Cloud Computing Security

Marnix Dekker, ENISA

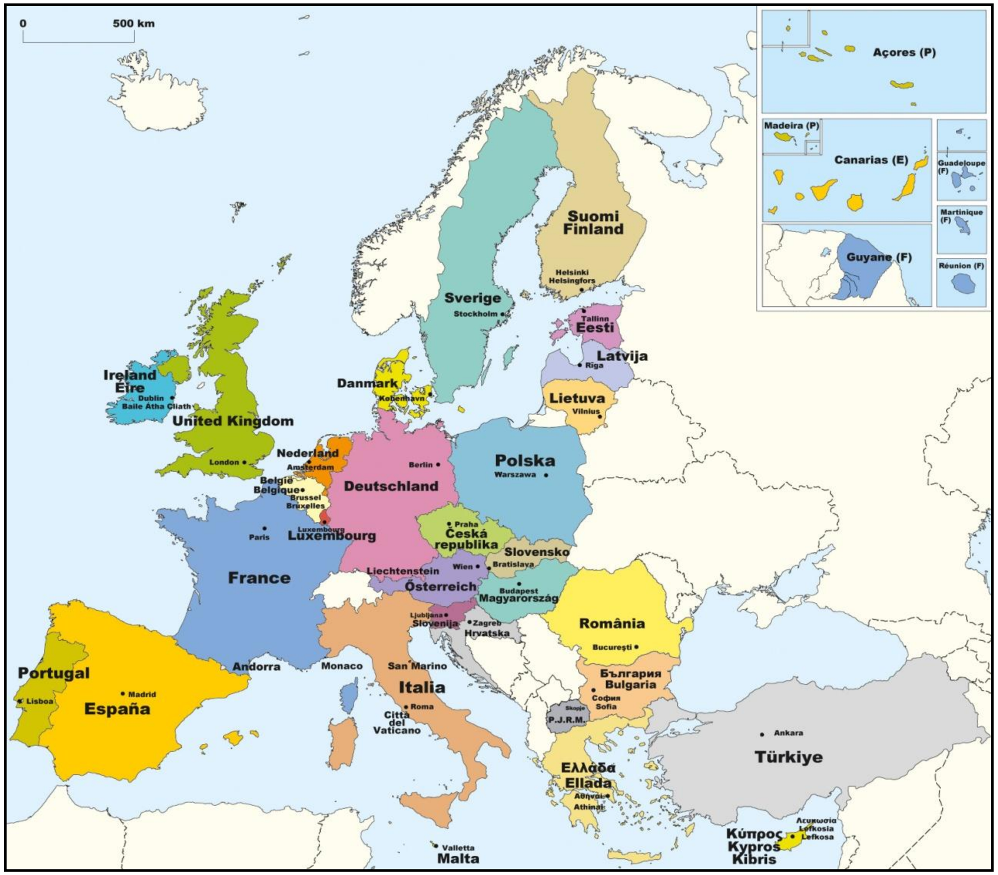
Govcloud session, at ITAPA 2010, Bratislava

Agenda

- **About ENISA**
- Our position on Cloud computing
- Activities in Cloud computing
- Highlights of ENISA’s 2009 Cloud computing report
- Ongoing and future work

