D2.7

Privacy Risk Modelling and Contingency - Final Report

This deliverable presents the final research results for ANASTACIA Task T2.3. It updates the general data protection requirements and privacy risks to be addressed, the generic mitigation and contingency actions to be considered, and the specific approaches to be implemented when addressing all the ANASTACIA use-cases.

Distribution level	PU
Contractual date	30.04.2019 [M28]
Delivery date	14.05.2019 [M29]
WP / Task	WP2 / T2.3
WP Leader	UMU
Authors	Adrian Quesada Rodriguez (MAND) Cedric Crettaz (MAND) Bojana Bajic (AS) Jorge Bernal Bernabé (UMU) Alejandro Molina Zarca (UMU) Stefano Bianchi (SOFT)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat SpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.ANASTACIA-h2020.eu

TABLE OF CONTENTS

INDEX OF TABLES

PUBLIC SUMMARY

This deliverable presents the final research results of ANASTACIA Task 2.3 “Privacy Risk Modelling And Contingency”. It updates the general data protection requirements and network-level privacy risks to be addressed, the generic mitigation and contingency actions to be considered, and the specific approaches to be implemented when addressing four of the use-cases selected by the ANASTACIA consortium for the demonstrator of the framework.

To accomplish this goal, the deliverable updates the examination on the normative and technical frameworks that surround and determine ANASTACIA’s privacy-enhancing efforts (detailed in D2.3). Additionally, the document updates the seven privacy risks to be monitored by ANASTACIA, namely:

1. Unauthorized access or disclosure of personal data.
2. Unauthorized modification of personal data.
3. Unauthorized or inappropriate linking of personal data.
4. Unauthorized removal or deletion of personal data.
5. Excessive collection or retention of personal data.
6. Lacking protection of traffic information and location data.
7. Impairment of data subject’s rights.

Finally, the document performs an ISO-based risk analysis on the 11 ANASTACIA use-cases to identify the consequences, threats, impact and likelihood of the identified privacy risks and recommend detection, protection, mitigation and contingency actions for each.

The results of this work will be integrated in the final ANASTACIA demonstrators, and the risk assessments will directly inform the work of WP5.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document aims to update D2.3 and remodel relevant privacy risks to be addressed by ANASTACIA and to develop the contingencies for such risks whenever necessary. This task is threefold and adopted the systematic and sequenced methodology used in D2.3 for the identification of requirements and risks. For each identified privacy risk, a set of generic measurement points as well as contingency measures have been identified. Finally, the document aims to perform a throughout analysis of the whole range of ANASTACIA use-cases.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- ANASTACIA D.1.1 "Holistic Security Context Analysis."
- ANASTACIA D1.2 "User Centred Requirements Initial Analysis."
- ANASTACIA D1.3 "Initial Architectural Design."
- ANASTACIA D2.2 "Attacks Threats Analysis and Contingency Actions."
- ANASTACIA D2.3 "Privacy Risk Modelling and Contingency Initial Report"
- ANASTACIA D2.6 "Attacks Threats Analysis and Contingency Actions Final Report"
- ANASTACIA D5.1 "Dynamic Privacy and Security Seal Model Analysis"
- ANASTACIA D5.2 "Dynamic Privacy and Security Seal Monitoring Service"

1.3 REVISION HISTORY

Version	Date	Author	Description
0.1	19/01/2019	Adrian Quesada Rodriguez	Initial draft of new version of the deliverable
0.2	02/02/2019	Adrian Quesada Rodriguez; Alejandro Molina Zarca	Review of previous deliverable
0.3	06/03/2019	Adrian Quesada Rodriguez	Risk identification complete
0.4	01/04/2019	Adrian Quesada Rodriguez	Review of Use-cases and integration of additional Information
0.5	05/04/2019	Adrian Quesada Rodriguez	Added Information on questionnaires
0.6	10/04/2019	Adrian Quesada Rodriguez, Jorge Bernal Bernabé	Modified deliverable structure, added Annex 1
0.7	20/04/2019	Adrian Quesada Rodriguez	Initial clean version
0.8	24/04/2019	Cedric Crettaz	Definition of mitigation/contingencies and impact based on D6.2
0.9	30/04/2019	Adrian Quesada Rodriguez	Updated section 1 and conclusions

1.0	04/05/2019	Adrian Quesada Rodriguez	Final version for review
1.1	09/05/2019	Adrian Quesada Rodriguez, Stefano Bianchi, Alejandro Molina Zarca	Reviewed, final version

1.4 LIST OF ACRONYMS

Acronym	Meaning
BMS	Building Management System
CPS	Cyber-Physical System
DPIA	Data Protection Impact Assessment
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSPS	Dynamic Security and Privacy Seal
DLDS	Distributed Ledger and Distributed Storage
eIDAS	Electronic Identification and Trust Services (eIDAS) Regulation
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GUI	Graphical User Interphase
HSPL	High-level Security Policy Language
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Protection System
ITU	International Telecommunications Union
MEC	Mobile Edge Computing/Multi-access Edge Computing

Acronym	Meaning
MitM	Man-in-the-Middle
MSPL	Medium-level Security Policy Language
NIST	National Institute of Standards and Technology
PDP	Personal Data Protection
SDN	Software-defined networking

1.5 TERMS AND DEFINITIONS

Term	Definition
Audit	This refers to a systematic, independent and documented process for obtaining audit evidence [records, statements of fact or other information which are relevant and verifiable] and evaluating it objectively to determine the extent to which the audit criteria (including policies, procedures or other requirements) are fulfilled. (International Organization for Standardization, 2011)
Certification	This Refers to the provision by an independent body of written assurance (a seal or certificate) that the product, service or system in question meets specific requirements.
Cyber-physical systems	ICT system able to interact in continuous way with the physical system it operates in. The system is composed of physical elements equipped with computational capabilities and it presents three characteristics ("the three C"): computational capabilities, communication and control capabilities. (Cambiaso, Mongelli, et al., 2017, p. 3)
Cybersecurity:	Field of the computer science working on threat analysis, vulnerabilities identification and management and to the risk associated to ICT assets, with the aim of protect such systems from (internal or external) cyber-attacks potentially able to create (direct or indirect) damages with impact higher than a pre-defined threshold (e.g. economic, reputation, socio-politics damages, etc.) (Cambiaso, Mongelli, et al., 2017, p. 3)
Information security management systems	This refers to a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. (International Organization for Standardization, 2013).
Information Technology Security	Is the process of implementing measures and systems designed to securely protect and safeguard information (business and personal data, voice conversations, still images, motion pictures, multimedia presentations, including those not yet conceived) utilizing various forms of technology developed to create, store, use and exchange such information against any unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby preserving the value, confidentiality, integrity, availability, intended use and its ability to perform their permitted critical functions. (www.sans.org)

Internet of Things	Common life objects (e.g. fridge, TV, door sensor, video-cameras, light bulbs, weather stations, etc.) are able to communicate among themselves and with the environment by exploiting an Internet connection to exchange data in real time, without requiring external devices demanded to manage the communication. (Cambiaso, Mongelli, et al., 2017, p. 3). IoT has been defined as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. (International Telecommunications Union, 2012)
Network function virtualization	Network architecture concept using IT virtualization technologies to virtualize entire classes of functions in order to design, deploy and manage networking services. (Cambiaso, Mongelli, et al., 2017, p. 3)
Personal data	Any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. (EU Data Protection Directive (95/46/EC))
Privacy impact assessment	A privacy impact assessment is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. (ISO)
Risk	Effect of uncertainty on objectives (ISO Guide 73)
Software-defined networking	Approach used in the computer network fields to provide network administrators the ability to initialize, control, update and manage in a dynamic way the network configuration through apposite interfaces and protocols and by abstracting low level functionalities of the network nodes. (Cambiaso, Mongelli, et al., 2017, p. 3)
Threat	Potential cause of an unwanted incident, which might result in harm to a system or organisation (ISO/IEC 27000:2016).

2 METHODOLOGY AND APPROACH

This deliverable updates and expands on the exhaustive and comprehensive analysis process carried out as part of ANASTACIA D2.3. To this end, a similar methodological approach was followed to:

- review the initial analysis with continuous feedback received from the partners involved in ANASTACIA WP2 and WP5; and
- expand the privacy risk model and contingencies, addressing the 11 use-cases envisioned by the project.

To this end, the following actions were performed:

1. **Review, update and synthetization of previous research**: which led to a clearer document structure, better aligned with the presentation of the privacy requirements for the ANASTACIA platform as a whole and a clearer description of both the privacy risks and the potential measurement points to be considered.
2. **Alignment with attack threats analysis:** A joint effort with partners was followed to update the list of enablers and monitoring capabilities which might be most relevant for determining the privacy status of a monitored system. This process was informed directly by the developments and inputs provided by partners to D2.2 and D2.6.
3. **Restatement of the ISO-based risk assessment methodology:** which was synthetized in section 5 to ensure clarity and readability of the document outputs.
4. **Privacy Risk Assessment and Contingency definition:** In order to comply with both the ANASTACIA DOA and the envisioned activities to be carried out throughout the project's demonstrators, a separate privacy risk assessment process was carried out for each envisioned use-case. These will be introduced in the project's DSPS as the system's baseline risk assessment (part of the eventual DPIA which should be carried out by the organization's DPO).
5. **Update of the privacy risk evaluation and contingency verification strategy:** In order to ensure alignment of the deliverable's outputs with the latest developments in WP5, an update to the strategy was proposed.

3 UPDATED CHARACTERIZATION OF ANASTACIA'S CAPABILITIES

"ANASTACIA is a framework for the management of complex networks and systems. Following technologies and scenarios are in particular addressed: Internet of Things (IoT), Software Defined Networks (SDN), Building Energy Management System (BEMS), Multi-access Edge Computing (MEC), also considering Network Function Virtualization (NFV) and Policy Based Management aspects." (Cambiaso, Mongelli, et al., 2017, p. 2). Considering the necessity to guarantee secure data transmissions and the sensitive nature of the information shared by the network, ANASTACIA aims to provide holistic and innovative tools for the detection, prevention and management of both security and privacy threats.

ANASTACIA's interest on IoT Security and Privacy is more than necessary: *"as the connectivity of objects exponentially increases, so are the possibilities for hacking into the system. It is noted that IoT covers a huge scope of diverse markets and the needs of security and privacy vary depending on the types of services. In order to find general requirements from the user perspective, we focus on the common risks coming from the IoT communication patterns that apply to heterogeneous IoT services and applications"*(Cambiaso, Mongelli, et al., 2017, p. 13). As such, the system's focus will be the detection of threats at a network-level to overcome the large range of possible attack vectors in the realm of IoT deployments[1].

"Cyber-security can be seen as a purely ICT related issue or as a legislative and regulation compliance problem. Nevertheless, it needs a new approach able to consider all the components of the system, in order to define a security plan able to effectively protect the commercial interests, the immaterial assets and the infrastructure of the organization, by protecting them from risks and threats that may potentially target the system." (Cambiaso, Mongelli, et al., 2017, p. 4). As this is particularly true when addressing privacy risks, ANASTACIA will incorporate network-level privacy enhancing mechanisms[2] which will make use of the functionalities listed above to address the security of processing requirements found in current personal data protection legislation, while incorporating human-based privacy impact verifications whenever necessary to ensure compliance and the protection of the rights of data subjects.

In order to achieve this goal, ANASTACIA will rely on a technical framework of "*policy-based network and security management to deal with cyber-attacks in CPS-IoT scenarios through SDN and NFV."* (Cambiaso, Mongelli, et al., 2017, p. 17). It will detect security and privacy vulnerabilities and react accordingly to mitigate both active[3] and passive[4] cyberattacks to the IoT/CPS deployments through one or more of the following functionalities[5]:

a) **Basic Security mechanisms for Software-defined networking (SDN)**
   - Traffic flow forwarding
   - Traffic flow dropping

[1] *"network-level security can be implemented across the entire range of IoT devices, rather than device-level security that is specific to a particular device; unlike device-level security that is embedded into devices and is hence difficult to upgrade, network-level security can be implemented in the cloud, and can be enhanced on a continuous basis; network-level security can be offered by a third-party who has expertise in this specific area, rather than by the device manufacturer who may not have the drive or the skills to implement security properly; network-level security adds an extra layer of protection that can augment any device-level security implemented by the manufacturer"* (Sivaraman, Gharakheili, Vishwanath, Boreli, & Mehani, 2015, p. 2).

[2] *"(…) In order to detect and resolve security/privacy issues for IoT, we propose an external entity (…) that develops, customizes, and delivers to the user extra safeguards at the network level for the IoT devices in their household. A simple example might involve (…) adding the appropriate access control rules that protect a specific IoT device, while a more complex example might involve dynamic policies that change access control depending on the context (e.g. the family members being present or absent from the house)"*(Sivaraman et al., 2015, p. 2).

[3]Which include packet crafting attacks (such as replay attacks, masquerading, malware and zero-day attacks); packet alteration attack (such as Man-in-the-Middle attacks); and service compromising attacks (such as SQL injection attacks, Denial of Service (DoS) and Distributed Denial of Service Attacks (DDoS), and their new modalities like Slow DoS (Cambiaso, Papaleo, Chiola, & Aiello, 2013), and Slowcomm (Cambiaso, Papaleo, & Aiello, 2017).

[4] Data interception attacks, including traffic analysis, sniffing/eavesdropping and keyloggers.

[5] *Annex 1 includes a table which provides further information on the currently deployed enablers, this information will be used by WP5 to inform DSPS users of the mitigation and contingency mechanisms implemented by ANASTACIA.*

- Traffic flow mirroring
- Traffic flow bandwidth reduction

b) Basic security mechanisms for IoT

- Power management (on/off control)
- Interface management
- Traffic protection management

c) Network Function Virtualization (NFV)

- Virtual firewall
- Virtual Intrusion Detection System (IDS)
- Virtual Intrusion Prevention System (IPS)
- Virtual switch/router
- Virtual honeypot/honeynet
- Virtual secure web proxy
- Virtual private network (VPN)[6]
- Virtual bandwidth control

These functionalities will be enriched by ANASTACIA's monitoring enablers:

- **Montimage Monitoring Tool (MMT)**: software able to analyse network traffic and extract protocols metadata. By using Deep Packet and Flow Inspection techniques (DPI/DFI)[7], the tool is capable of extrapolating metadata[8] and detect security breaches and attack and give this information in input to other modules of ANASTACIA and implement novel algorithms and systems able to counter cyber-attacks.
- **ATOS Security Incident and Event Management (XL-SIEM)**: These solutions provide cross-level cybersecurity event and information management capabilities. Different types of security systems can be integrated, correlating events across multiple layers and identifying anomalies in real-time. Its core capacities enable the decentralized compilation and distribution of sensor events[9] and provide strong correlation capabilities for the generation of alarms, providing the user with a vision of the security status of the deployed infrastructure.
- **UTRC Agents**: Which will be providing anomaly-based intrusion detection[10] that will be used to build a data-driven model based on collected operational data of the machines. This model will continuously monitor and analyse newly collected data in order to detect if a severe deviation from expected behaviour can be noticed.

The functionalities provided by these and other security-driven enablers will be fundamental towards the monitoring and prevention of security threats, which in turn shall enrich ANASTACIA's efforts to secure personal data. As such, from a legal perspective, the set of preventative controls and mitigation activities undertaken by ANASTACIA's security framework can be considered as necessary to comply with GDPR's art. 42[11].

[6] The Virtual Secure Web Proxy and Virtual Private Network enablers have been planned in the ANASTACIA architecture but will not be implemented in the final architecture, third party VPNs might be utilized instead to mitigate the associated threats.
[7] See footnote 5 in ANASTACIA D.2.3 for further clarification of the MMT Probe.
[8] See footnote 6 in ANASTACIA D.2.3 for further clarification of the MMT software capabilities.
[9] See footnote 7 in ANASTACIA D.2.3 for further clarification of the information submitted by the XL-SIEM agent to the XL-SIEM server.
[10] See footnote 8 in ANASTACIA d.2.3 for further clarification of the processes that support the UTRC Agents.
[11] Article 42: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

While security-based enablers of the ANASTACIA platform can be understood as included in personal data protection activities in compliance with the security requirements in article 32 of the GDPR, ANASTACIA has additionally developed privacy-specific enablers which enhance the capabilities of the platform beyond its initial network-level approach and protect data as it transits the network. These enablers include authentication, authorization and encryption tools[12] which will be implemented at the application layer.

