Security and Resilience in Cloud Computing

Rossen Naydenov
Officer in Network and Information Security
European Network and Information Security Agency
Rossen.Naydenov@enisa.europa.eu

ENISA - Who We Are

- Established in 2004
  - Based in Greece (Athens and Heraklion)
  - Approximately 75 staff
- Mission:
  - Promote the exchange of Information Security best practices
  - Establish NIS dialogue between Member States and Industry
  - Bridge communities
  - Provide expertise and advice
- 3 Areas
  - Regulation, implementation, cooperation
  - Conduct studies and provide recommendations
  - CERTs and Cyber Exercises

ENISA's Work in the area of Cloud

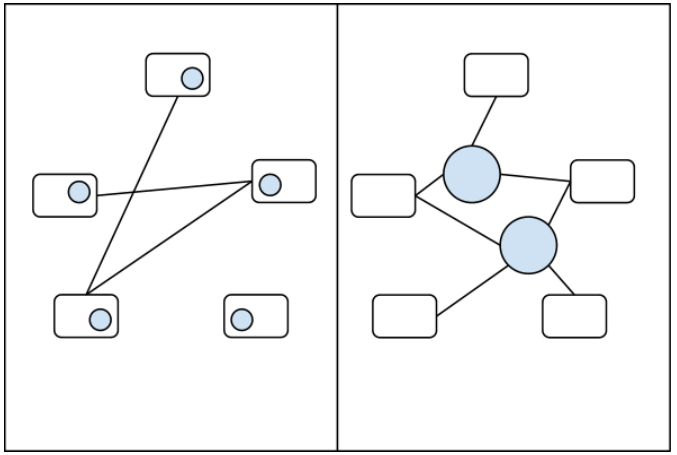
- 2009 Cloud computing risk assessment
- 2009 Cloud security Assurance framework
- 2012 Procure secure (Security in SLAs)
- 2013 Critical cloud computing
- 2013 Incident reporting for cloud computing
- 2013 Securely deploying GovClouds
- 2013 Support EU Cloud Strategy
- 2014 Cloud Certification Meta-Framework
- 2014 Procurement security in GovClouds
- 2015 Cloud Security guide for SMEs
- http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

Cloud Security Highlights: Procure Secure

- Guide for customers on monitoring security parameters of cloud services
- Checklist with questions to ask
- Security parameters
  - How to define
  - How to measure
- Examples of security parameters
  - Service availability
  - Incident response
  - Vulnerability management

Cloud Security Highlights: Critical Cloud Computing

- Analyse critical dependencies on cloud computing
  - Which critical services depend on cloud computing
  - What would be the impact of failures
- Recommendations
  - What should we do to prevent large scale failures
  - Which datacentres and cloud services should be considered critical
- Some ideas
  - Transparency about dependencies
  - Incident reporting for cloud providers
  - Minimum security measures for cloud providers



Incident Reporting for Cloud Computing

- Scope
  - EU Cyber security directive: Article14
- Objectives
  - Support the implementation of the incident reporting
  - Provide advice and facilitate exchange of best practices: *how regulators can supervise security, how to analyse risks from a national perspective*
  - Identify Incident report parameters – duration, geographic spread, number of organizations affected
- Deliverable: Incident reporting for cloud computing

Governmental Clouds

- Scope
  - Support the EC Cloud strategy to facilitate the take up of cloud services by the public sector in the EU
- Objectives
  - Overview of the cloud computing uptake in the public sector, across the EU
  - Identification of standards implementation approaches (outsourced, insourced, procurement rules etc.)
  - Recommendations on implementing governmental cloud
- Deliverable: Securing Governmental Cloud Computing Infrastructures across the EU

Cloud Computing Activities - Overview

- One multi annual expert group on Cloud
  - ENISA cloud security and resilience experts group
- Deliverables 2015
  - Good Practices for the use of Cloud Computing in the area of Finance Sector
- Supporting activities
  - Supporting the EU cloud strategy:
    - EU Certification Special Interest Group (SIG)
    - ETSI Standardization Working Group (WG)
    - Task Force on Cloud adoption in the Finance Sector in cooperation with European Banking Authority (EBA)
    - Cooperation on Secure Retail Payments (SecuRePay group)

ENISA Cloud Security and Resilience Experts Group

- Experts group setup: 25 experts from
  - 11 governmental bodies (NL, ES, GR, DK, UK, RO etc.)
  - 10 cloud providers/ vendors (Amazon web services, Google, Microsoft, Atos, HP, Verizon, BT, TrendMicro)
    - ENISA portal, discussion forum, mailing list
    - Regular meetings to discuss hot topics
- Objectives
  - EU Cyber Security Strategy
  - Network Information Security Directive
  - ENISA's cloud horizon

Current Developments on Cloud Computing

Good Practices for the use of Cloud Computing in the area of Finance Sector

- Identification of critical challenges to cloud computing adoption in the Finance sector
- Assess legal and regulatory context (challenges and opportunities) in all member states
- Support industry and understand their uptake – why do some use and some don't use cloud
- Propose recommendations

Current Developments on Big Data

Good Practices and Recommendations on the Security and Resilience of Big Data Services

- Analyze the state of Big Data adoption
  - What architectures are commonly used
  - What applications are commonly used
- Identify and document Big Data Industry's use cases
  - Which sectors use Big Data
  - For what purposes
  - Is the security model different than the general accepted
- Conclusions and key NIS recommendations

ENISA Contributions to Critical Sectors

ENISA is part of the Trusted Service Providers' (TSP) group on incident reporting under Article 19.

- ENISA Article 19 expert group chaired by ENISA, composed of experts from authorities:
  - Certification Authority/Browser (CAB) forum
  - The European Commission
  - The Forum of European Supervisory Authorities (FESA)

ENISA Contributions to Critical Sectors Telecom

ENISA is part of the Telecom working group on incident reporting under article 13a.

- The working group consists of: National Regulatory Authorities (NRAs) and ministries in the EU
- ENISA also chairs a Telecom industry group which consists of major telecom providers – Telecom Italia, Vodafone, Telefonica, etc.

ENISA Contributions to Critical Sectors Finance

ENISA is part of the SecuRe Pay (Security of Retail Payments) working group.

- The working group consists of:
  - EU central banks and national supervisory authorities,
  - the European Central Bank (ECB)
  - the European Banking Authority (EBA)
  - Also The European Commission, Europol and national supervisory authorities of Norway, Liechtenstein and Iceland have observer status.

Three working streams on:

- Major incidents
- Strong Customer Authentication
- Common and Secure Requirements for Communication

Summary

ENISA is a broker between Industry and Institutions (MS, EU, …)

In general ENISA will:

- Provide guidance and good practices for Cloud and Big Data and in general for securing critical information infrastructure
- Develop good practices that would pave the way for a harmonized implementation of rules and regulations (e.g. in the area of cloud area)
- Engage with communities (Industry's) through different expert groups and validate our results through workshops

Where you can help

- Provide insights on key Network Information Security Challenges you face
- Contribute information to work in progress – participate in surveys or in expert groups
- Raise questions on current issues and/or regulations

Questions?