
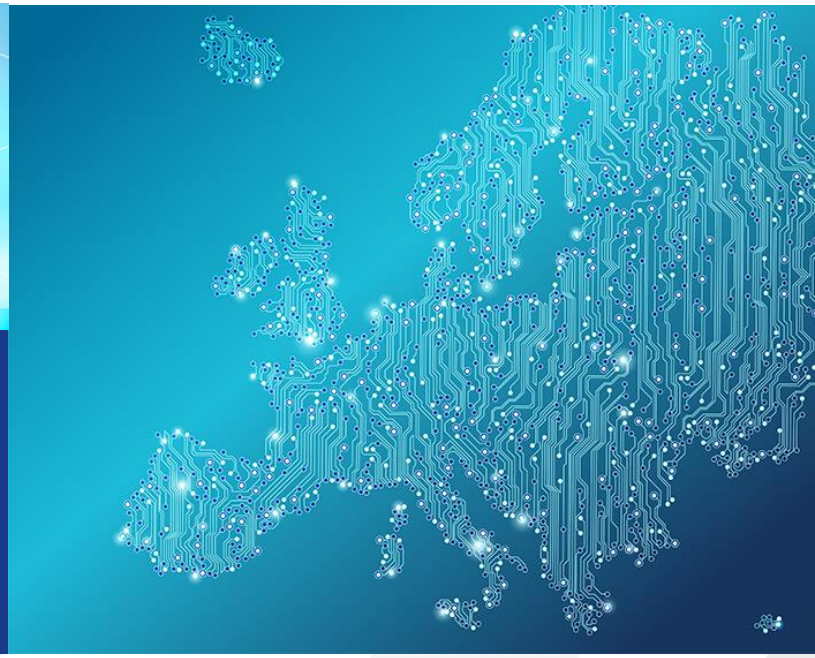

# Cyber Security Challenges in Big Data

Rossen Naydenov
Officer in Network and Information Security - ENISA

European Union Agency for Network and Information Security

# Positioning ENISA activities

HANDS ON

POLICY IMPLEMENTATION

MOBILISING COMMUNITIES

RECOMMENDATIONS


# What is Big Data

- No ISO standard for defining Big Data

- Big Data system is defined as the technologies, the set of tools, the data and the analytics used in processing large amount of data.


- **Characteristics**
  - Volume – size of data
  - Velocity – the speed at which the data is coming/being processed
  - Variety/Variability – the difference in speed, format, semantics
  - Veracity – trustworthiness of data

# Big Data Benefits

**Finding New Insights**

- Blending and analysing internal and external data brings new insights

**Competitive Advantage**

- Provide better services – more personalized
- Offer new services

**Identifying trends**

- Helps better prepare the organization for the future
- Better business development

**New Market Possibilities**

- Big Data organization could offer services to new customers in another market area

# Big Data Security Challenges

## Access Control & Authentication

- Ensuring proper access to users and entities
- Different entities have different security capabilities

## Source Validation & Filtering

- Sources are from external (not trusted) mediums
- Filtering of sources might not be possible due to their nature

## Secure Data Management

- Enormous data is difficult to store and secure
- The produced results may also be sensitive

## Application and Infrastructure Security

- Applications not always designed with security in mind
- Infrastructure devices with different level of security

# Big Data Security - Status

- Big Data Players still not a very big community
- Applications and devices not always have security embedded
- Filtering sources is becoming a problem - new sources are becoming available, with new devices (IoT)come to play constantly
- New sources do not provide enough information to be trusted
- Supply chain security – most of the sources are supplied by third party providers

# Big Data Security – Findings 1/2

- **Access control and authentication** – Different entities authentication and access to data from multiple locations may not be sufficiently controlled.
- **Secure Data Management** – Backup and restore become an issue with the enormous data gathered that needs to be protected
- **Source Validation and Filtering** – new sources become available every day, makes validation and filtering nearly impossible
- **Application Security** – application security needs to be tested, some of them offer no security, could lead to wrong computation
- **Infrastructure security** – most of the sources are by devices exposed to the elements and to malicious behavior

# Big Data Security – Findings 2/2

- **Encryption** – New types of encryption allow for computation without the need of revealing the private key for decryption
- **Distributed Systems Security** – this is inherited from the use of Cloud in Big Data systems, distributed denial of service could be a potential threat
- **Devices interoperability** – new sources and devices do not offer the same level of security
- **Logging and Monitoring** – the logs generated by the Big Data system become Big Data
- **Supply Chain Security** – how can an end user validate that the devices used in the Big Data systems are secure

# Potential Opportunities

## Offer security in the Big Data products

- If a vendor could develop or offer security capabilities in their products would be a key benefit

## Help adapt or create standards for use in Big Data

- Standards must evolve to offer the right tools for protection
- Certification for security of Big Data systems

## Privacy and Data protection by design

- Embedding privacy measures and privacy enhancing technologies (PETs) directly into the design of data processing systems.

## Continue enhancing the skills of people

- Trainings and certification to people to use and create secure Big Data systems

# Conclusions

- Big Data brings significant business benefits to the organizations

- cyber security and privacy are key enablers for the smooth Big Data adoption

- existing standards and do not cover fully cyber security challenges related to Big Data

**ENISA will co-operate with policy makers (e.g. EC), standardization bodies & private sector (e.g. Big Data providers) to achieve secure Big Data adoption in the critical sectors**

# Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu