GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform

FARES 2019

Tuesday 27th August, 2019

Martin Horák, Václav Stupka, **Martin Husák**

MUNI ICS

CSIRT-MU

Introduction

GDPR – General Data Protection Regulation

- Novel legal framework of the EU, enforcable from May 2018.
- Implies also obligations of the CERT/CSIRT community.
- Caused heated debates, including fear and uncertainty.

DPIA – Data Privacy Impact Assessment

- Recommended procedure to investigate risks to privacy in an assessed system.
- Detailed assessment of a system that processes personal data.

Information Sharing in Cyber Security

CSIRT-MU

Information Sharing in Cyber Security

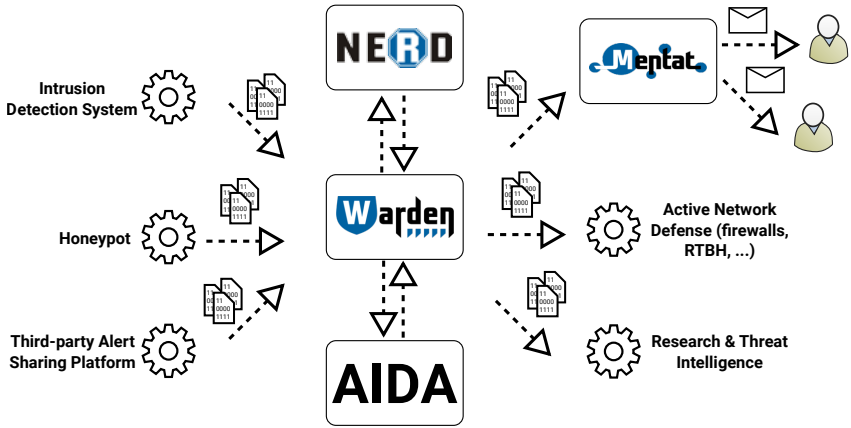
Information sharing in cyber security

- Fundamental to CERT/CSIRT operations.
- In many cases automated via sharing platforms and other tools.
- GDPR-compliant, as stated in the related work.

SABU Alert Sharing Platform

- System asssessed in this work.
- Exchange of intrusion detection alerts between peers mostly in Czech Republic.
- Voices of fear and uncertainty from the community regarding the GDPR.

SABU – Assessed Alert Sharing Platform



CSIRT-MU

Security Alert Sharing Platforms and Personal Data

What are personal data?

- "any information about identified or identifiable person"
- including online identifiers – IP addresses, emails, URLs, . . .

What is shared among CSIRTs?

- IoC – IP addreses, email, URLs, . . .
  in some cases even pieces of transferred content.
- Shared data can be combined with other data to identify a person,
  thus, all shared data should be treated as personal.

Data Protection Impact Assessment

CSIRT-MU

Data Protection Impact Assessment

The DPIA Process in Brief

1. Getting information about the assessed system
2. Mapping the description of the assessed system
3. Risk identificaiton and evaluation
4. Controls identification
5. Documentation and planning of review schedule

CSIRT-MU

Risk identificaiton and evaluation

1. Inability of data subject to exercise rights

- Lot of peers, operators, various identifiers, . . .
- Inference with the rights of subjects is proportionate to the intended purpose of processing and legitimate interests.
- Risk is very low.

2. Loss of control over the use of personal data / loss of confidentiality

- Peers are likely to provide unnecesasry details on an incident.
- Information may leak via any peer in the platform.
- Risk is minimal – community is trustworthy and only minimal required data are stored (no attachments with potentially sensitive data).

Risk identificaiton and evaluation

3. Inability to access services or opportunities

- Blacklists should not be based solely on the reputation database.
- Reputation scoring may be considered as profiling in the meaning of the GDPR.
- Severity and likelihood are medium.

4. Other economic or social disadvantage

- Reputational damage if a subject was under a cyber attack.
- Risk is very low.

Controls identification

Existing

- Encryption of network communication.
- Deleting the obsolete data.
- Data access management and accounting.
- Legal documents describing responsibilities and duties of peers.

Newly proposed

- Peers should state security as a purpose for collecting the data.
- Peers should allow access to the system only to operators who signed NDA.
- Users of the data should be aware of the origin of the data.

Documentation and Planning of Review Schedule

Suggested structure

1. Identification of purposes for which was DPIA conducted.
2. Description of getting information about the assessed system – what documents were examined, which stakeholders were consulted, and what were the lessons learned.
3. Description of the information system, information flows, and mechanism of personal data processing.
4. Identification and evaluation of risks for rights and freedoms of data subjects.
5. Identification of existing controls and newly proposed controls.
6. Plan for the implementation of newly proposed controls.
7. Conclusion of DPIA results and planning the review schedule.

CSIRT-MU

Conclusion

Conclusion

GDPR and Cybersecurity Operations

- GDPR affects sharing the information among CERTs/CSIRTs
- Intrusion detection alert sharing platform were threatened by fears and doubts.

Solution for the SABU platform

- Conducting DPIA, a thorough analytical process, to assess risk in the system.
- Result – “much ado about nothing” – risks are not high.
- Still, the DPIA results are solid argument for data sharing under GDPR.
- Side effects – improving quality of the system, its documentation, and community management.

THANK YOU FOR YOUR ATTENTION!

sabu.cesnet.cz

@csirtmu

Martin Husák

husakm@ics.muni.cz

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION, YOUTH AND SPORTS

MUNI ICS

CSIRT-MU