Finally, the work described in this Deliverable will be heavily supported by ANASTACIA's Dynamic Security and Privacy Seal (DSPS)[13], which will seek to complement the actions of the end-user of the systems monitored by ANASTACIA (CISO/DPO) and facilitate his understanding of the complex outputs of ANASTACIA's technological enablers. To this end, the DSPS will seek to inform the end-user (DPO/CISO) on the most relevant privacy and security issues while supporting the integration of ANASTACIA's insights with organizational due-diligence of controls and compliance activities (towards maximizing transparency and accountability). Particularly, the DSPS will:

- Introduce a privacy-by-design and by default compliant architecture, services and graphical user interface (GUI) that seek to combine the certainty and trustworthiness of conventional certification schemes with real-time certification surveillance capabilities through the real time dynamic monitoring (provided by ANASTACIA) of the certified system.
- Compile alerts and threats from ANASTACIA, compatible monitoring solutions (using the STIX 2 standard) and the end-user (CISO/DPO) and showcase them through a unified GUI, displaying IoT/CPS privacy and security information while providing decision support capabilities, and data visualization (considering accessibility/ease of use requirements).
- Empower the end-user by enabling the client's Data Protection Officer (DPO) and Chief Information Security Officer (CISO) to provide feedback to the raised alerts directly through the GUI and to enhance the information obtained from the monitoring system with technical, legal, and organizational documentation. This data will be stored in a privacy-by-design distributed storage solution (powered by Shamir Secret Sharing Scheme), which will be associated with the DSPS blockchain-based seal ledger (Hyperledger Fabric), to ensure the data is non-repudiable, immutable, and easily verifiable in direct relation to the events showcased by the DSPS both by the end-user (for internal audit and compliance purposes) and associated certification bodies (to determine the validity of relevant certifications).

The Dynamic Security and Privacy Seal (DSPS) aims to provide a holistic solution to privacy and security monitoring, addressing both the organizational and technical requirements enshrined by the GDPR through the implementation of a layered process which should provide the end-user with a broad perspective over the state of the monitored system (which will consistently track and unify the organizational/human elements considered by personal data protection regulations with the technical insights provided by ANASTACIA's monitoring and reaction services). Once implemented, this process will not only provide advanced trust-enhancing information functionalities to ANASTACIA users, but will also serve as a surveillance solution for audit/certification/legal compliance purposes. It will generate a non-repudiable historic track of system variations and potential threats (technical and organizational) to the sealed system while enhancing the contextual information available to the client, auditors or regulatory authorities.

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. (…)" (European Parliament, 2016)

[12] See infra Annex 1 for a detailed examination of these enablers.

[13] These final list of DSPS capabilities will be described in the upcoming ANASTACIA D5.3.

4 APPLICABLE PERSONAL DATA PROTECTION REQUIREMENTS

This section aims to update the applicable legal requirements identified by Deliverable 2.3, contextualizing them vis-à-vis ANASTACIA's capabilities (particularly considering its focus on network-level monitoring and mitigation) and towards their implementation in the use-cases to be addressed by ANASTACIA according to D.1.2 and 6.2.

As defined by ANASTACIA D.2.3, the following list of requirements constitute an effort to synthetize the requirements found in the GDPR and other relevant sources into a set of technical requirements to be addressed by ANASTACIA's monitoring systems and enablers. The list of requirements found in this Deliverable is not aimed towards providing legal advice to end-users regarding their obligations under the GDPR, but rather as a first step towards the identification of potential risks that could be addressed or prevented by ANASTACIA's monitoring and reaction platform.

Req-1 Enable privacy safeguards by default

Summary description:

Privacy safeguards shall be enabled by default, without requiring further intervention by the user. This requirement stems from the GDPR, which states that "*The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons*"(European Parliament & European Council, 2016).

Associated enablers/components/functionalities:

- **Security enablers**: ANASTACIA can introduce preventative security mechanisms for network resources and databases, this includes the DTLS proxy, the CpABE data privacy enabler[14] and the Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems. These elements will be enabled by default and introduced pre-emptively to address issues in any devices in the network that do not include these functionalities.

Req-2 Identification of data categories, non-processing of special categories, and protection of traffic and location data

Summary description:

ANASTACIA should incorporate express organizational and technical measures to avoid the processing of sensitive data and/or the identification of sensitive data from any of the datasets and measurements available to the system (apply the data minimization principle and storage limitation principles, among others). Special care must be taken to identify the categories of data which might have been involved in a potential breach in the monitored system, to ensure that the correct remedial and informational measures are adopted.

Associated enablers/components/functionalities:

- **Channel Protection and encryption enablers**: by introducing encryption tools in communications within the network (and outbound communications) alongside basic anonymization techniques, ANASTACIA will help CISOs comply with this requirement.

[14] See infra annex 1

- **DSPS' DPIA**: ANASTACIA's DSPS will include a DPIA tool which will help DPOs to comply with this requirement by identifying the data categories that are to be processed. This is a fundamental part of the organizational activities towards ensuring that no unauthorized special categories are processed.

Req-3 Data management and respect of data subject rights

(information / access / rectification / restriction / objection / deletion)

Summary description:

This requirement aims to fulfil several of the rights granted by the GDPR to data subjects, including the rights of access, rectification, opposition and deletion of personal data. This requirement has several additional implications: a) In compliance with the right of information, the data subject is to be informed as soon as possible after a breach to his/her personal data has taken place; b) the right of access entails also the requirement to ensure that the system upon which such right is to be exercised is available as soon as possible after facing a data breach, so as to ensure the data subject remains in control of his personal data. Finally, all necessary measures are to be incorporated to ensure that whenever a request for deletion has been received from the data subject, any controllers or processors which possess copies of the information should be informed, asked to comply with such request.

Associated enablers/components/functionalities:

- **Authorization enablers**: While ANASTACIA is not aimed to address application-level data protection activities, some of its enablers can support data management activities (CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems).
- **DSPS DLDS**: A key element of the planned implementation of the DSPS is the deployment of a secure storage and ledger system, which should be introduced to integrate organizational compliance activities into the security and privacy alert report lifecycle (see ANASTACIA D5.1 for further information).

Req-4 Data retention

Summary description:

A reasonable retention period should be set, after the expiration of which, data should be erased or de-identified. Unnecessary personal data should be erased by the system without undue delays. All processes related to ANASTACIA end-users should utilize reasonable or non-extensive data retention periods as well as implement any technical measures as necessary to ensure that unnecessary personal data are neither requested nor registered by the system (storage limitation and data minimization principles). Effective deletion of the data should be ensured and transparency on the followed procedures kept towards the end-users.

Associated enablers/components/functionalities:

- **DSPS DLDS**: The DSPS has been developed in a privacy-by-design and by default compliant manner to ensure the data stored therein is not stored beyond what is strictly necessary for compliance or legal accountability purposes. To this end, the blockchain ledger functionality has been designed to store only document hashes and perform proof of existence activities, while the documents managed by the distributed storage are independently managed and can be deleted as required. Furthermore, none of the associated functionalities require the processing of personal data without proper legal basis.

Req-5 Deidentification of Personal Data

(Anonymization, Pseudonymization, Non-identifiability)

Summary description:

The GDPR recognizes that the rights of access, rectification and erasure (including the right to be forgotten), restriction of processing, and data portability shall no longer be applicable when the controller of personal data is able to demonstrate that it is not able to identify a data subject. This requirement then focuses on the information and practices that are necessary to ensure that identifiability[15] is no longer possible.

Associated enablers/components/functionalities:

- **CpABE data privacy enabler**: ANASTACIA will introduce functionalities capable of adding access control, communication channel security and encryption to those devices in the network that do not support these elements by default.

Req-6 Records and audit of processing activities and disclosures

Summary description:

This requirement should be introduced and considered for all monitoring activities for which ANASTACIA is utilized *"based on the assumption that the ANASTACIA framework would be deployed in the context of personal data processing activities which are not defined by ANASTACIA itself, yet by the entity deploying ANASTACIA's system as a service; in that regard, ANASTACIA will typically fulfil the tasks of a Data Processor, and in so doing it provides some means to achieve the purposes set by another entity, the Data Controller*"(Bianchi et al., 2017, p. 62).

Associated enablers/components/functionalities:

- **DSPS**: The DSPS has been designed to help CISOs and DPOs to comply with security requirements (such as evidence collection and generation/safeguard of audit logs). Furthermore, it includes DPIA tools to enable the organizational activities and reports required from DPOs/CISOs by the GDPR.

Req-7 Security of processing

(prevention of unauthorized access, alteration, disclosure and destruction of personal data)

Summary description:

This high-level requirement aims to ensure the introduction of technical and organizational security safeguards to protect personal data by both the monitored IT systems and ANASTACIA. From an organizational point of view, the requirement addresses the need to define, implement (and update) security mechanisms and policies to the very design of the system.

Associated enablers/components/functionalities:

- Security enablers: ANASTACIA can introduce preventative security mechanisms for network resources and databases, this includes the DTLS proxy, the CpABE data privacy enabler and the Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems (among others).
- DSPS: ANASTACIA will complement the security of processing controls with direct actions of CISOs and DPOs, thus helping them plan and report on the organizational controls that must be introduced.

[15] De-identification is a *"General term for any process of removing the association between a set of identifying data and the data subject"*(International Organization for Standardization, 2008, p. 3).

Req-8 Data breach information

Summary description:

In direct relation with the transparency and accountability principles enshrined by the GDPR, the ANASTACIA system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, in order to enable that user to fulfil its obligations to notify data breaches to competent Data Protection Authorities and concerned data subjects.

Associated enablers/components/functionalities:

- DSPS: ANASTACIA will immediately potential security and privacy issues to DPOs and CISOs to minimize the time required for identifying any data breach that takes place within the monitored networks. Furthermore, the DSPS GUI will introduce some functionalities aimed at showcasing the remaining time before the data breach information report is to be submitted to end-users and data protection authorities and will record the rationale for the submission or non-submission of this report.

Req-9 Encryption of personal data by default

Summary description:

All personal data should be encrypted whenever it is stored or transferred, and strong encryption mechanisms[16] should always be used.

Associated enablers/components/functionalities:

- **Security enablers**: ANASTACIA can force encryption of data streams in the network and request the encryption of some of the data in the devices through its DTLS proxy and CpABE data privacy enablers
- **DSPS**: it will use state of the art encryption methodologies to secure any personal data related to CISOs and DPOs to minimize any potential data breach.

Req-10 Update and review privacy measures

Summary description:

Technical and organizational measures to ensure the privacy of end-users should be implemented and periodically updated/reviewed as necessary to ensure their effectiveness. Organizational and technical processes to ensure the effectiveness of security measures are required by the GDPR and constitute part of ANASTACIA's principal objectives. Generally, this requirement calls for audits and cross-verification of the security measures that have been implemented, and of the verification mechanisms themselves to maximize accountability and transparency and ensure the security and confidentiality of personal data.

Associated enablers/components/functionalities:

- **Policy editor**: Which will enable the CISO to update the technical security mechanisms implemented to prevent and mitigate potential threat scenarios.
- **DSPS**: The ANASTACIA DSPS will provide the end-user the opportunity to generate new DPIAs and to update them accordingly to ensure the lessons learned from the alerts are incorporated in the privacy policies of the organization.

[16] Cryptographic protocols: TLS, IPsec, Kerberos, PPP with ECP, ZRTP, etc.

5 PRIVACY RISK ASSESSMENT AND CONTINGENCY PLANNING

This section will aim to develop the high-level technical and human-based protection, detection, mitigation and contingency activities necessary to address each identified risk in the diverse ANASTACIA use-cases. To this end, the activities and strategy introduced in ANASTACIA D2.3 will be revisited and updated whenever necessary in consideration of the associated research outcomes detailed in D2.6 and D6.2.

The section is divided in three key parts: the restatement and update of the privacy risk assessment methodology used in D2.3; the restatement and update of the relevant privacy risks (particularly vis-à-vis ANASTACIA capabilities); and a case-by-case analysis of each one of the ANASTACIA use-cases.

5.1 PRIVACY RISK ASSESSMENT METHODOLOGY

According to ISO 31000/2009, *"Risk assessment is the overall process of risk identification, risk analysis and risk evaluation"* (International Organization for Standardization, 2009, p. 17). This section will be subdivided in accordance to this definition and shall follow ISO/IEC 31010 guidance on the risk assessment techniques to be implemented. Once risks have been correctly assessed, a set of contingencies based on current ANASTACIA reaction capabilities will be described.

1. Risk identification

The first step in performing an assessment is the generation of "*a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives (…) Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered"* (International Organization for Standardization, 2009, p. 17).

The first step towards identifying potential privacy risks is the definition of risk criteria which *"should reflect the (…) values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements"* (International Organization for Standardization, 2009, p. 17). As defined throughout previous sections of this research, relevant criteria in the context of ANASTACIA are given by the GDPR[17] (and secondarily by the e-Privacy regulation). The GDPR clearly focusses on one type of risk: adverse risk to the individual. The risks to the rights and freedoms of individuals of "varying likelihood and severity" may result from personal data processing which could lead to "physical, material or non-material damage" (European Parliament & European Council, 2016, Recital 75).

2. Risk analysis

[17] This criterion has been further expanded by the Art. 29 Working Party (WP 248) to enable the identification of high-risk processing. According to this document, high risk processing includes "*Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35(3)(c)).(…) Sensitive data: this includes special categories of data as defined in Article 9 (…) This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data (…)Datasets that have been matched or combined, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject (…) Innovative use or applying technological or organisational solutions: (…) (Article 35(1) and recitals 89 and 91) (…) the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedom. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. (…). For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy (…). [and finally] When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91). (…)*(Article 29 Data Protection Working Party, 2017, p. 8).

"Risk analysis involves developing an understanding of the risk. [it] provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. (…) Risk is analysed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account. (…) consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts."(International Organization for Standardization, 2009, p. 18).

This supports what ISO/IEC 29134 defines as the objective of privacy risk analysis: *"to analyse the potential consequences and threats of the privacy risks identified, and to estimate their respective levels of impact and likelihood"*.

i. Consequence identification

This deliverable builds upon the outputs of D2.3 and streamlines the consequence identification process to focus on the consequences for data subjects of a potential data breach. Thus, the following classification will be followed:

1. *"Negligible: PII principals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).*
2. *Limited: PII principals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).*
3. *Significant: PII principals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).*
4. *Maximum: PII principals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as unserviceable debt or inability to work, long-term psychological or physical ailments, death, etc.)."*(International Organization for Standardization, 2017, p. 32)

As defined in D2.3, it is recognized that consequences vary depending on the severity of the breach (i.e. amount of information extracted, classes of personal data affected by the breach, etc.) and *"may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."*(European Parliament & European Council, 2016, Recital 85). As consequences vary depending on the nature of the monitored system and the organizational controls introduced as part of the deployment, ANASTACIA's DSPS will integrate a Privacy Impact Assessment Tool to further support the risk assessment process, along with the design of the data protection strategy, of a monitored system[18].

[18] "*A strategy which embeds the protection of personal data – also in terms of security – into the design and functioning of the systems, needs therefore to be devised and followed. The strategy should incorporate the following elements: a) clear allocation of roles within the personal data processing, in order to: a. identify the data controller, the data processor(s) and the persons processing personal data under the authority of the controller or processor; b. formally bind the data processor(s) to guarantee a certain level of safeguards for personal data; c. map any potential stakeholder that may process personal data outside the European Union and formally bind it to guarantee a certain level of safeguards for personal data; d. assign the relevant authorization and authentication profiles to the persons processing personal data under the authority of the controller or processor. b) appointment of a Data Protection Officer, where necessary, in the light of the business and related data processing activities carried out by the data controller and/or processor; c) a Data Protection Impact Assessment (DPIA), where necessary; this process is anyway recommended for services, applications, systems that process personal data, even though they do not seem risky at the outset. The DPIA is a crucial step to ascertain whether*

ii. Impact

This element reflects the potential affectation to data subject that is expected to take place in case of a data breach in which the security designed mechanisms have been utilized. This evaluation goes beyond the mere restatement of the consequences, but rather should consider the defensive capabilities of the installed monitoring and reaction tools to identify the need for additional controls (be them technical, such as the installation of additional monitoring tools, or organizational, such as the adoption of particular preventative and/or reparative practices in the organization).