The EU

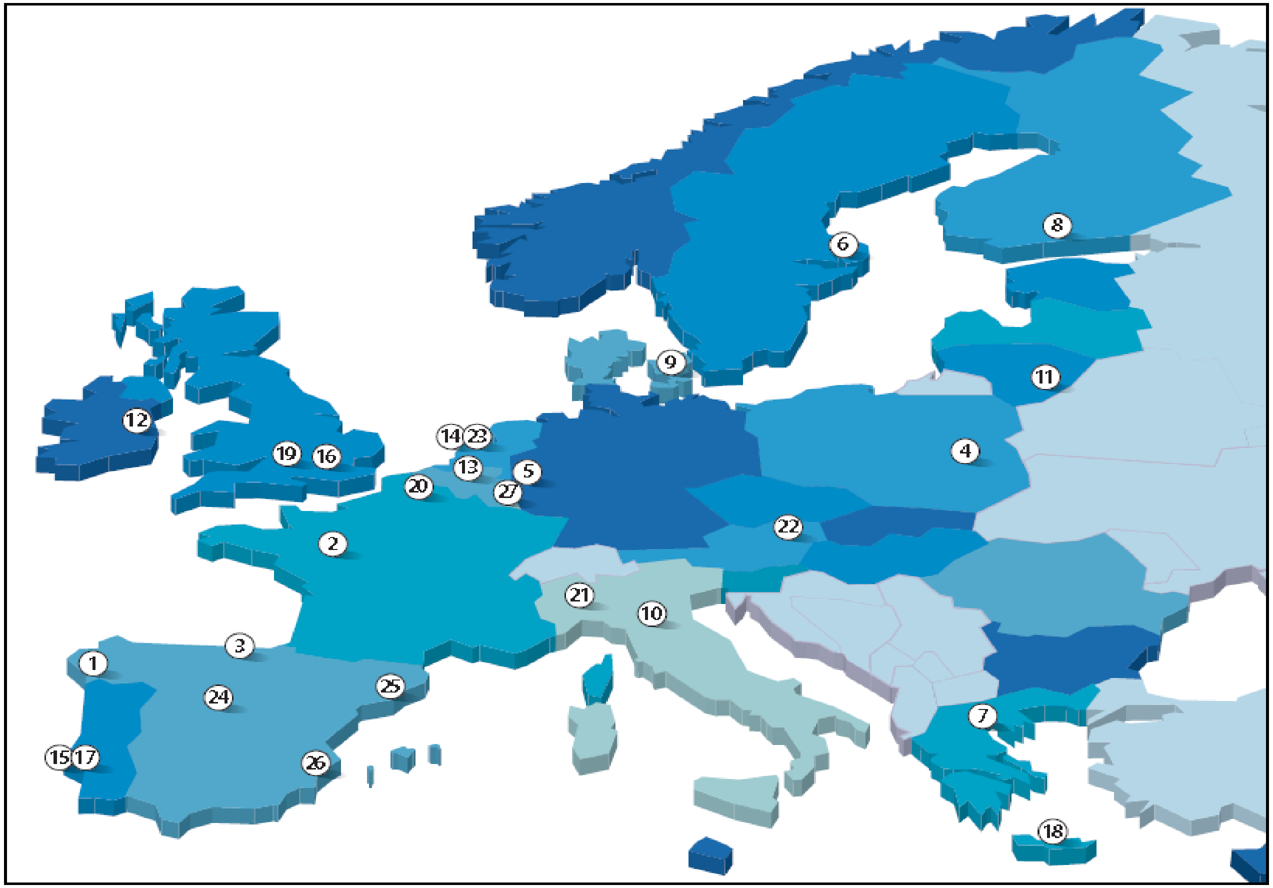
- 500 million people in 27 countries



- 23 languages
- 1 EU anthem
  - “Ode and die Freude” from Beethoven’s 9th

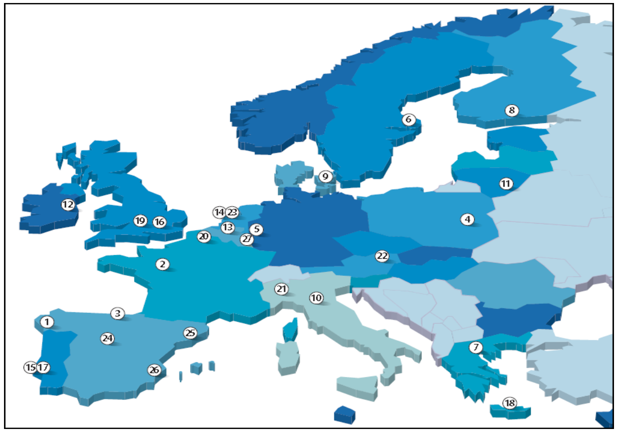
EU agencies

- 27 agencies spread across the EU



The EU agencies

- Agencies are separate from the EU institutions.
- Set up by legislation for very specific technical, scientific or managerial tasks.
- For example:
  - CFCA - Community Fisheries Control Agency
  - EASA - European Aviation Safety Agency
  - ECDC - European Center for Disease Prevention and Control
  - EEA - European Environment agency
  - Et cetera.



About ENISA

- European Network and Information Security Agency
- ENISA is a body of expertise on information security
- Set up in 2004 by the EU - a new mandate is due in 2012.
- Located in Heraklion, Greece.
- Employs around 30 information security experts and 20 staff.
- Assists EU Member States and the EU Commission with issues that affect the European Union as a whole.
- Facilitates the collaboration and information exchange across the EU.
- ENISA has an advisory role (not operational) and the focus is on prevention and preparedness.

