using passwords as an authentication method is nowadays still very popular, although it has been a major vulnerability in recent years. Information on secure use of passwords and requirements related its use can be found in the Password guideline document by NIST3. Password is characterized as a memorized secret authenticator, as a secret value is intended to be chosen and memorized by the user. These must be sufficient by complexity and secrecy that it would be impossible for an attacker to guess or otherwise discover them. Using passwords, however, do not provide rigorous proof of parties' identity. In RAMP, the IoT platform is based on FIWARE, which uses Keyrock to identify users. The authentication scheme in RAMP IoT platform is based on Open Auth 2 authentication scheme (presented in D1.1.) which allows authentication and authorization security to services and applications.

3.2 Certificates

Secure communications require encryption of data, which in turn requires key management and authentication of communicating parties. The most common form of encryption is a Public Key Infrastructure (PKI) that can be used to encrypt a message to transfer information securely through network. PKI is a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. Digital certificate is an electronic document used to prove the validity of a public key. PKI is required for activities where more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred. PKI is natively supported with most of the components used in RAMP systems. In RAMP, the communication between the RAMP IoT and RAMP marketplace is encrypted with Transport Layer Security (TLS). TLS is a security protocol that is used to provide privacy and data integrity for Internet communications, and thus to implement secure web apps. A single RAMP-IoT server should embody a single set of private keys and a corresponding certificate. These can be utilized in several TLS ports. The RAMP marketplace itself is authenticated via a third-party certificate.

3.3 Security certification

The European standardization organizations officially recognized by the EU (CEN, CENELEC and ETSI) provide standards that help SMEs to prove the quality, safety, reliability and performance of their products and services, and the compliance with legal and technical requirements. ISO 27001[4] is a well-known standard for information security, cybersecurity, and privacy protection. The standard protects the confidentiality, integrity, and availability of information by means of processes, instructions, risk management and management tools. The standard contains several mandatory requirements considering, for example, the organization's operating environment, leadership, planning, support functions and the operation itself, that everyone acting in accordance with the standard must implement. The usage of internationally recognized standard provides clear guidelines for organizations manage their information security, and it improves the customers and co-operation parties' trust in the organization.

[1] SME Guide on Information Security Controls https://www.sbs-sme.eu/sites/default/files/SBS%20SME%20Guide_Information%20Security%20Controls.pdf last accessed 18.12.2023

[2] SME Guide for the Implementation of ISO/IEC 27001 On Information Security Management https://www.sbs-sme.eu/sites/default/files/publications/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min%20%281%29.pdf last accessed 18.12.2023 .

[3] https://pages.nist.gov/800-63-3/sp800-63b.html#sec4

[4] https://www.iso.org/standard/27001

3.4 Guidelines in relation to company policies

Separate test installations can be managed either according to existing company policies or with separate policies, which in turn require that the test setup is isolated from the rest of the IT systems of a company. Depending on company policies and, possibly certified, defined processes, these exclusions (i.e. installation or configuration in violation of the mentioned policy) need to be properly documented.

3.5 GDPR

General Data Protection Regulation (GDPR)[5] is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). All EU countries started to apply it since 2018. The GDPR requires that when collecting and handling personal data, the person whose data is involved (i.e., data subject) must have given a consent for the collection and processing of data. In addition, all parties involved in the processing of this data should sign the agreement, and the data subjects must be informed of the parties handling their personal data. According to GDPR, the data collector is obligated to provide at least the following information:

- Who is handling, processing, and storing the data.
- Why is the data processed.
- What is the legal basis for the handling.
- Who is the receiver of the data.

The persons whose data is being collected has to be given the following rights to their personal data:

- Free access to their own personal data, and the right to transfer data from a system to another.
- The right to correct and supplement their own personal data when they feel that the data is incorrect, defective or inaccurate.
- The right to remove the personal data (the right to be forgotten).
- The right to refuse the usage of the personal data in solely automatic processing.