According to ISO, to estimate the level of impact, the consequences and planned or implemented controls should be considered to determine the potential damage caused by each identified risk. Considering the nature of the ANASTACIA monitored systems in the use-cases, an initial assessment has been introduced for each use-case in order to support this deliverable and the upcoming demonstrators. In the case of a real-life implementation, the Impact assessment should take place a-priori (along with the risk analysis items detailed here) in a Privacy Impact Assessment. ANASTACIA will integrate a DPIA tool in the DSPS to facilitate this exercise.

iii. Likelihood

Estimating the likelihood should consider the vulnerabilities of the supporting assets and the capabilities of risk sources to exploit them. The following reference classification is provided by ISO/IEC 29134 to clarify the likelihood of an event.

1. *Negligible: Carrying out a threat by exploiting the properties of supporting assets does not appear possible for the selected risk sources (…).*
2. *Limited: Carrying out a threat by exploiting the properties of supporting assets appears to be difficult for the selected risk sources (…).*
3. *Significant: Carrying out a threat by exploiting the properties of supporting assets appears to be possible for the selected risk sources (…).*
4. *Maximum: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy for the selected risk sources (…).*(International Organization for Standardization, 2017, p. 33).

Following the identification of relevant threat agents, identification of the capabilities of the potential threat can be performed. For the purposes of this Deliverable (and in accordance with the methodology of D2.3, the general threat agent classification found in (Casey, 2007) will be used and threat agent capabilities will be assigned as follows:

Generic classification:

1. None
2. Minimal
3. Operational
4. Adept

Relevant threat agent capabilities for the ANASTACIA use-cases:

---

personal data run risks in terms of security, and what the remedies are to those risks; d) implementation of the principles of data protection by design and by default throughout the whole data lifecycle; e) policies and procedures to periodically test the security resilience of a system (e.g., penetration tests, vulnerability assessments, etc.) and carry out the relevant remediation activities; f) adherence to codes of conduct and /or certification mechanisms for security of personal data g) a well-defined internal procedure to cope with any data breaches and notification thereof: a. to the competent Data Protection Authority, within 72 hours after having become aware of it; b. to the data subjects involved, without undue delay, unless any of the following conditions are met: i. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; ii. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; iii. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner." (Cambiaso, Mongelli, et al., 2017, pp. 36–37).

Threat Agent	Capabilities (Max skills)
Commercial establishments	Adept (4)
Insider threat	Operational (3)
IoT device providers	Operational (3)
IoT service providers	Operational (3)
Malicious attacker (Hacker)	Adept (4)
Malicious attacker (Script kiddy)	Minimal (2)
Marketing companies	Operational (3)
Online service providers	Operational (3)
State	Adept (4)

Table 1: Capabilities per threat agent

Based on this analysis, likelihood can be determined by ascertaining the relevant risks in each use case and the capabilities of the relevant threat agents.

3. Risk Evaluation

"The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered. (…) In some circumstances, the risk evaluation can lead to a decision to undertake further analysis." (International Organization for Standardization, 2009, p. 18).

The results of this evaluation will define the implementation of a set of predefined contingency activities, which should be tailored specifically to the context of each ANASTACIA deployment. For the purposes of this this deliverable, the proposed contingency actions will be defined in the framework of the use-case-specific approaches. In a real-life implementation of ANASTACIA, this evaluation should take place after each alert has been raised (and secondarily as part of the DPIA update process).

In the greater context of the ANASTACIA project, the final Risk Evaluation activities will be performed by both the CISO and the DPO through the DSPS GUI, which will record the resulting decisions and verify the actions of the end-users. More information on this process can be found in Section 6 Privacy Risk Evaluation and Contingency Verification Strategy for ANASTACIA.

5.2 ANASTACIA-RELEVANT PRIVACY RISKS

This section will seek to update the ANASTACIA-relevant Privacy Risks defined by D2.3. To this end, each risk will be summarily described and related with the legal requirements stated in Section 4. Additionally, measurement points[19] will be detailed along the relevant ANASTACIA protection, detection and mitigation capabilities.

Risk 1: Unauthorized access or disclosure of personal data (loss of confidentiality)

- Summary description: Access or disclosure to/of personal data generated or held by a device or object, by an unauthorized user or device.
- Associated requirements: 1, 2, 7, 9, 10
- Measurement points:

[19] Given the nature of the risk and ANASTACIA's capabilities, only high-level measurement points can be provided. Final risk assessment must be performed by DPO upon notification by ANASTACIA's DSPS.

    - Unusual account or device activity (as determined by time of the access, IP address, amount of data transferred, port used, etc.)
    - Unauthorized devices identified on the network
    - Unauthorized connections to external networks/servers according to the system security policies
- Relevant ANASTACIA Protection Mechanisms: HSPL authorization policies
- Relevant ANASTACIA Detection Mechanisms: VNF AAA Architecture
- Relevant ANASTACIA Mitigation Mechanisms: MSPL authorization, filtering, forwarding, privacy and channel protection policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems

Risk 2: Unauthorized modification of personal data (loss of integrity)

- Summary description: Modification or affectation to the integrity of the personal data generated or held by a device or object, by an unauthorized user or device.
- Associated requirements: 1, 2, 7, 9, 10
- Measurement points:
    - Unusual account or device activity (as determined by time of the access, IP address, amount of data transferred, port used, etc.)
    - Unauthorized devices identified on the network
    - Unauthorized connections to external networks/servers according to the system security policies
- Relevant ANASTACIA Protection Mechanisms: HSPL authorization policies
- Relevant ANASTACIA Detection Mechanisms: VNF AAA Architecture
- Relevant ANASTACIA Mitigation Mechanisms: MSPL authorization, filtering, forwarding, privacy and channel protection policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems

Risk 3: Unauthorized or inappropriate linking of personal data (Potential for data re-identification)

- Summary description: Unauthorized interconnection of two or more data sources by a device, object or user in the ANASTACIA-monitored network.
- Associated requirements: 1, 5
- Measurement points:
    - Unusual data flows between network devices.
    - Lacking encryption mechanisms in data flows within the network.
    - Unauthorized users/devices decrypting data flows
    - Devices not implementing anonymization protocols
- Relevant ANASTACIA Protection Mechanisms: Channel Protection, Anonymity, Encryption (TLS)
- Relevant ANASTACIA Detection Mechanisms: VNF AAA Architecture; IDS/IPS
- Relevant ANASTACIA Mitigation Mechanisms: MSPL privacy and anonymity policies, SDN switch; Firewall, VPN, TLS; CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems

Risk 4: Unauthorized removal or deletion of personal data (loss of availability)

- Summary description: Personal data is removed or deleted by an unauthorized user or device.
- Associated requirements: 1, 2, 7, 9, 10
- Measurement points:

    - Unusual account or device activity (as determined by time of the access, IP address, amount of data transferred, port used, etc.)
    - Unexpected disconnection of authorized device or object from the network
- Relevant ANASTACIA Protection Mechanisms: HSPL authorization policies
- Relevant ANASTACIA Detection Mechanisms: VNF AAA Architecture
- Relevant ANASTACIA Mitigation Mechanisms: MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems

Risk 5: Excessive collection or retention of personal data (loss of operational control)

- Summary description: Devices or objects do not respect restrictions on collection/retention of data defined by policies/configuration.
- Associated requirements: 1, 2, 3, 4, 5, 6, 7
- Measurement points
    - Devices/objects do not execute scheduled internal memory purges
    - Devices/objects are always active regardless of policies requesting disconnection when authorized users/devices are on the network
    - Devices/objects (or their capabilities/sensors) active when not prompted to by user
    - Unauthorized devices/objects compiling records of network traffic (Man-in-the-middle attacks)
- Relevant ANASTACIA Protection Mechanisms: HSPL authorization policies
- Relevant ANASTACIA Detection Mechanisms: DPI with the MMT-Probe; IDS/IPS; VNF AAA Architecture
- Relevant ANASTACIA Mitigation Mechanisms: MSPL authorization and privacy policies; virtual and physical firewall and router

Risk 6: Lacking protection of traffic information and location data

- Summary description: Information associated with device usage and/or location is disclosed or incorrectly protected. Lacking encryption of external communications (outbound/inbound) to the ANASTACIA-monitored network.
- Associated requirements: 1, 2, 7
- Measurement Points:
    - Unencrypted data streams to/from the ANASTACIA-monitored network.
    - Detection of brute-force attacks on encrypted devices/data streams (high number of access attempts)
    - Usage of insecure communication channels
    - Lacking traffic shaping mechanisms in encrypted communications through public networks
    - Improper assignment of device IDs (which might enable an attacker to identify the location of a device)
    - Unauthorized devices identified on the network
- Relevant ANASTACIA Protection Mechanisms: Data encryption (TLS), channel protection, HSPL authorization and channel protection policies
- Relevant ANASTACIA Detection Mechanisms: MMT DPI/DFI, virtual IDS/IPS, XL-SIEM; UTRC agents
- Relevant ANASTACIA Mitigation Mechanisms: TLS, virtual firewall and router, MSPL authorization and channel protection policies

Risk 7: Impairment of data subject's rights (System downtime)

- Summary description: Downtime or loss of control of the platform prevents information, access, rectification, restriction, objection and deletion processes by data subject.
- Associated requirements: 3, 7, 8
- Measurement points:
  - Detection of any of the monitored security threats (particularly DoS and DDoS)
  - Downtime in the system's GUI
  - System or devices not generating/saving logs
- Relevant ANASTACIA Protection Mechanisms: Channel protection (provide replication to avoid system downtime)
- Relevant ANASTACIA Detection Mechanisms: IDS/IPS, MMT DPI/DFI
- Relevant ANASTACIA Mitigation Mechanisms: Firewall and router, SDN switch

5.3 Use-Case-Specific Approaches: Privacy Risk Assessment and Contingency

This section will update and complete the use-case specific approaches detailed in ANASTACIA D.2.3 with the information found in D.2.6 and 6.2. Additionally, a use-case specific privacy risk assessment will be generated to emulate the core elements of the DPIA that would be likely be performed as part of the preparatory organizational activities of each use-case. These elements will be transmitted to ANASTACIA WP5 for their integration with the DSPS for demonstration and development purposes.

UC_0.1 - Secure/privacy-compliant Campus ICT infrastructure management

*"The Keamanan Campus is renowned for having a sophisticated **ICT/IoT infrastructure that controls all main buildings and facilities in the Campus**, which are under the direct responsibility of the Campus Manager, Mr Cahaya Budi.*

*In parallel to several BMS tools, Mr Budy has a brand new installation of an ANASTACIA-powered security & privacy monitoring solution, which allows him to have an immediate view of the status of the monitored infrastructure without the burden of checking different dashboards and inspecting technical logs: a nice Dynamic Security & Privacy Seal (DSPS) change its status according to detected threats, whereas a simplified UI summarizes the **main mitigation actions autonomously undertaken by the system**. The DSPS is green since the ANASTACIA-powered solutions was installed, several months ago, when Mr Budi also easily configured the main security policies according to the internal Campus regulations.*

*Yet, on a sunny Monday morning, an **anomalous traffic** is detected coming from a part of the network devoted to the management of **CCTV security cameras**, that **register videos from many different places** and forward them to a proxy server, **where streaming are pre-processed before relevant information (i.e. video sections in which people access restricted labs) are sent for storage and further inspection** to the CED in the central control room.*

*The potential threat is immediately detected by the system that, according to the security policies currently deployed, notifies Mr Budi changing the colour of the DSPS (from green to orange), suggesting **potential privacy breaches** that should be further investigated and starting the **definition of a mitigation plan** meant to limit any potential damage.*

The ANASTACIA-powered system takes action at three different levels:

*1) as for IoT devices under potential attack (this time, the CCTV cameras), the system momentarily **shuts them down to limit any further problem**;*

*2) at security level, by means of dedicated security VNFs, the system automatically **deploys several different virtual appliances (a firewall, an AAA server, an Intrusion Detection System)** in order to intensify the monitoring and reinforce the overall security level;*

*3) at network level, the system reconfigures the whole setup in order to leverage SDN functionalities and **temporarily isolate the part of the network under attack**, **redirecting the traffic to a duplicated pre-processing edge server** according to the newly defined network. **Cameras are then gradually reactivated**, in order to verify which specific device has been hacked or if the detected anomalous traffic has to be considered somehow a "false positive".*

Mr Budi, who is not a network expert and ignores most of the sophisticated network/security technologies that are used by the system to define and enforce the mitigation plan, gets a simplified report of the main actions undertaken.

*Furthermore, he also receives a **notice on potential privacy issues** that should be further investigated, since he is also the Campus Data Controller: in particular, the **identified threats**, impacting on a server that processes video streaming captured when access to restricted labs are detected by motion sensors, might have caused a **data leakage related to sensitive information**, and deserve further attention by the ICT staff, that is thus immediately summoned for an **internal meeting to verify any data leakage**.*

*Notwithstanding the mitigation actions were successfully undertaken and all functionalities were efficiently restored, the **DPSP stays orange, until a manual confirmation that also privacy issues have been duly addressed** is provided by Mr Budi and the ICT staff – both **security and privacy are then fully restored**."*

ANASTACIA D1.2 "User Centred Requirements Initial Analysis." (2017, p. 18)

Risk analysis

This scenario is focused on the execution of a malicious attack exploiting CCTV security cameras to compromise data confidentiality. In this case, once the attack is accomplished, the network is characterized by the presence of anomalous traffic, representing the effect of the attack.

Consequence identification

The scenario includes the following potential consequences:

- Unauthorized access to sensitive network resources and information, the extent of which is unknown: risk 1, 2, 4
- Potential linking and re-identification of data subjects by unauthorized devices: risk 3
- Spoofing of devices within the network (and access to network metadata): risk 5
- Anomalous outbound traffic (containing potentially sensitive information): risk 6

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_0.1	Maximum (3)	Significant (2)	Limited (2)	Significant (3)	Limited (2)	Maximum (4)	Negligible (1)

Table 2 UC_0.1 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[20]	ANASTACIA Controls	Impact level
Risk-1	Maximum (4)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler	Significant (2) Reason: Controls diminish risk of unauthorized access to personal data but data should be encrypted at application layer
Risk-2	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2) Reason: The possibility to modify the data is reduced.
Risk-3	Limited (2)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Negligible (2) Reason: Predefined encryption + channel protection diminishes risk
Risk-4	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2) Reason: authorization policies mitigate risk of data deletion
Risk-5	Limited (2)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Negligible (1): Reason: Enough controls along with limited consequences
Risk-6	Maximum (4)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Limited (2): Reason: ANASTACIA-defined encryption reduces this risk.
Risk-7	Negligible (1)	Channel protection; Firewall and router, SDN switch	Negligible (1): Reason: Organizational activities + security controls limits downtime

Table 3 UC_0.1 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[21]

[20] See supra section **Errore. L'origine riferimento non è stata trovata.**.

[21] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

UC_0.1	1, 2, 3, 4, 6	(unknown)	Adept (4) [22]	Maximum (4)

Table 4 UC_0.1 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for some of these risks could be **maximum** and even when considering ANASTACIA controls, there is a **significant** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

The security protection approach defined by ANASTACIA D2.2 and D2.6 recommends the following actions:

Detection:

- Detection of the attack can be accomplished by monitoring the network traffic generated by the CCTV cameras to identify anomalous conditions. This can be done by implementing anomaly-based detection algorithms.

Mitigation:

- Once the attack is detected, mitigation activities may be deployed at two different levels:
  - at the network level, it is possible to temporarily block communications (or connections involving external unwanted nodes/services) of the affected devices. A similar approach working at SDN level may isolate the affected nodes and redirect their network traffic to a secure internal location.
  - At the host level, it is possible to reconfigure the hosts to temporarily interrupt communications (by keeping images and videos retrieval from the environment). Although a more practical solution may trigger self-reboot or self-shutdown activities on the hosts, this may not be a good solution, since it would induce some sort of denial of service, hence, promoting a cyber-physical threat.

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible)

[22] The maximum likelihood is to be assumed in case of an unknown threat agent, as preventive and corrective measures should be deployed regardless of the assumed likelihood of an ongoing event.

of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Vulnerabilities of installed smart cameras and IoT devices
- Potentially sensitive nature of the data processed during the attack (performance of contextual analysis for each affected device)
- Location, data processed and additional capabilities (enabled or not) of devices in the network
- Procurement policies and vendors
- Maintenance policies
- Post-attack debriefing of ICT team

UC_MEC.1 - Spoofing attack on the security camera system

> *"A smart **security camera system** was installed in a city to prevent illegal actions. The recorded videos are sent to nearby MEC servers which can operate **a data pre-treatment before sending interesting information to the Cloud. A group of hackers wants to have access to the unprocessed videos to obtain critical information about citizens, in order to blackmail them**. They want to use **a spoofing technique** to make the cameras believe their servers are the MEC servers. **They managed to get the IP address of the server and they are able to use it**.*
>
> *To prevent this attack, Bob, the Administrator, will use ANASTACIA to ensure that the security camera systems **allows data exchange only between trusted equipment, by using secure protocols, authentication, correct network access controls and system design**. ANASTACIA will be used to monitor and use Penetration Testing modules to quickly react in order to eliminate this intrusion. ANASTACIA will be used to provide a quality-of-security seal that ensures that systems are correctly patched against such technique and will deploy Firewalls with DPI capability VNF in the proper locations."*
>
> *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* (2017, p. 22)

Risk analysis

This scenario is focused on the execution of a spoofing attack, aimed to impersonate (at the IP layer) a smart security camera data collector system to retrieve sensitive videos. The aim of the attacker is indeed to collect videos coming from the security cameras distributed on the territory, for blackmail purposes.

Consequence identification

The scenario includes the following potential consequences:

- Unauthorized access to sensitive information, the extent of which is unknown; man-in-the middle could lead to some data modification or loss: risk 1, 2, 4
- Compilation of unencrypted personal data by third parties: risk 3
- Access to the network and spoofing of sensitive network resources and metadata: risk 5
- Anomalous outbound traffic (containing potentially sensitive information and location data): risk 6

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_MEC.1	Maximum (4)	Negligible (1)	Significant (3)	Limited (2)	Significant (3)	Significant (3)	Negligible (1)

Table 5 UC_MEC.1 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[23]	ANASTACIA Controls	Impact level
Risk-1	Maximum (4)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler	Significant (2) Reason: controls (including encryption and data privacy) mitigate but cannot negate risk of access without additional controls at application layer
Risk-2	Negligible (1)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Negligible (1) Reason: limited risk of data modification + enough controls
Risk-3	Significant (3)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Limited (2) Reason: network-level controls mitigate but cannot negate risk
Risk-4	Limited (2)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Negligible (1) Reason: Risk of deletion based mainly on success of man-in-the-middle attack
Risk-5	Significant (3)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Negligible (1) Reason: limited risk + sufficient controls
Risk-6	Significant (3)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Limited (2) Reason: related to data access, access controls + intrusion detection limit risk
Risk-7	Negligible (1)	Channel protection; Firewall and router, SDN switch	Negligible (1) Reason: Risk related to system downtime (for ANASTACIA. Organizational controls are still recommended

Table 6 UC_MEC.1 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This

[23] See supra section **Errore. L'origine riferimento non è stata trovata.**.

exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[24]
UC_MEC.1	1, 3, 6	Malicious attacker (Hacker)	Adept (4)	Maximum (4)

Table 7 UC_MEC.1 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for some of these risks could be **maximum** and even when considering ANASTACIA controls, there is a **significant** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

The security protection approach defined by ANASTACIA D2.2 and D2.6 recommends the following actions:

Detection:

It is possible to detect the attack by also accomplishing SNMP data analysis and by designing proper routes configuration aimed to simplify detection of traffic from suspicious sources. In particular, by spoofing the IP address of the server, the attacker is supposed to adopt a different (and potentially suspicious) route.

Mitigation:

In order to protect the system from the attack, it is possible to adopt the following approaches:

- Data and communication encryption, coupled with authentication and authorization methods, adopted for communications between the smart security cameras and the collector service
- Proper routes configuration and packets filtering techniques to block traffic from suspicious sources

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved

[24] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Vulnerabilities of installed smart cameras and IoT devices
- Potentially sensitive nature of the data processed during the attack (performance of contextual analysis for each affected device)
- Location, data processed and additional capabilities (enabled or not) of devices in the network
- Procurement policies and vendors
- Maintenance policies
- Post-attack debriefing of ICT team
- Security controls regarding credential and certificate management, encryption mechanisms and other potentially affected devices in the network.
- Associated criminal activity and risk management actions aimed at mitigating potential cascade effects of this attack (due to potential leakage of security information on the black market, etc.).

UC_MEC.2 - Man-in-the middle attack on the MEC server scenario

*"A SME offers **security camera systems** to its clients by proposing **Mobile Edge Computing Solutions**. Eve is a **disgruntled employee** who wants to damage the company's image, by **spreading on the internet sensitive security videos from its employer's biggest client**. Their **security cameras are sending all of the recorded videos to MEC servers**, deployed by the security SME in its client sites, to operate the **information processing**. As Eve was working in this biggest client security cameras project, **she illegally kept all the credentials and certificates enabling her to decrypt the transmission between the MEC server and the cameras**, which allows her to organize a **man-in-the-middle attack**, and **download the videos** on her home computer.*

However, Bob, the administrator will use ANASTACIA to ensure that the system can react to minimize such attacks. ANASTACIA will assist BOB to provide an enforced network access policy and allow him to protect the change of credentials."

ANASTACIA D1.2 "User Centred Requirements Initial Analysis." (2017, p. 26).

Risk analysis

This scenario is focused on the execution of a man-in-the-middle attack against security cameras. The attacker is in this case an insider/employee of the targeted company, and his aim is to retrieve sensitive videos to store them illegally and/or share them outside of the network (e.g. on personal servers located in the house of the insider).

The attack is accomplished by exploiting credentials, certificates and video decryption keys owned by the employee/attacker. In addition, the attack exploits a man-in-the-middle approach to impersonate the smart camera management server system, to the eyes of the security cameras. Such server is supposed to retrieve videos from the security cameras.

Consequence identification

The scenario includes the following potential consequences:

- Unauthorized access to sensitive network resources and information, the extent of which is unknown: risk 1, 2, 4
- Unauthorized data flow decryption and personal data linking: risk 3
- Spoofing of devices within the network (and access to network metadata): risk 5
- Anomalous outbound traffic (containing potentially sensitive information): risk 6

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_MEC.2	Maximum (4)	Significant (3)	Maximum (4)	Significant (3)	Maximum (4)	Significant (3)	Negligible (1)

Table 8 UC_MEC.2 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[25]	ANASTACIA Controls	Impact level
Risk-1	Maximum (4)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler	Significant (3) Reason: Anastacia's controls should minimize the impact after the malicious user has been identified, however organizational protocols should be implemented to manage authorized users
Risk-2	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2); Reason: Upon detection, Anastacia authorization policies can mitigate the impact
Risk-3	Maximum (4)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Significant (3) Reason: once Man-in-the-middle alert is raised, affected devices can be isolated.
Risk-4	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2) Reason: ANASTACIA controls prevent unauthorized devices from deleting information.
Risk-5	Maximum (4)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Limited (2) Reason: upon detection of the threat, controls should mitigate risk
Risk-6	Significant (3)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Limited (2) Reason: The risk for location and traffic information being disclosed can only be partly reduced given the attack vector
Risk-7	Negligible (1)	Channel protection; Firewall and router, SDN switch	Negligible (1) Reason: No system downtime (for end-user point of view) is foreseen

[25] See supra section **Errore. L'origine riferimento non è stata trovata.**.

Table 9 UC_MEC.2 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[26]
UC_MEC.2	1, 3, 6	Insider threat	Operational (3)	Maximum (4)

Table 10 UC_MEC.2 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for some of these risks could be **maximum** and even when considering ANASTACIA controls, there is a **significant** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

Detection:

Detection of the MEC.2 attack may be accomplished by adopting and possibly combining different approaches:

- Logging certificates adoption to check validity, origin and owner of the certificates
- Monitoring host-to-host communications of the security cameras (e.g. at IP or MAC levels), in order to identify unexpected data shares
- Analysing network communications (e.g. through appropriate NIDS) to identify man-in-the-middle attacks exploiting for instance ARP tables
- Analysing of communications and related flows (we suppose that videos are shared/exfiltrated outside of the organizations by exploiting the network, and by avoiding low-rate transfers), it is possible to identify anomalous traffic generated from the host operating as the MITM; similarly, behavioural analysis activities may be adopted to detect man-in-the-middle attacks through the use of constraint programming techniques

Mitigation:

It is possible to mitigate the attack by working on the firewall devices, by limiting by design the communications of the security cameras, only allowing them to communicate with the legitimate smart security camera server (filtering, for instance, the ARP spoofing traffic identified by the detection process)

Regarding data exfiltration/sharing outside of the organization, it's possible to block connectivity of the affected devices, once transfers are identified. Also, it is possible to avoid packets encapsulation (used for tunneling purposes), by accomplishing deep packet inspection.

[26] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Affected videos: to identify relevant data subjects and sensitive data involved
- Processes and compliance activities performed by Human Resources department
- Security controls regarding credential and certificate management, encryption mechanisms and other potentially affected devices in the network.
- Associated criminal activity and risk management actions aimed at mitigating potential cascade effects of this attack (due to potential leakage of security information on the black market, etc.).

UC_MEC.3 - DoS/DDoS attacks using smart cameras and IoT devices

*"The smart security cameras and IoTs can be used for a **massive distributed denial-of-service (DDoS)** as the attack that disrupted U.S. internet traffic on the October 21th 2016, where the attacks were made possible by the large number of unsecured internet-connected digital devices, such as **home routers** and **surveillance cameras**. Even though some of these devices are not powerful computers, they can generate massive amounts of bogus traffic, especially using a large numbers of IoT devices.*

*All these bogus traffic are sent to targeted servers. In the MEC architecture these traffic will **pass through the MEC server**, since this server is situated at the access.*

To prevent this attack, Bob, the Administrator, will use ANASTACIA to ensure that MEC server will detect the attack and react to mitigate it. Moreover, ANASTACIA will be used to monitor and use Penetration Testing modules to quickly react in order to eliminate this intrusion. ANASTACIA will be used to provide a quality of security seal that ensures that systems are correctly patched against such technique and will

deploy the adequate number of VNF security functions such as Firewalls and DPI in the proper locations."

ANASTACIA D1.2 "User Centred Requirements Initial Analysis." (2017, p. 29).

Risk analysis

As previously detailed, this scenario involves a Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks through smart cameras and IoT devices belonging to the targeted network.

ANASTACIA Deliverable 2.2 describes the attack as follows: *"In the cyber-security panorama, Denial of service (DoS) attacks are considered a serious threat, since their aim is to compromise connectivity capabilities of an entire network or internal nodes/hosts. (…) For our scenario, a DoS is accomplished by a malicious user with malicious goals. Although a denial of service attack could make it possible to dismantle an entire building or organization network, the use case is focused on an attack against a smart camera system. Although the severity rank of the attack is lower than in case of a target to the entire network, it should be considered that in this case the attack may be the first step of a more accurate plan (e.g. involving physical access to the building (…) In this scenario, an attacker, external at the network, controls a set of internal nodes/zombies and instructs them to execute a ping flood DoS attack on the network. In this case the attacking hosts are* ***compromised*** *IoT devices and smart cameras)"*(Cambiaso et al., 2018, p. 12).

Consequence identification

The scenario includes the following potential consequences:

- System downtime: risk 7
- Compromised network resources: risk 1, 2, 3, 4, 5, 6

While the possibility of affectations to data subject's rights is clear in this use-case given the downtime and associated loss of control over personal information (Risk 7), the fact that a malicious attacker can gain access to the ANASTACIA network and effectively control compromised IoT devices and smart cameras, should also be considered as it demonstrates that the security of processing requirement has been breached. This in turn raises the potential risk of unauthorized access, disclosure, modification, removal or deletion of personal data (Risks 1, 2, and 4). While we are unable to determine the exact access or control level that has been obtained by the malicious attacker on the devices the fact that network traffic is altered by these malicious actions also points out that the network's traffic information and device location data might not be secure (Risk 6).

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_MEC.3	Limited (2)	Limited (2)	Negligible (1)	Limited (2)	Limited (2)	Limited (2)	Significant (3)

Table 11 UC_MEC.3 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[27]	ANASTACIA Controls	Impact level
Risk-1	Limited (2)	HSPL authorization policies MSPL authorization policies; Virtual	Negligible (1)

[27] See supra section **Errore. L'origine riferimento non è stata trovata.**.

		firewall and router, SDN switch, CpABE data privacy enabler	Reason: attack vector aimed towards service disruption, not access data, mitigation and controls should minimize effects
Risk-2	Limited (2)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Negligible (1) Reason: attack vector aims to disrupt service not modify data, mitigation and controls should minimize effects
Risk-3	Negligible (1)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Negligible (1) Reason: Attack vector is not compatible with re-identification, mitigation and controls should minimize effects
Risk-4	Limited (2)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Negligible (1) Reason: attack vector seeks to disrupt service, not delete data, mitigation and controls should minimize effects
Risk-5	Limited (2)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Negligible (1) Reason: controls should be sufficient to prevent network sniffing through infected devices carrying out DDoS
Risk-6	Limited (2)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Negligible (1) Reason: location and traffic data might be disclosed by infected devices before DDoS is identified
Risk-7	Significant (3)	Channel protection; Firewall and router, SDN switch	Limited (2) Reason: The protection of the communication channels should minimize system downtime. Organizational controls should be in place to address the issue

Table 12 UC_MEC.3 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[28]

[28] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

UC_MEC.3	7	Malicious Attacker (Hacker / Script kiddies)	Adept (4)[29]	Maximum (4)

Table 13 UC_MEC.3 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for some of these risks could be **significant** even when considering ANASTACIA controls, there is a **limited** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

D.2.6 updates the protection approach to include the following actions

Detection:

- Traffic analysis inside the IoT network
- Detection of unusual ICMP traffic.
- *"the proposed protection system* (ping flood packet blocking or packet limiting, upon which any infringing communications from the network would raise an alarm) (which) *should be binded on the destination address of the targeted system, to counter IP spoofing and DDoS attacks"* (Cambiaso et al., 2018, p. 14).

Mitigation:

- Deployment of firewall rule to filter the malicious attack.
- Attempt to restart the affected devices, if issue persist, disable devices and request technical inspection
- *"Particularly, in this case a mitigation plan is followed in order to interrupt the attack, thus making the smart IP camera able to properly communicate on the network, independently from the fact the detection alert was triggered when the camera was able to communicate (hence, before the DoS is reached) or not (hence, under the DoS)"*. (Cambiaso et al., 2018, p. 15).

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved

[29] While DoS/DDoS attacks can be theoretically performed by malicious attackers with diverse skill levels, the maximum capability level is assumed as the use case denotes a massive attack.

- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Compromised network resources and software/firmware updates to be performed
- Total system downtime and affectation to data subjects (alternative communication mechanisms, complaints received, effective loss of control over personal data, etc.)
- Effectiveness of security mechanisms (DoS, DDoS attack prevention, virtual honeypots/honeynets, etc.)
- Operational and organizational security policies (maintenance, update, etc.)

UC_MEC.4 - IoT-based attack in the MEC Scenario

"Telco networks are experiencing a drastic revolution embracing the opportunity to deploy Cloud Edge environments to host third-party services near to IoT devices. Edge-based service deployment can provide reduced latency compared to ***Cloud-based provisioning and offer location-based contextual data awareness****. In this vein, a SME which provides security video surveillance via camera systems is interested in enhancing the* ***video pre-processing by leveraging the resources provided by the MEC environments.*** *Furthermore, accounting for the increased number of attacks related to IoT devices, the SME would require a higher level of security for their surveillance services, monitoring the traffic generated by its cameras and mitigating potential security threats.*

To guarantee the required security features, the Telco provider will adopt the ANASTACIA framework within its system, by appropriately integrating it with the existing network and service mechanisms, such as SDN, NFV, and cloud edge computing technologies. In this way, the Telco provider will be able to offer advanced Security-as-a-Service solutions, exploiting its capillary and flexible cloud-based network infrastructure. To meet the security requirements of the video surveillance SME, appropriate virtual instances of detection systems (e.g., IDS) will be deployed in the edge environment and will analyse the traffic generated by the cameras.