3.6 Backups

Data backups are essential to ensure that the data is not lost in the case of system failures, after a security attacks of disasters. The backup copy can be used to recover or restore the state in case the data is damaged, deleted or lost. Two to three copies of data should be maintained, possible in at least two different storage formats. One copy should also be stored off-site, for example, in a cloud. The back-ups are best carried out according to existing company policy. However, the third-party services also can take care of back-ups. Usually, the back-ups are automatically handled by the cloud provider as a part of their services. The GDPR must also be noted in the case of data back-ups, as the GDPR also involves data storing. Also, it must be noted if personal data is transferred outside the European Union or the European Economic Area.

If an existing backup system can’t be used for this purpose, it is advised to note which are the parts that need to be backed up. These include at least configuration settings, and the data stored in the system. If the system is run as a virtual system, a snapshot of the full system can be put in backup plans.

3.7 Network topology

If company policy or information security management system requires, the platform might need to be separated from the rest of the network. In such setup the platform acts like a DMZ (demilitarized zone – a screened subnet) to the company network. This does not mean that the DMZ would be fully exposed to the public internet. Requirements for such a setup vary and are largely dependent on the existing network and therefore they can’t be covered fully within the scope of this document.

3.8 Intrusion Detection and Prevention Systems

Both IDS (intrusion detection system) and IPS (intrusion prevention system) are necessary security technologies to monitor network traffic and to identify any malicious behavior and block the exploit attempts

[5] https://gdpr.eu/

before completing. IDS is a passive monitoring solution (a piece of installed software or a physical appliance) that monitors for detecting and notifying cybersecurity threats. Depending on the context, an IDS can be deployed on a particular host, when it monitors only host's processes and network, or it can be deployed the network level, when it monitors the entire network. IPS is a technology that also strives to identify potential security threats, but IPS also takes action to block the identified threats and prevents the intrusion from occurring. Several types of intrusion detection methodologies are available with variations in configuration and cost.

4 Conclusions

As new security threats appear constantly, the SMEs implementing or using BF platforms need to consider what new requirements or scenarios arise when using them with their production environment. Five organizations had already encountered security challenges already when implementing the KTE. The poll revealed that organizations have security experts (in-house or third party), and they adhere organization policies. Therefore, they are aware of the importance of security issues and that the security policies and guidance are required to be defined already at the organization level. Four organizations had identified that new cyber security set up is required when moving their KTE technology from test to production. The identification of new kinds of requirements or scenarios is essential for SMEs before using Better Factory platforms with their production environment.

Appendix A

What is the name of your KTE?

What APPSs did you use?

DOMAIN	Solution (APPS)	Used in KTE
Cognitive HRI	Pose Detection & Tracking	
	FAMS (Fatigue Monitoring System) + IM (Intervention Manager)	
Logistics Automation	Agent Optimization	
	Person Detection & Tracking	
	Heatmap of Human Occupancy	
Resource Optimization	ProOpt (Process Optimization)	
	BPO (Business Process Optimization)	
	Superset Dashboard	
Production Reconfiguration	APM (Advanced Plant Model)	
	MPMS (Manu Process Mgnt System)	

Do you have in-house or outsourced cyber security experts?		
In-house		
Outsourced		

Do you have any security certification?		
No,		
Yes, ISO27001		
Yes, other,		

Did you have internal needs for access control in the KTE?		
No		
Yes,		

Did you have need for access control in external interfaces in the KTE?		
No		
Yes,		

Did you use cloud services in the KTE?		
Yes		
No		

Have you identified your most valuable assets within the KTEs?	
What are they?	

What kind of authentication methods did you use?		
User name, password		
Single sign on		
Other		what:

What interfaces in your network did you provide for your customers, partners or subcontractors in the KTE?

Did you utilize PKI (Public Key Infrastructure) in your KTE?		
Yes		
No		

Did you have your own PKI infrastructure, or do you rely on 3rd party CA/RA (Certificate Authority/Registration Authority) capabilities?		
Own		
3rd party		
Both		

Did you use one or many PKI infrastructures (customers/subcontractors)?		
One		
Many		

Did you use IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) systems or similar technologies?		
No		
Yes		what:

How did you do your backups in your KTE?		
No backups		
According to company policy		
Other		

How did you manage personal information in KTE (GDPR) – if any?		
Did not manage personal information in KTE		
According to company GDPR policy		
Other		what:

What security challenges did you have in implementing the KTE?

Will moving KTE technology from test to production use require a new cyber security set up?

H2020 Innovation Action – This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 951813.