In this scenario, a group of ***hackers*** *aims at* ***exploiting vulnerabilities in the cameras used by the video surveillance SME to generate attacks*** *(such as DoS, scanning, etc.) against sensitive servers, which can be either the MEC hosting servers to create an* ***interruption in the processing of security videos or external third-party Internet servers.*** *The monitoring modules deployed by the ANASTACIA framework are able to fast detect the on-going attacks and to trigger the orchestration of appropriate countermeasures, such as isolating the compromised cameras by modifying the forwarding paths of software-based networks."*

ANASTACIA D1.2 "User Centred Requirements Initial Analysis." (2017, p. 33)

5.3.1.1 Risk analysis

This scenario is focused on the exploitation of vulnerabilities affecting IoT camera systems, aimed to make the camera perpetrate malicious cyber-attacks against third parties. Such malicious attacks include DoS, scanning, or other well-known threats.

Consequence identification

The scenario includes the following potential consequences:

- Exploiting vulnerabilities in video cameras, granting unauthorized access to sensitive network resources and information: risk 1, 2, 4
- Perpetrating attacks through controlled systems: Risks 3 and 5
- Affectation of location-based resources: risk 6
- System downtime on both internal and external systems: risk 7

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_MEC.4	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)

Table 14 UC_MEC.4 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[30]	ANASTACIA Controls	Impact level
Risk-1	Significant (3)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: While not stated, attacker could potentially access sensitive data before attacks are addressed, depending on speed of detection the impact could be lesser or higher
Risk-2	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: unidentified attacker could modify personal data in devices under his control until detection, controls mitigate the situation to a point, but additional actions are required
Risk-3	Significant (3)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited2) Reason: Given attack vector, affected devices could be used to re-identify personal data before anomalous patterns are detected.
Risk-4	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler;	Limited (2) Reason: affected devices could be ordered to stop recording data before

[30] See supra section **Errore. L'origine riferimento non è stata trovata.**.

		Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	detection, controls should mitigate this to some extent
Risk-5	Significant (3)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: affected devices could be used to perpetrate additional attacks (sniffing/scanning, etc). impact depends on speed of detection by controls
Risk-6	Significant (3)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: affectation of location-based services might disclose personal data
Risk-7	Significant (3)	Channel protection; Firewall and router, SDN switch; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: there's a possibility of system downtime (both internal and external) if the system does not react quickly

Table 15 UC_MEC.4 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[31]
UC_MEC.4	1, 2, 4, 5, 6, 7	Malicious attacker (Hacker)	Adept (4)	Maximum (4)

Table 16 UC_MEC.4 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for some of these risks could be **significant** and even when considering ANASTACIA controls, there is a **limited** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

Detection:

Detection of the attack may involve two different temporal periods:

[31] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

- At exploitation time, in case a known-vulnerability is exploited, it is possible to identify (and block) exploitation
- At post-exploitation time, hence, only after the IoT cameras are exploited, it is possible to identify running attacks (generated by the cameras themselves), by analyzing network traffic flows and communications, to identify known threats (for instance, through signature-based detection, combined with DPI), or unknown threats (for instance, by adopting network anomaly-based IDS)

Mitigation:

Mitigation may be accomplished by blocking outgoing traffic from the affected IoT cameras, or by diverting malicious traffic to harmless locations (under the control of the network administrator) through network reconfiguration accomplished through SDN/NFV approaches. Moreover, it is important to consider that, in order to identify known threats, periodic vulnerability assessment activities may be executed to identify potential threats and targets of an attack, in order to patch vulnerabilities.

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Compromised network resources and software/firmware updates to be performed
- System logs (before and after detection to ensure no additional attacks were not detected)
- Total system downtime and affectation to data subjects (alternative communication mechanisms, complaints received, effective loss of control over personal data, etc.)
- Effectiveness of security mechanisms (DoS, DDoS attack prevention, virtual honeypots/honeynets, etc.)
- Operational and organizational security policies (maintenance, update, etc.)

UC_BMS.1 Cyber-attack at a hospital building

"Annihilos is a criminal gang who takes credit in destroying the reputation of big businesses. They are targeting BetterDays, a large international healthcare provider. The operations of BetterDays include owning and operating several hospitals worldwide, providing health insurance, and running ambulance and emergency services in many countries.

Annihilos intends to ***exploit a zero-day vulnerability*** *in the building management system that BetterDays uses in a large city hospital. The vulnerability allows the building management system to accept an external internet-based emergency web service message that will bring elevators and escalators in emergency mode to designated floors and overriding automatic operations of HVAC systems. But the emergency mode will also activate the fire safety services in the respective floors too. Annihilos plans to activate emergency in several floors simultaneously using several lifts. Since the fire-safety system listens, activates and responds to the emergency by activating the sprinklers and foams, it is possible to increase the risk of structural damage to the building and threat of lives in the hospitals. The false alarm could be escalated throughout the BetterDays hospital building as well as invite the city's fire-brigade response. Moreover, by accessing the HVAC network, Annihilos could switch-off emergency terminal units, overwrite heating and cooling set-points in various floors, stress the heating equipment towards damage, etc. Annihilos could increase the energy consumption, utility and HVAC maintenance costs of BetterDays hospital building.*

In addition, during the panic, ***Annihilos gang members plan to gain physical unauthorized access to the data-centre of the hospital whose secure doors will be disengaged during an emergency. Annihilos could install rogue applications in the datacentre workstations to transfer or transmit sensitive data of their business and private data of their clients. Subsequent to the emergency, the rogue applications in data-centre workstations will allow Annihilos to launch a remote attack (e.g., via SQL injection) on the servers that host the hospital document management system.***

Chris, the hospital manager, can use ANASTACIA to ensure that BetterDays is safe from any such attack from Annihilos, as described in the following session."

ANASTACIA D1.2 "User Centred Requirements Initial Analysis." (2017, p. 36)

Risk analysis

This scenario is focused on the execution of an advanced and combined attack based on the exploitation of a 0-day vulnerability, granting the attacker access to the target network. Once access is obtained, different "actions" are accomplished (activation of emergency in several floors of the building, switch-off of emergency units, overwrite of heating and cooling configurations, etc.), also including the gaining of physical unauthorized access to the facilities, needed to install malicious applications on specific network nodes, making them exfiltrate sensitive data outside of the organization and, simultaneously, perpetrate network attacks (e.g. SQLi) against document management services.

Consequence identification

The scenario considers significant consequences due to the nature of the planned attack (as it directly mentions the possibility of direct security affectation to the lives and well-being of data subjects. As such, all the envisioned risks are involved in this use-case, as detailed below:

- Physical unauthorized access to data centre, with direct possibility to transfer, edit or delete sensitive data: risk 1, 2, 4
- Obtain unauthorized access to personal data stored in the system and force reidentification of such data: risk 3
- Installation of rogue applications and spoof devices within the network (and access to network metadata): risk 5
- Dormant malicious applications to transmit potentially sensitive information in the future: risk 6
- Direct affectation to end-user rights through system downtime and physical attack to building infrastructure: risk 7

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_BMS.1	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)	Maximum (4)

Table 17 UC_BMS.1 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[32]	ANASTACIA Controls	Impact level
Risk-1	Maximum (4)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: ANASTACIA controls should identify the patterns and context of the attack and prevent unauthorized access to sensitive data. If initial attack is successful, impact might be inevitable given physical attack vector.
Risk-2	Maximum (4)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler¸ Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: ANASTACIA controls should identify the patterns and context of the attack and prevent unauthorized modification of sensitive data. If initial attack is successful, impact might be inevitable given physical attack vector.
Risk-3	Maximum (4)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Limited (2) Reason: if initial attack is successful, physical access to the infrastructure might deny the controls implemented by ANASTACIA
Risk-4	Maximum (4)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: ANASTACIA controls should identify the patterns and context of the attack and prevent unauthorized deletion of sensitive data. If initial attack is successful, impact might be inevitable given physical attack vector.

[32] See supra section **Errore. L'origine riferimento non è stata trovata.**.

Risk-5	Maximum (4)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Limited (2) Reason: Controls should avoid initial attack from succeeding, otherwise, impact might be inevitable given physical attack vector.
Risk-6	Maximum (4)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Limited (2) Reason: Controls should avoid initial attack from succeeding, otherwise, impact might be inevitable given physical attack vector.
Risk-7	Maximum (4)	Channel protection; Firewall and router, SDN switch; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: Controls should avoid initial attack from succeeding, otherwise, impact might be inevitable given physical attack vector.

Table 18 UC_BMS.1 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[33]
UC_BMS.1	1, 2, 3, 4, 5, 6, 7	Malicious attacker (Hacker)	Adept (4)	Maximum (4)

Table 19 UC_BMS.1 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for all these risks could be **maximum** and even when considering ANASTACIA controls, there is a **limited** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

Detection:

- By definition, it is not possible to detect 0-day vulnerabilities exploitation. Nevertheless, it is possible to deploy anomaly-based NIDS (making use for instance of machine learning methods) to identify anomalies on the network
- The different "actions" executed by the attacker can be detected by implementing and deploying appropriate logging systems

[33] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

- The possibility to obtain physical unauthorized access to the facilities can be detected by implementing proper authentication and access control lists on the services adopted for access management and access to physical locations, combined with a physical identification of intrusions through the adoption of physical security systems
- Exfiltration outside the organization of sensitive data may be identified by deploying anomaly-based NIDS, designed to detect anomalous traffic on the network
- Running attacks (e.g. SQLi) can be identified by NIDS through DPI approaches

Mitigation:

- The different "actions" executed by the attacker can be mitigated by restoring systems and configuration to previous states after the alert.
- The possibility to obtain physical unauthorized access to the facilities can be prevented by implementing proper authentication and access control lists on the services (for instance, also considering timing accesses), adopted for access management and access to physical locations along with other physical security controls and training in alert scenarios
- Exfiltration outside the organization of sensitive data may be mitigated by blocking or redirecting network communications
- Running attacks (e.g. SQLi) can be mitigated at the network level, by NIDS and/or by redirecting the network traffic to harmless nodes

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Security and organizational mitigation activities and training of personnel
- Additional security controls should be introduced to the external document system after any part of the organizational infrastructure has been attacked
- Impact of the attack to data subjects should be considered and reported if any stage of the planned attack is successful given the malicious nature of the risk source.

- Cooperation with law enforcement and potential use of threat information sharing solutions to prevent and mitigate likelihood of zero-day attacks
- Update policies for all devices in the organization

UC_BMS.2 Insider attack on the fire suppression system

> *"Adam, the operations technician, is a **disgruntled employee** who intends to cause economic **cost to his employer by damaging building assets such as electronic controllers, servers, CCTV cameras, furniture, etc**. To carry out his sinister motive, he intends to exploit the building operations workstation he is entrusted with. The workstation is used to manage the fire-alarm panel input/output. He could compromise the workstation **by installing malware via a USB drive.** This **workstation has network access beyond the reach of much of the network access controls such as firewalls and authentication, authorization, and accounting mechanisms deployed upstream**. Adams's intention is to use the **malware to exploit an unpatched application** that controls the fire alarm panel in order to activate unauthorised release of pressurized water or gas suppressants to flood and damage the building.*
>
> *Bob, the operations manager, will use ANASTACIA to ensure that appropriate network and system design, implementation, monitoring and reaction are considered to **minimise such an insider attack.** ANASTACIA will assist Bob to provide a quality of security seal that ensures that systems within the building are correctly **patched against known malware and that proper deployment of firewalls with deep packet inspection capability that act as points of demarcation between back-end workstations and IoT/CPS controllers**. More importantly, ANASTACIA will assure Bob that should pressurized fire suppressants are released to areas vulnerable to fire, other building operations such as evacuation of occupants, alerting of wardens and responders, elevator and escalator operations, ventilation, etc., follow the emergency operation mode."*(2017, p. 41)

Risk analysis

The use-case is focused on the injection, by an insider, of malware on the network in order to target a fire alarm application system with the aim to control a fire suppression system. The following figure depicts this situation:

ANASTACIA D.2.2 correctly points out that the main threat in the use-case relates to the insider (and secondarily to the malware that he/she introduced to the network). *"This kind of threats is extremely dangerous, since insiders typically have advanced knowledge on the targeted system and access to restricted areas. For the selected use case, the malware is spread by using different attack vectors, such as USB infection of a building operation workstation of the malicious employee, or by exploiting wireless connectivity to access the network and spread the malware."*(Cambiaso et al., 2018, p. 22).

Consequence identification

While the use-case is focused on the potential damages to the building caused by an insider threat, the high-level of network access granted to the vulnerable workstation implies potential risks to the personal data of both persons accessing the building infrastructure (and thus being recorded by the security systems) and to those data subjects found in corporate databases connected to the building's network. As such, the following requirements are of relevance:

From a privacy point of view, the attack will have the greatest effects in relation to data protection requirements 3, 6 and 7. This because the best way to prevent insider threats involve[34] potentially invasive measures which could affect the privacy of both end-users and employees. For this reason, any measures implemented to prevent malware or intrusions into a system should respect the personal data protection principles (particularly transparency and accountability). ANASTACIA therefore should meet these requirements and avoid generating any further risks when attempting to prevent security or privacy threats.

The specific attack depicted by this use case is particular as it recognizes the possibility of having malware "spread via network using a computer internal to the infrastructure of the targeted organization. The malware exploits an unpatched application of the fire suppression system to access sensitive sensors."(Cambiaso et al., 2018, p. 22). Considering both the malicious intent of the attacker and the broad potential range of impact of the malware, privacy risks 1, 2 and 4 are of maximum relevance to this use-case. A similar situation can be identified with regards to privacy risks 3 and 7, as the attacker could effectively use the same attack vectors to compile or aggregate information from multiple sources and to negatively affect the system's availability (or any other safeguards integrated at an application level to respect the rights of the data subject). Finally, while less likely given the aims and nature of the attacker, privacy risks 5 and 6 should be considered as also possible in this use-case.

The scenario includes the following potential consequences:

- Unauthorized access to sensitive network resources and information, the extent of which is unknown: risk 1, 2
- Damage to company assets: risk 4
- Malware-based attack on network and access to network metadata: risk 3
- Potential for direct affectation of end-users and system downtime: risk 7

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_BMS.2	Maximum (4)	Maximum (4)	Significant (3)	Maximum (4)	Limited (2)	Limited (2)	Significant (3)

Table 20 UC_BMS.2 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[35]	ANASTACIA Controls	Impact level
Risk-1	Maximum (4)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: security controls should be able to mitigate the impact and likelihood for unauthorized access to sensitive data
Risk-2	Maximum (4)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch;	Limited (2) Reason: security controls and particularly the behavioural engine

[34] *"An important consideration regarding the insider threat issue is the balance between security and employee privacy: it is generally known that there is no expectation of privacy when using an organization's network and devices, nevertheless, employee monitoring is an area that many organizations prefer to avoid. Nowadays, any computer system is attacked by malicious users, then it is necessary to implement an attack detection system and a response plan to avoid damaging the system."* (Cambiaso, Mongelli, et al., 2017, p. 6).

[35] See supra section **Errore. L'origine riferimento non è stata trovata.**.

		CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	can help address the threat for data modification
Risk-3	Significant (3)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Limited (2) Reason: network encryption reduces the risk but does not negate it, depending on the capabilities of the affected workstation, organizational policies could contribute
Risk-4	Maximum (4)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler; Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems	Limited (2) Reason: The deletion of data (both physical and organizational) can be prevented by avoiding the initial threat of unauthorized access
Risk-5	Limited (2)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Negligible (1) Reason: attack vector isn't focused necessarily on impersonating devices in the network but authorization policies (well implemented) should prevent it
Risk-6	Limited (2)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Negligible (1) Reason: The data encryption implemented by Anastacia should mitigate risk of data disclosure
Risk-7	Significant (3)	Channel protection; Firewall and router, SDN switch	Limited (2) Reason: Risk of affectations to data subjects remains, however the

Table 21 UC_BMS.2 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[36]
UC_BMS.2	1, 2, 3, 4, 5, 6, 7	Insider threat	Operational (3)	Maximum (4)

Table 22 UC_BMS.2 Likelihood Assessment

[36] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for some of these risks could be **maximum** and even when considering ANASTACIA controls, there is a **limited** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

Deliverable 2.2 proposed a layered approach to protecting the system from an insider/malware attack. This approach included the following elements:

- Network level protection: based on network traffic analysis to identify and drop malicious packets.
- Host level protection: based on controlling hosts and limit privileges and activities users can execute
- Application server protection: based on continuous vulnerabilities patching on both the system and its nodes and exposed applications.

Detection:

The detection approach recommended by ANASTACIA D.2.2. for this use-case was based mainly on log inspection[37] accomplished by the monitoring components along with the implementation of access control rules on actions/boundaries: *"By adopting this approach, it is possible to have a complete vision of the current state of the system in order to identify the attack in time, for proper mitigation."* (Cambiaso et al., 2018, p. 23).

These same set of detection actions can be implemented to detect privacy threats:

- The AAA Architecture could be utilized to detect unauthorized or unexpected/unusual behaviour from terminals (unusually contacting devices in the network, transferring or receiving large amounts of information, using abnormal authentication credentials, etc.) particularly once the network and ANASTACIA have been properly configured with a set of privacy policies which identify those network resources in which personal data could be found.
- Log inspection by the monitoring components could greatly enhance the effectiveness of this approach, particularly if access to application-level or device-level logs is possible, as this could lead to the identification of the specific resources that are being accessed.
- Token validation

Mitigation:

- Mitigation of these risks will depend on the implementation of SDN/NFV functionalities and enablers like MMT DPI/DFI and virtual firewalls. D.2.2. recommends the implementation of three separate approaches for mitigation (design time, run-time and continuous mitigation) at host, application and network levels. The most relevant of these from a privacy standpoint in the ANASTACIA context is the runtime-mitigation at a network level, which aims to validate users and devices accessing the network and blocking IPs which irregularly access the network.
- IoT honeynet
- Transparent forwarding

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

[37] D.2.2 recommended the inspection of logs from the network, host, protection software, access, application and IoT devices.

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Organizational process to identify insider and report it to authorities.
- Examine reports and logs from AAA and malware detection/prevention mechanisms at the application/host level.
- Human resource policies (particularly re. security elements at end of contract), risk mitigation and training.
- Physical security mechanisms in place (to minimize risk of unauthorized access to devices in the network by insider threats)
- Location, data processed and additional capabilities (enabled or not) of devices in the network which might be vulnerable to similar attacks (particularly determine whether ports or services could be disabled to minimize risk potential).
- Maintenance policies
- Post-attack debriefing of ICT team
- Results of recent security audits

UC_BMS.3 Remote attack on the building energy microgrid

"Clara is an ex-colleague of David who is the plant manager at Eisen Inc., a steel producer. Clara is now a security contractor for the competitor of Eisen Inc. Not surprisingly, Clara is aware of the existence of a misconfigured network path (any source IP address) for a utility provider (trusted IP address) of Eisen Inc. ***This allows the external energy provider to directly interface with the SCADA (supervisory control and data acquisition)*** *system of the Eisen Inc's energy microgrid. But the* ***SCADA data historian is accessible due to an unpatched bug in the networking middleware that allows a privileged escalation of access****. Clara will exploit this bug to launch a remote attack (e.g., via SQL injection) on the database servers that host the SCADA data historian. She could* ***steal Eisen Inc.'s business credentials****, overwrite boiler setpoints, rewrite activation ratios between generators and battery, fake network demands, etc. Clara could increase the energy consumption and utility costs of Eisen, stress the generators*

and boilers towards damage, and disable the shut-down capability of the blast-furnace.

David will use ANASTACIA to ensure that the Eisen Inc.'s network access policy enforcement is not compromised. Further, ANASTACIA will help David to detect insecure operations of the processes, equipment or controllers. David will rest assured that the reactive and resilient features of ANASTACIA will activate safe-mode of operations should abnormalities occur."

ANASTACIA D1.2 "User Centred Requirements Initial Analysis." (2017, p. 45)

Risk analysis

In this situation, a malicious user targets an energy micro-grid by exploiting network nodes to violate a SCADA database through a SQL injection attack. The following figure illustrates the use-case:

ANASTACIA D.2.2 describes SQL attacks as representing *"well-known serious threat for web applications [Halfond, 2006]. By executing such threats, an attacker is potentially able to retrieve or alter database information. Indeed, web applications vulnerable to SQL injection attacks may allow an attacker to gain complete access to the adopted databases. Usually, databases are directly accessed by web servers in order to access structured data from the (web) user interface. SQL injection attacks exploit vulnerabilities affecting web pages, often deriving from bad code quality"*(Cambiaso et al., 2018, p. 16).

Consequence identification

As defined in D.2.3, this scenario is very related to two of the identified personal data protection requirements (2 and 4) as the attacker (knowledgeable of the security mechanisms implemented and their vulnerabilities) is able to directly access the ANASTACIA-monitored network and access the plant's database, potentially stealing company credentials with which she could cause further affectations to the systems and personal data of employees and customers alike.

Several characteristics of the attack as defined by Deliverable 2.2 are to be considered when determining the risks involved and their potential consequences to the fundamental rights of data subjects, namely:

- While the attacker is external to the network, it has previously worked at the company.
- "*The attacker exploits a web page vulnerability to inject SQL malicious code in order to access or manipulate the SCADA database. Such exploitation is based on the generation of the query by using unfiltered inputs provided by the user".* (Cambiaso et al., 2018, p. 16).
- The attacker's aim may be
    - To alter/tamper the database content.
    - To bypass access restrictions (to accomplish privilege escalation).
    - To access/steal sensitive data.

In this context, the risks raised by the threat are many:

- There is an extremely high risk of unauthorized destruction of personal data (risk 4) given her express intentions to directly tamper or damage the plant's infrastructure.
- Significant risks of access, reidentification, modification of personal data and affectation to data subject rights (risks 1, 2, 3 and 7) can be identified given the type of attack launched, the attacker's ties with a competitor and the very possible downtime that is to be caused by the attack.
- Additionally, there is a significant risk (6) that even if the attacker were to be unsuccessful in further escalating her access rights, the fact she is knowledgeable of the protocols and vulnerabilities in the system will enable her to directly or indirectly (through a traffic analysis attack, for example) obtain traffic information and device location data from the network (which could involve employee personal data).

- Finally, the attacker could exploit the network and company infrastructure to complement other attack vectors[38], thus raising the possibility of excessive collection or retention of personal data (risk 5) from unsuspecting third parties.

The following table summarizes the assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_BMS.3	Significant (3)	Significant (3)	Significant (3)	Maximum (4)	Limited (2)	Significant (3)	Significant (3)

Table 23 UC_BMS.3 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[39]	ANASTACIA Controls	Impact level
Risk-1	Significant (3)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler	Limited (2) Reason: The data privacy enabler along with other privacy-related solutons should mitigate risk of unauthorized access and identify irregular credential usage
Risk-2	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2) Reason: Data integrity risks are mitigated by the authorization policies, however some risk remains from an application level
Risk-3	Significant (3)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Significant (3) Reason: The encryption of the data mitigates the risk of re-identification, however, the risk remains as is unless an additional action is undertaken at the application level (tokenization, etc.)
Risk-4	Maximum (4)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2) Reason: The availability of the data is also ensured with a limited risk.
Risk-5	Limited (2)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Limited (2) Reason: The risk is somewhat lowered by the attack vector and the existing controls, however organizational contingencies are most likely to

[38] For example, using her access to the power plant's network to exfiltrate personal data from a third party's malware infected computer. Indeed, it is possible to develop malware to use power lines to exfiltrate data from air-gapped computers. "*In this case, a malicious code running on a compromised computer can control the power consumption of the system by intentionally regulating the CPU utilization. Data is modulated, encoded, and transmitted on top of the current flow fluctuations, and then it is conducted and propagated through the power lines*" (Guri, Zadov, Bykhovsky, & Elovici, 2018). This kind of attack could be impossible to track via regular network-level monitoring (as the malware would be based in the host and could make use of a zero-day vulnerability to avoid detection) and records of the flow fluctuations (and thus, of the exfiltrated data) would be kept by the power company.

[39] See supra section **Errore. L'origine riferimento non è stata trovata.**.

Risk-6	Significant (3)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Limited (2) Reason: The protection brought by ANASTACIA is reducing this risk.
Risk-7	Significant (3)	Channel protection; Firewall and router, SDN switch	Limited (2) Reason: The level of the risk is low, but it remains alive if another bug is found.

Table 24 UC_BMS.3 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[40]
UC_BMS.3	1, 2, 4	Insider threat	Operational (3)	Maximum (4)

Table 25 UC_BMS.3 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for some of these risks could be **maximum** and even when considering ANASTACIA controls, there is a **significant** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

Considering the nature of the attack, protection efforts should include organizational activities to be undertaken in line with the data minimization principle (minimization, anonymization, etc.) and introducing input sanitization mechanisms to their systems and applications. Meanwhile, sufficiently strict access control, log inspection policies should be introduced to ANASTACIA to accomplish continuous oversight of the system's security.

As defined by ANASTACIA D.2.2, detection of these attacks will depend mainly on ANASTACIA's capability to monitor the logs from three principal components: database, network, and application server. This effort should be aimed at identifying unexpected queries, network accesses and anomalous or large 1 to 1 traffic in the network (particularly as relating to those devices which have been identified as potentially containing or processing personal data). These efforts should be further enhanced by the implementation of deep-packet and flow inspection tools.

ANASTACIA D.2.6 updates this approach to include the following detection and mitigation actions:

Detection:

- Traffic analysis on the incoming link of the server using DPI.

[40] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

- Detection of SQL queries in the requests

Mitigation:

- Deployment of firewall rule to filter the traffic from the attacker.

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Vulnerabilities of affected devices in the network.
- Implement review processes for client credentials if an attack is identified
- Location, data processed and additional capabilities (enabled or not) of devices in the network.
- Human resources policies (background checks performed and post-employment follow-up for risk assessment).
- Policies for revocation of access and scheduled system wide credential changes.
- Maintenance policies
- Post-attack debriefing of ICT team.
- Results of recent security audits.

UC_BMS.4 Cascade attack on a megatall building

*"FoulGame is a notorious group of **criminal hackers** who specialize in attacks on internet-connected services of global brands. They have set their eyes **to destroy the brand name of Hilltop Group who owns many iconic hotels worldwide**. FoulGame intends to use internet-connectivity of the buildings operations to create **an emergency in a mega-tall hotel building**. They hope that the **emergency will generate panic, trap the guests in escape elevators, activate fire-suppression sprinklers, confuse first-responders, etc.***

FoulGame wants to exploit a ***zero-day vulnerability of the HVAC system network that allows an external service such as an internet-service or original equipment manufacturer (OEM) to set default values (e.g., -40 ºC) to temperature sensors.*** *For practical reasons, HVAC zonal temperatures are also monitored by the fire safety systems as a precaution. But if the temperature exceeds a threshold (e.g., +80 ºC), an emergency is activated. This could cascade to alarms and sprinklers activating, air-handlers stopping, elevators becoming disabled, fire-doors and corridors closing, etc.* ***Risk to lives of occupants due to activation of fire-suppression systems, depletion of oxygen in the air, and rush and stampede in the stairwells will be catastrophic****.*

Hilltop Group can use ANASTACIA to ***identify and rate cyber-security security vulnerabilities automatically for the entire building.*** *ANASTACIA will use system design and operational data to discover dependencies between cyber-physical systems and operations for the entire megatall structure. Hilltop Group will use ANASTACIA to predict potential security consequences of interacting operations between subsystems and* ***generate threat isolation strategies****. ANASTACIA will continuously* ***enforce access and security policies*** *and resilient control strategies comprehensively at various cyber-physical levels, viz. the temperature sensors, fire-panels, elevator system managers, air-handling unit controllers, fire-suppression sprinkler systems, etc."*

(2017, p. 48)

Risk analysis

This use-case is based on the exploitation of the system by a malicious user to manipulate critical temperature sensors through a zero-day vulnerability to bypass signature-based intrusion detection systems and trigger fire and evacuation alarms.

ANASTACIA D.2.2 describes the threat as follows: *"A zero-day vulnerability (0-day) is exploited by an attacker that makes use of unknown vulnerabilities on the system to target it [Bilge, 2012; Endorf, 2004]. Indeed, unlike well-known vulnerabilities, "known" by the system and often mitigated, a zero-day attack is unknown to the targeted system, usually attacked in such way for the first time. Since the vulnerability is discovered for the first time during the execution (if it is detected), there may not be known solutions or patches able to efficiently protect the system."*(Cambiaso et al., 2018, p. 19)

Consequence identification

As defined in D2.3, the attack has the potential to threaten the life and security of the inhabitants of a mega-tall building and for this reason the security requirements (Req-7 and secondarily Req-10) are fundamental to the minimization of further impacts to the individual and to avoid any further escalation of the privacy risks. As defined by Deliverable 2.2, the case involves a hacker group, *"external to the network, who exploits a zero-day vulnerability to remotely target a sensitive device, in order to access the entire network and attack the infrastructure."*(Cambiaso et al., 2018, p. 19).

The fact that the attack has been launched by a group of hackers is the most relevant element when determining the potential privacy risks involved in this scenario. As these groups are very adept at performing the tasks they aim to achieve. In this case, they aim to negatively impact the brand name of the hotel under attack. Considering these elements and the malicious nature of the attacker it is just as likely that they will seek to target the personal information of individuals connected to the building's vulnerable networks as it will maximize the potential impact of their current attack (achieve privilege escalation through employee identity theft) and grant them with additional attack vectors for future attacks.

In this context, all the privacy risks are to be as relevant with diverse potential consequences associated with each. The fact that the tools (including knowledge of additional zero-day vulnerabilities on the system)

available to the attackers to perform such attacks is unknown, along with their capabilities and motivation should be enough to raise the alarm level significantly.

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
UC_BMS.4	Maximum (4)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)	Significant (3)

Table 26 UC_BMS.4 Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[41]	ANASTACIA Controls	Impact level
Risk-1	Maximum (4)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler	Limited (2) Reason: Data isolation and access enablers limit risk to a manageable level (if complemented with application and organizational controls)
Risk-2	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2) Reason: Data isolation and access enablers limit risk to a manageable level (if complemented with application and organizational controls)
Risk-3	Significant (3)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Limited (2) Reason: Data isolation alongside with malicious activity detection and encryption mechanisms should prevent the re-identification of data
Risk-4	Significant (3)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Limited (2) Reason: If initial attack is not successful, risk can be limited to manageable levels
Risk-5	Significant (3)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Limited (2) Reason: Risk of excessive collection cannot be completely eliminated given the zero-day attack that is being used, however unauthorized device activity could be prevented by ANASTACIA
Risk-6	Significant (3)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Negligible (1) Reason: risk of location and traffic data being used by the attackers is negligible given the type of attack used.
Risk-7	Significant (3)	Channel protection; Firewall and router, SDN switch	Negligible (1) Reason: ANASTACIA should prevent system downtime and prevention of

[41] See supra section **Errore. L'origine riferimento non è stata trovata.**.

			other risks diminishes potential impact to data subject rights.

Table 27 UC_BMS.4 Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[42]
UC_BMS.4	1, 6, 7	Malicious attacker (Hacker)	Adept (4)	Maximum (4)

Table 28 UC_BMS.4 Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for at least one of these risks could be **maximum** and even when considering ANASTACIA controls, there is a **limited** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

As mentioned by D.2.2, there is no common and general protection plan that can be adopted to defend a system from zero-day attacks. However, certain actions like the deployment of a honeynet and continuous maintenance and training of the intrusion detection and prevention systems could help to palliate the risks involved in the scenario.

While detection and mitigation of zero-day attacks is no simple task, implementation of strong intrusion detection systems (capable of both anomaly detection and misuse or signature-based detection) is a good step to maximize the probability of detection. Furthermore, while most of the privacy risks associated to the use-case could be performed through the exploitation of a zero-day vulnerability, it is highly unlikely that the attackers will depend solely on one mechanism. For this reason, by correctly implementing the whole range of tools available to ANASTACIA, the possibility of identifying and mitigating the many security threats associated to any of the privacy risks is considerably enhanced.

ANASTACIA D.2.6 updates this approach to include the following detection and mitigation actions:

Detection:

- Buffered sensor data from smart buildings
- Detection of misbehaviour of the system
- Enabling of continuous and integrated monitoring of multivariate signals, event logs, heartbeat signals, status reports, operational information, etc.

[42] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

Mitigation:

- Block of the adversary, based on VDSS feedback
- Restore of sensors data (back process)

This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- Network isolation policies and successful deployment.
- Access policies.
- Risk assessment and predefined emergency response policies (with law enforcement cooperation).
- Device update policies and threat sharing initiatives to minimize potential risk of a zero-day attack.

5.4 Advanced Attack Scenarios

Slow DoS attack (Advanced Persistent Threats)

"FoodSell is a food distribution company selling products through a locally hosted e-commerce website. This website is everyday used by hundreds of customers to buy high quality food products directly from FoodSell.

The FoodSell network is equipped with ANASTACIA, monitoring anomalies on the network and notifying Bob, the network administrator of FoodSell.

ANASTACIA is able to autonomously monitor the network traffic directed to/coming from the publicly accessible e-commerce website, hence identify malicious and anomalous requests.

On Christmas day, when only a few employees are working at FoodSell, ANASTACIA identifies anomalous traffic directed to the website. Also, ANASTACIA verifies the availability of the e-commerce website, that is now

unreachable. A distributed denial of service attack is running, against the e-commerce website of FoodSell.

As a consequence, after triggering a warning message directed to network administrators, ANASTACIA identifies the source IP addresses of the attack, hence, closes the connections (by sending spoofed packets to the attacked server) and bans/blocks such IP addresses.

At this point, server's availability is verified again, resulting that the server is reachable/online again. An information message is sent to the network administrators, notifying them that the attack is mitigated.

Thanks to ANASTACIA, the system is able to identify and mitigate the attack, also making network administrators aware of the cyber-attack."

Risk analysis

The principle of a Slow DoS Attack consists to send HTTP requests to a server but not at a high frequency like a classical DoS Attack, but at low frequency. This allows this kind of DoS attacks to be invisible by the tools detecting standard DoS attacks. The main goal of a Slow DoS Attack is to open multiple connections to a remote server with slow HTTP requests. These requests are not completely sent by the attacker and the server is waiting indefinitely on the end of the HTTP requests. For example, sending incomplete HTTP headers or partial HTTP POST requests will use the resources of the server, because the issued connections are always open. At the end, there will be a depletion of connections, because all the open connections will be owned by the requests made by the attacker. Of course, the attacker can choose to distribute the sources of the Slow DoS Attack to gain more invisibility against the tools protecting the server.

Consequence identification

The scenario is particularly focused on the potential downtime generated through a slow DoS attack, which is directly related to privacy risk 7.

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
Slow DoS attack (Advanced Persistent Threats)	Negligible (1)	Negligible (1)	Negligible (1)	Negligible (1)	Negligible (1)	Negligible (1)	Maximum (4)

Table 29 SDOS Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[43]	ANASTACIA Controls	Impact level
Risk-1	Negligible (1)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler	Negligible (1) Reason: Attack vector is, generally speaking, not compatible with this risk.
Risk-2	Negligible (1)	HSPL authorization policies, MSPL authorization policies; Virtual	Negligible (1)

[43] See supra section **Errore. L'origine riferimento non è stata trovata.**.

		firewall and router, SDN switch; CpABE data privacy enabler	Reason: Attack vector is, generally speaking, not compatible with this risk.
Risk-3	Negligible (1)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Negligible (1) Reason: Attack vector is, generally speaking, not compatible with this risk.
Risk-4	Negligible (1)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Negligible (1) Reason: Attack vector is, generally speaking, not compatible with this risk.
Risk-5	Negligible (1)	HSPL authorization policies MSPL authorization policies; virtual and physical firewall and router	Negligible (1) Reason: Attack vector is, generally speaking, not compatible with this risk.
Risk-6	Negligible (1)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Negligible (1) Reason: Attack vector is, generally speaking, not compatible with this risk.
Risk-7	Maximum (4)	Channel protection; Firewall and router, SDN switch	Limited (2) Reason: ANASTACIA's enablers should be capable of correctly mitigating the attack, however organizational controls should be introduced to prevent impacting end-user rights.

Table 30 SDOS Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Most Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[44]
UC_0.1	7	(unknown)	Adept (4)[45]	Maximum (4)

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for at least one of these risks could be **maximum** and even when considering ANASTACIA controls, there is a **limited** potential for the risks impacting the data subjects in some manner.

[44] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

[45] The maximum likelihood is to be assumed in case of an unknown threat agent, as preventive and corrective measures should be deployed regardless of the assumed likelihood of an ongoing event.

For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

Protection approach

Two facts complicate the detection and the protection of this type of DoS attacks: the distribution of a Slow DoS Attack and the low speed of the requests. With multiple sources and so, multiple source IP addresses, the points of origin of the attacks are multiple and can be considered as a normal traffic between the server and the rogue clients. Since the logs on a server are updated after the completion of a HTTP request or at the end of a connection, there is nothing useful appearing in the logs. So, reading the logs in a classical way is not a serious option to detect this kind of DoS attacks.

Detection:

As defined in ANASTACIA D2.6 and D6.2, several approaches are possible using different techniques like statistic, machine learning or spectral analysis. In the case of Slow DoS Attacks, the detection can, in principle, be done either by having agents installed in the devices or by analyzing the traffic towards a targeted device. Agent based monitoring provides with information about the situation of the device targeted. This includes logs produced by the attacked service or installation of HIDS tools. In any case, the applicability of this approach depends on the capabilities of the devices targeted, which, in case of IoT devices, are scarce

In the context of ANASTACIA, the live network traffic is captured and statically analysed. This analysis is used some protocol dependent parameters and their values are extracted in order to compare and/or distinguish different network scenarios. An abnormal time is statically detected through this method, in particular a higher value than expected. This means that endless HTTP requests are sent to the server.

Mitigation:

While it is trivial to detect and mitigate a single attacking host, it is extremely difficult to identify a distributed attack. This fact derives from the fact that IP address filtering may be applied to detect and mitigate a SlowComm attack (see, for instance, previous tests on mod-security), while in case of a distributed attack this concept may not be adopted with ease. For this reason, the specific security mitigation activities to be undertaken in this use-case are those defined in detail by D.2.6. This approach should be integrated with the implementation of the ANASTACIA protection, detection, and mitigation enablers detailed in supra Section 5.2.

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions

Contingency actions to be implemented by the DPO and reported back through the DSPS include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.

- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be recommended by the DSPS in this scenario include analysis of:

- User rights protection mechanisms in place (to address potential access/deletion/modification, etc. requests during system downtime).
- System or platform redundancy capabilities and policies
- Organizational action plans to mitigate further affectation to associated services caused by the DoS

IoT Zero-day attack

"SportWear is a multi-national company with several production farms distributed all around the world.

Such farms are equipped with last generation IoT manufacturing technologies and they produce everyday thousands of products to distribute to SportWear's customers. In particular, smart IoT temperature sensors are adopted to monitor the environmental temperature, to dynamically reconfigure the load of the manufacturing machines on the farm and/or to identify critical situations on the farm.

The SportWear network eco-system is equipped with ANASTACIA, monitoring devices and cyber-attacks to the network. ANASTACIA is able to autonomously identify running attacks to the environmental IoT network, to autonomously trigger alerts and, when possible, counter attacks.

A malicious user connected to the ANASTACIA IoT network runs a 0-day attack against IoT sensors designed to monitor the environmental temperature, to block their communications on the network. The attacker targets each sensor of the network. The aim of the attacker is to cause a block to the manufacturing.

While some of the (ANASTACIA empowered) IoT nodes manage to autonomously mitigate the attack, others are affected by the attack. In the first case, ANASTACIA notifies the network administrators with a warning. In the latter case, ANASTACIA identifies the attack and triggers an alert for the network administrators to manage the issue and restore the situation.

Thanks to ANASTACIA, the system is able to identify the attack and promptly notify the network administrators."

Risk analysis

The attack consists to a Zero day attack on an IoT modem which is in fact a ZigBee gateway between a computer connected to the Internet and a ZigBee network. The vulnerability concerns the Remote AT Command implemented with a bug. In this case, the Remote AT Commands allow to configure the ZigBee network by changing numerous parameters, including the identifier of the ZigBee network. This is particularly dangerous, because IoT devices registered into a ZigBee network can be associated to a new rogue ZigBee network discretely. So, it means that the data provided by the IoT devices is available to a third rogue party.

Consequence identification

The scenario presents a number risks given the innovative nature of the attack implemented and the characteristics of the target network. As such, the following consequences are of relevance:

- Unauthorized access to sensitive network resources and information, the extent of which is unknown: risk 1, 2, 4
- Unauthorized compilation of network data: risk 5
- Anomalous outbound traffic (containing potentially sensitive information): risk 6

The following table provides an assessment of the potential consequences involved:

Use Case	Risk 1	Risk 2	Risk 3	Risk 4	Risk 5	Risk 6	Risk 7
IoT Zero day attack	Limited (2)	Limited (2)	Negligible (1)	Limited (2)	Significant (3)	Limited (2)	Negligible (1)

Table 31 0day Consequence Assessment

Impact

Given the planned capabilities of the ANASTACIA system, mitigation activities might reduce the impact of the attack and the consequences for data subjects, the following table provides some additional information:

Impact	Consequences[46]	ANASTACIA Controls	Impact level
Risk-1	Limited (2)	HSPL authorization policies MSPL authorization policies; Virtual firewall and router, SDN switch, CpABE data privacy enabler	Negligible (1) Reason: Possibility of identifying personal data in a factory sensor network is limited, the ANASTACIA and organizational controls implemented should greatly mitigate actual impact to data subjects
Risk-2	Limited (2)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Negligible (1) Reason: Possibility of modifying personal data in a factory sensor network is limited, the ANASTACIA and organizational controls implemented should greatly mitigate actual impact to data subjects
Risk-3	Negligible (1)	Channel Protection, Anonymity, Encryption (TLS); SDN switch; Firewall, VPN, TLS	Negligible (1) Reason: Possibility of re-identifying personal data in a factory sensor network is limited, the ANASTACIA and organizational controls implemented should greatly mitigate actual impact to data subjects
Risk-4	Limited (2)	HSPL authorization policies, MSPL authorization policies; Virtual firewall and router, SDN switch; CpABE data privacy enabler	Negligible (1) Reason: Possibility of deleting personal data in a factory sensor network is limited, the ANASTACIA and organizational controls implemented should greatly mitigate actual impact to data subjects
Risk-5	Significant (3)	HSPL authorization policies MSPL authorization	Limited (2) Reason: Given the attack vector and the fact that both modems and sensors

[46] See supra section **Errore. L'origine riferimento non è stata trovata.**.

		policies; virtual and physical firewall and router	are attacked, the possibility of using the network to compile personal information is substantial, mitigation and contingency actions limit but do not exclude impact to data subjects
Risk-6	Limited (2)	Data encryption (TLS), channel protection, HSPL authorization policies; virtual firewall and router, MSPL authorization policies	Negligible (1) Reason: Possibility of identifying location or traffic data in a factory sensor network is limited, the ANASTACIA and organizational controls implemented should greatly mitigate actual impact to data subjects
Risk-7	Negligible (1)	Channel protection; Firewall and router, SDN switch	Negligible (1) Reason: The attack vector is not aimed at directly affecting data subject rights or causing service disruption per se. The ANASTACIA and organizational controls implemented should greatly mitigate actual impact to data subjects

Table 32 0day Impact Assessment

Likelihood determination

Likelihood of a successful attack must account the potential consequences, the controls implemented and the estimated impact level such an attack would imply. These elements must be associated with the capabilities of the diverse threat actors which could be interested in performing it, as they are key elements in determining how persistent they will be once they face the security controls that have been deployed. This exercise requires an organization-wide effort to be performed by the CISO, DPO and other interested stakeholders to properly manage risk.

In the context defined by the use-case the following elements are pertinent:

Use Case	Relevant Risks	Relevant Risk Sources	Capabilities	Likelihood[47]
UC_0.1	1, 2, 3, 4, 5, 6, 7	Malicious attacker (Hacker)	Adept (4)[48]	Maximum (4)

Table 33 0day Likelihood Assessment

Risk evaluation, protection approach and contingency planning

As defined before, this use-case presents a **high** likelihood of an event involving privacy risks affecting data subjects. Consequences for most risks could be **significant** and even when considering ANASTACIA controls, there is a **limited** potential for the risks impacting the data subjects in some manner. For this reason, the following protection approach is implemented alongside with the contingencies detailed below.

[47] These values will vary depending on the specific circumstances of each analysed IoT/CPS deployment that is to be examined by ANASTACIA. In the case of the use cases examined by this deliverable, the likelihood value will always be maximum due to the fictitious and certain nature of the described attacks.

[48] The maximum likelihood is to be assumed in case of an unknown threat agent, as preventive and corrective measures should be deployed regardless of the assumed likelihood of an ongoing event.

Protection approach

As defined in D.2.6, to be efficient, the detection and the protection should be made directly on the ZigBee nodes and there are three possibilities at different levels:

1. Firmware level: Creation of a modified version of the firmware, implementing Remote AT Commands filtering or allowing AT Commands elaboration at the application layer. This solution requires a device firmware upgrade to allow total AT Command packet management and at the end, allows the user to configure the IoT device to exclude Remote AT Commands interpretation. This can work only if the firmware is easily modifiable and open-source.
2. Device configuration level: Providing to the user the ability to configure a device to disable support to Remote AT Commands. This needs to implement a specific setting able to disable automatic Remote AT Command interpretation.
3. External level: Demanding protection capabilities to an external application program. This solution is the most effective because it implies to continuously monitor the communication between the ZigBee modem and the connected IoT nodes. If a node is not reachable, an automatic reconfiguration is done to establish again a good connectivity.

Detection and mitigation

As mentioned by D.2.2, there is no common and general protection plan that can be adopted to defend a system from zero-day attacks. However, certain actions like the deployment of a honeynet and continuous maintenance and training of the intrusion detection and prevention systems could help to palliate the risks involved in the scenario.

While detection and mitigation of zero-day attacks is no simple task, implementation of strong intrusion detection systems (capable of both anomaly detection and misuse or signature-based detection) is a good step to maximize the probability of detection. Furthermore, while most of the privacy risks associated to the use-case could be performed through the exploitation of a zero-day vulnerability, it is highly unlikely that the attackers will depend solely on one mechanism. For this reason, by correctly implementing the whole range of tools available to ANASTACIA, the possibility of identifying and mitigating the many security threats associated to any of the privacy risks is considerably enhanced.

ANASTACIA D.2.6 updates this approach to include the following detection and mitigation actions:

Detection:

- Buffered sensor data from smart buildings
- Detection of misbehaviour of the system
- Enabling of continuous and integrated monitoring of multivariate signals, event logs, heartbeat signals, status reports, operational information, etc.

Mitigation:

- Block of the adversary, based on VDSS feedback
- Restore of sensors data (back process)

Privacy Contingency Plan

Once a potential security/privacy threat has been identified, ANASTACIA's should inform the CISO and DPO of:

- The nature of the threat and the actions undertaken to address it
- The latest DPIA available on the system records, to identify predetermined technical and organizational contingencies and actions
- A whether the threat has been materialized in an affectation to data subject's rights.

Contingency actions to be implemented include:

- Definition of incident type and description of circumstances that led to its discovery, along with a description of the incident and contingency actions performed
- Identification of organizational/technical dependencies of the systems involved (vendors/providers, etc.)
- Identification and classification of potential data subjects affected, along with the types of data involved
- Performance of final risk evaluation: definition of privacy relevance of the alert, identification of actual consequences, impact and effectiveness of controls, as well as the identification (if possible) of threat actor involved in the event. Feedback should be provided through the DSPS and an assessment of the risk to the data subject detailed by the DPO.
- A justified decision on whether the event warrants: a) notification to Data Protection Authorities; b) notification to the data subjects; c) an update to the DPIA.
- Compilation of proof of activities undertaken and upload to DSPS.
- Electronic signature of documentation

Specific contingencies to be introduced in this particular scenario include analysis of:

- Affected devices which were not able to be addressed by ANASTACIA
- Attack vector and nature of the zero-day attack implemented (along with review of associated policies, from provisioning to update and maintenance)

6 PRIVACY RISK EVALUATION AND CONTINGENCY VERIFICATION STRATEGY FOR ANASTACIA

ANASTACIA's DSPS will introduce several enablers for Chief Information Security Officers (CISO) and Data Protection Officers[49] (DPO) to help the fulfilment of the risk assessment cycle and comply with the organizational requirements detailed in supra section 4, particularly:

- **Requirement 6 - Records and audit of processing activities and disclosures:** As part of the transparency/accountability actions to be undertaken by the DPO and CISO, a detailed examination of the finally implemented technical and organizational contingencies (which might extend beyond the effective control of ANASTACIA) must be recorded. The provision of this feedback is fundamental for the successful management of risks, for this reason proper documentation must be kept on the final (human-based) risk evaluation phase of privacy risk assessment.
- **Requirement 10 - Update and review privacy measures:** Once the risks have been materialized and the preventative strategies (protection plan, detection actions and mitigation activities) have taken place, the lessons learned should be considered and integrated in the organizational policies and technical controls/mitigations and contingency plans.

Through these envisioned tools, alert information obtained from ANASTACIA's monitoring and reaction frameworks will be intertwined with verified CISO/DPO feedback and stored for accountability/transparency compliance.

To this end, a strategy must be defined to ensure that technical detection, protection and mitigation mechanisms are well aligned with the human-based contingency activities which are necessary to ensure compliance with the GDPR's dispositions. This strategy will directly inform WP5 tasks and will be reflected in both the final version of the DSPS and the upcoming D5.3.

The following strategy has been shaped in consideration of the information available to ANASTACIA and the capabilities of the envisioned system[50]. The general steps that are to be followed to ensure proper integration of the technical and organizational mechanisms are:

1. **Initial system privacy and security verification:** as defined in ANASTACIA Deliverable 5.1, a privacy and security verification should take place before the system is set in place. This step aims to develop the necessary baselines to detect whether a privacy breach has taken place and to perform the organizational tasks required to identify and authenticate the system administrator and data protection officer which will be performing any human-based activities.
2. **Security Risk Assessment / Data Protection Impact Assessment (DPIA):** task to be completed jointly by ANASTACIA representatives, the system administrator and the DPO. This task should be aligned to the organization's privacy policies, legal requirements and data flows, and should be accompanied by the identification of the devices or network elements which are particularly vulnerable to privacy risks (due to the types of data compiled and processed for example).
3. **Detection and automatic mitigation of privacy and security threats:** security threats identified by the system will automatically raise alarms to the DSPS. Policy-defined mitigation activities will be performed by ANASTACIA to reduce the impact of the privacy and security threats.
4. **Recommended contingencies displayed:** The DSPS will update its status automatically to reflect any changes in system security and privacy and will alert the system administrator of potential risks to the system. Its GUI will also present instructions to the DPO on recommended contingencies to be

[49] See ANASTACIA D.5.1, D5.2 and the upcoming D.5.3 for more information.

[50] It is necessary to recognize that the personal data protection requirements identified through section 4 (and as further defined by the GDPR) included elements which are not addressable through ANASTACIA. As such, the risks and associated contingency mechanisms identified throughout this deliverable should be closely examined by the DPO in charge of the system that is monitored by ANASTACIA. The DPO should be well aware of ANASTACIA's capabilities and limitations, and dully perform the system/data verification that might be beyond ANASTACIA's capabilities to properly determine whether a breach of personal data has taken place.

implemented by considering the types of affected devices, the duration and impact of the attack and the effectiveness of the mitigation activities.

5. **DPO/CISO input required to DSPS before restoration of privacy seal:** while most of the security elements of the DSPS will be automatically updated to reflect the restoration of normal system behaviour, those elements of the DSPS[51] which reflect personal data protection in the system will continue to reflect the potential breaches until the DPO certifies[52] through direct feedback and electronically signed documentation declaring that the contingencies have taken place and that the technical and organizational review (and update, if necessary) has been performed. This feedback process will be performed thorough the implementation of a post-alert questionnaire requiring an evaluation of the risk and the potential introduction of scheduled activity reports to be submitted by both the DPO and the CISO. An early example of the post-alert questionnaires to be presented to the DPO/CISO can be found in Annex 2.
6. **Data Protection Impact Assessment Update (optional)**: the CISO/DPO will be provided with an opportunity to update their assessments and to add them to the DSPS, both for transparency/accountability purposes and for future reference.

[51] For more information on the DSPS, see (Quesada Rodriguez et al., 2017).

[52] DPO certification of human-based contingency activities will be performed through electronic signature (as governed by the eIDAS Regulation (Kirova, 2016)) or equivalent means capable of fulfilling the non-repudiation principle and guaranteeing that the DPO has approved the activities implemented to address the situation.

7 CONCLUSIONS

This deliverable presents the final results of ANASTACIA Task 2.3 research. It updates the data protection requirements and network-level privacy risks to be addressed by the ANASTACIA platform; the mitigation and contingency actions to be considered; and the specific approaches to be implemented when addressing the 11 use-cases of the project.

To this end, the deliverable performed an ISO-based risk analysis process was then followed to identify the consequences, threats, impact and likelihood of the identified privacy risks and, after their evaluation a set of recommended actions were designed for each. Additionally, the risk evaluation and contingency verification strategy were further specified to introduce the results of the contingency actions implemented by the DPO to ANASTACIA's DSPS in order to ensure the platform's compliance with the broader (local, national or sector-specific) data protection requirements applicable to the organization.

The models and contingency mechanisms developed in this document will be tested in the following months through their integration with the workflow of ANASTACIA WP4 and WP5.

8 REFERENCES

Article 29 Data Protection Working Party. (2017, April 4). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. Retrieved from ec.europa.eu/newsroom/document.cfm?doc_id=44137

Bianchi, S., Troglio, G., Belabed, D., Mady, A., Farris, I., Scudiero, L., … Trapero, R. (2017, June 30). *ANASTACIA D1.2 "User Centred Requirements Initial Analysis."* Retrieved from http://anastacia-h2020.eu/deliverables/ANASTACIA-WP1-T1.2-SOFT-D1.2-UserCentredRequirementsInitialAnalysis-v11.pdf

Cambiaso, E., Mongelli, M., Vaccari, I., Trapero, R., El-Din Mady, A., Belabed, D., … Scudiero, L. (2017, June 30). *ANASTACIA D.1.1 "Holistic Security Context Analysis."* Retrieved from http://www.anastacia-h2020.eu/deliverables/ANASTACIA-WP1-T1.1-CNR-D1.1-HolisticSecurityContextAnalysis-v0.6.pdf

Cambiaso, E., Papaleo, G., & Aiello, M. (2017). Slowcomm: Design, development and performance evaluation of a new slow DoS attack. *Journal of Information Security and Applications*, *35*, 23–31. https://doi.org/10.1016/j.jisa.2017.05.005

Cambiaso, E., Papaleo, G., Chiola, G., & Aiello, M. (2013). Slow DoS attacks: definition and categorisation. *International Journal of Trust Management in Computing and Communications*, *1*(3/4), 300. https://doi.org/10.1504/IJTMCC.2013.056440

Cambiaso, E., Vaccari, I., Punta, E., Scaglione, S., Bianchi, S., Trapero, R., … Rivera, D. (2018, February 28). *ANASTACIA D2.2 Attacks Threats Analysis and Contingency Actions*.

Casey, T. (2007, September). *Threat Agent Library Helps Identify Information Security Risks*. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Intel - Threat Agent Library Helps Identify Information Security Risks.pdf

CNIL. (2018, February). *Analyse d'impact relative à la protection des données (PIA) La méthode*. Retrieved from https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf

European Parliament, E. C. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). , Pub. L. No. 32016R0679, 119 OJ L (2016).

European Parliament, & European Council. *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. , (2016).

Guri, M., Zadov, B., Bykhovsky, D., & Elovici, Y. (2018). PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines. *ArXiv:1804.04014 [Cs]*. Retrieved from http://arxiv.org/abs/1804.04014

International Organization for Standardization. (2008, December). *ISO/TS 25237:2008 Health informatics -- Pseudonymization*. Retrieved from https://www.iso.org/standard/42807.html

International Organization for Standardization. (2009). *ISO 31000:2009(en) Risk management — Principles and guidelines*. Retrieved from https://www.iso.org/iso-31000-risk-management.html

International Organization for Standardization. (2011, November). *ISO 19011:2011 Guidelines for auditing management systems*. Retrieved from https://www.iso.org/standard/50675.html

International Organization for Standardization. (2013, October). *ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements*. Retrieved from https://www.iso.org/standard/54534.html

International Organization for Standardization. (2017, June). *ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment*. Retrieved from https://www.iso.org/standard/62289.html

International Telecommunications Union. (2012, June 15). *Recommendation Y.2060: Overview of the Internet of things*. Retrieved from https://www.itu.int/rec/T-REC-Y.2060-201206-I

Kirova, M. (2016, June). *eIDAS Regulation (Regulation (EU) N°910/2014)*. Retrieved from https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

One Trust LLC. (2018). *Incident Response Playbook and Ultimate Incident and Breach Management Handbook*. Retrieved from https://www.onetrust.com/resources/onetrust-incident-and-breach-response-toolkit/

Quesada Rodriguez, A., Bajic, B., Menon, M., Ziegler, S., Pacheco Huamani, A. M., & Kim, E. (2017, December 31). *ANASTACIA D.5.1 "Dynamic Privacy and Security Seal Model Analysis."* Retrieved from http://www.anastacia-h2020.eu/deliverables/ANASTACIA-WP5-T5.1-MAND-D5.1-DynamicPrivacyAndSecuritySealModelAnalysis-v1.0.pdf

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015). Network-level security and privacy control for smart-home IoT devices. *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 163–167. https://doi.org/10.1109/WiMOB.2015.7347956

ANNEX 1: ANASTACIA ENABLER DESCRIPTION

Type	Function	Name	Developer	Technical Description	Simple Description
Basic security mechanisms for IoT	Power management (on/off control)	iot_controller	UMU	"IoT controller is able to receive requests over a northbound rest API in order to communicate an manage IoT devices by using IoT specific protocols like CoAP or MQTT"	"IoT controller allows enforcing security policies related to IoT management. For instance, to access specific resource in the IoT device like power management or interface management."
Basic security mechanisms for IoT	Traffic protection management	dtls_proxy	ODINs/UMU	"DTLS proxy implements a northbound rest API which receives IoT specific channel protection configurations (DTLS) and it prepares a secure endpoint according on the received configuration."	"DTLS proxy allows enforcing channel protection security policies for those endpoints who are not DTLS enabled."
Network Function Virtualization (NFV)	Virtual honeypot	cooja/IoT Honeynet agent	UMU	"The IoT Honeynet agent implements a northbound rest API which receives Cooja CSC configurations and apply them in a new instance of Cooja IoT simulator. "	"Cooja is an IoT simulator for an specific IoT Operative System (Contiki). It allows to deploy Contiki-based IoT honeynets and honeypots using 6LowPAN as contraint communication protocol. "
Network Function Virtualization (NFV)	Virtual honeypot	Kippo	UBITECH	Kippo enabler implements a python-based SSH honeypot.	Kippo is an SSH honepot. It is used to log brute force attacks and the entire shell interaction performed by an attacker.
Privacy	Data encryption	CpABE_data_privacy	ODINS/UMU	"CpABE data privacy enabler implements attribute based encryption data privacy. This is, the data is cyphered with specific attributes and only the entities with the same attributes will be able to decrypt and therefore access the data. "	"Data privacy enabler allows that the data is only accesible for those which accomplish specific requirements."
Other	Authorization	XACML-PDP	ODINS	"XACML-PDP enabler implements a user interface to define XACML configuration and apply it in the Policy Decision Point, in order to authorize/unauthorize the access to specific resources."	"XACML allows specify authorization statements, e.g., ""Subject X can access specific kind of data"""
Other	Authentication	AuthN-enabler	ODINS	The PANA Authentication enabler implements secure bootstrapping process to apply them over the authentication system (e.g., AAA architecture).	Authentication enabler allows secure bootstrapping for new devices starting in the network.

"Behavioral Engine for Detecting Malicious Activities in Cyber Physical Systems"	CP-Learning threats detection	Monitoring agent	UTRC	"Data analysis agent is composed of messaging wrappers, constraint programming (CP) models for detection model and buffered sensor data from IoT networks. Data analysis agent performs system level monitoring by aggregating information from SEP using Kafka broker. The information processing inside agent can be done via, monitoring – received messages are processed, filtered and cleaned to enable data recording for future model training and attack verdict generation that will be sent to reaction components, and detection – system level analysis of current security state of SEP based on trained model and current information stored in monitoring buffer. The agent will generate appropriate attack verdict that will be sent to VDSS component via Kafka broker. "	"The model is built on IoT continuous stream of data (i.e., time-series) where the time interval between successive updates could vary from milliseconds to minutes. Our model consists of a network of relations between cyber-physical sensor data. We aggregate the different types of cyber-physical sensor data to truly model the normal behaviour of the system. This model is built to monitor and detect at different levels. For example, CPU consumption of a device can be included along its actual sensor data. Moreover, we consider variety of data that allows the model to be as generic possible. More specifically, the idea is to learn a set of relations which together when satisfied defines the normal behaviour of the system. The proposed approach for learning detection model that includes operational, system, and network data to detect advanced attacks. The developed decision model by learning a set of constraints/relations from the data that conjunctively defines the normal operation of a CPS. The constraint-based decision model is the core component of our behavioral detection engine that gathers and analyses information in order to identify any intrusion or outliers. "

ANNEX 2: POST-ALERT QUESTIONNAIRES

Data Protection Officer[53]:

1. *Alert information (Mandatory)*
   - *Date of incident*
   - *Date of discovery*
   - *Type of incident*
   - *Extended description (optional)*
2. *Description of incident (Mandatory)*
   - *Cause of incident*
   - *Assets involved*
   - *Contingency actions performed*
   - *Clients/vendors involved*
   - *Data elements (name, data, …)*
   - *Data subject categories*
   - *Number of data subjects*
   - *Number of records*
   - *Risk to the data subject (0-4)*
   - *Should this incident be notified to a Data Protection Authority?*

   Please justify this decision and attach supporting documentation
   - *Should this incident be notified to the data subject?*

   Please justify this decision and attach supporting documentation
3. *Please upload any supporting documentation that you deem relevant for transparency or accountability purposes.*

CISO:

1. *Alert information (Mandatory)*
   - *Date of incident*
   - *Date of discovery*
   - *Type of incident*
   - *Extended description (optional)*
2. *Based on the alert, should this be recorded as a information security incident?*

If yes, please specify:

   a. *Cause of the incident*

[53] Both these questionnaires have inspired on (CNIL, 2018; International Organization for Standardization, 2013, p. 27; One Trust LLC, 2018)

b. *Networks involved*

c. *Assets involved*

d. *Clients/vendors involved*

e. *Data compromised*

f. *Categories of individuals affected by the incident*

g. *Number of individuals affected*

h. *Number of data records compromised*

i. *Review of data risk*

j. *Prior public availability of the data*

k. *Use of encryption*

l. *Suspected threat agent*

m. *To what extent has the risk been mitigated by ANASTACIA?*

o. *Technical or organisational protection measures already in place*

p. *Describe contingency measures taken to address the alert*

2. Did you respond to the information security incident in accordance with the documented procedures? If yes, please provide details.

3. Did you define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence? If yes, please provide details.

4. Did you use the knowledge gained from analysing and resolving information security incidents to reduce the likelihood or impact of future incidents? If yes, please provide details.

5. Did you report the information security incident through appropriate management channels as quickly as possible? If yes, please provide details.

6. Please provide a simplified summary of the situation to be submitted to the DPO along with any recommendations you might have.