Main activities of ENISA

- Advising and assisting the Commission and the Member States on information security.
- Collecting and analysing data on information security practices in Europe and emerging information security risks.
- Promoting risk assessment and risk management methods.
- Awareness-raising and collaboration with different actors in the information security field.

Agenda

- About ENISA
- **Our position on Cloud computing**
- Activities in Cloud computing
- Highlights of ENISA’s 2009 Cloud computing report
- Ongoing and future work

ENISA's view on Cloud Computing

Cloud computing is a new way of delivering computing resources, not a new technology.

ENISA’s view on Cloud Computing

- Highly abstracted computing resources
- Near instant scalability and flexibility
- Near instantaneous provisioning
- Customers share resources
- Service on demand, usually with a pay as you go billing system.
- Programmatic management of resources
    - For example through a webservices API

ENISA's goals

- Help business and governments reap the cost benefits of cloud computing

in a secure way (maintaining service availability, data confidentiality and data integrity).

ENISA’s goals

- Establishing trust across providers and clients

by promoting information security best-practices and standards.

ENISA’s goals

- Improving transparency

ENISA's goals

- Recommending R&D investments

Agenda

- About ENISA
- Our position on Cloud computing
- **Our activities in Cloud computing**
- Highlights of ENISA’s 2009 Cloud computing report
- Ongoing and future work

Our activities in cloud computing

- Cloud Computing: Benefits, Risks and Recommendations for Information security 2009
- Assurance framework 2009
- Research Recommendations 2009
- GovCloud – a security and resilience analysis (due 2010).
- Member of the Common Assurance Maturity Model (CAMM) consortium (ongoing).
- Procurement and monitoring guidance for government cloud contracts (ongoing).

Agenda

- About ENISA
- Our position on Cloud computing
- Our activities in Cloud computing
- **Highlights of ENISA's 2009 Cloud computing report**
- Ongoing and future work

Highlights of ENISA's 2009 Cloud computing report

Cloud Computing
November
09
Benefits, risks and recommendations for information security
enisa

- Cloud Computing: Benefits, Risks and Recommendations for Information security
- 27 experts involved
- Focussed on a SME needs and requirements.

Highlights of ENISA's 2009 Cloud computing report

Cloud Computing

Benefits, risks and recommendations for information security

November | 09

- ○ 8 security benefits
- ○ 53 vulnerabilities considered
- ○ 24 cloud-specific risks identified
- ○ Information Assurance (framework), Legal and Research recommendations.

Security Benefits

Benefits of Scale

Economy of scale

- Security measures are cheaper when implemented on a larger scale
  - Filtering
  - patch management
  - hardening of virtual machine instances and hypervisors
  - Et cetera
- Redundancy and failover across multiple locations comes is part of the standard package.
- More specialized staff, and more experienced staff.
- Money spend on security buys better protection.

Standardization of resources

- Updates can be rolled out much more rapidly across a homogenous platform
- Default VM images and software modules can be updated with the latest patches and security settings
- Snapshots of virtual infrastructure (in IaaS) can be taken regularly and compared with a security baseline.

The Risks

Cloud services are big juicy targets

- Most risks are not new, but they are amplified by resource concentration
  - Trustworthiness of insiders.
  - Hypervisors - hypervisor layer attacks on virtual machines are very attractive.
  - More data in transit (not always encrypted)
  - Management interfaces

Loss of Governance

- The client cedes control to the Provider on a number of issues effecting security:
  - External pen testing not permitted.
  - Very limited logs available.
  - Usually no forensics service offered
  - No information on location/jurisdiction of data.
  - Outsource or sub-contract services to third-parties (fourth parties?)
- SLAs may not offer a commitment to provide the above services, thus leaving a gap in security defences.

Lock in

- Few tools, procedures or standard formats for data and service portability.
- Difficult to migrate from one provider to another, or to migrate data and services to or from an in-house IT environment.
- Potential dependency of service provision on a particular CP.

Compliance Challenges

- Cloud Provider cannot provide evidence of their own compliance to the relevant requirements
- Cloud Provider does not permit audit by the Cloud Customer
- In certain cases, using a cloud implies certain kind of compliance cannot be achieved

Legal and contractual risks

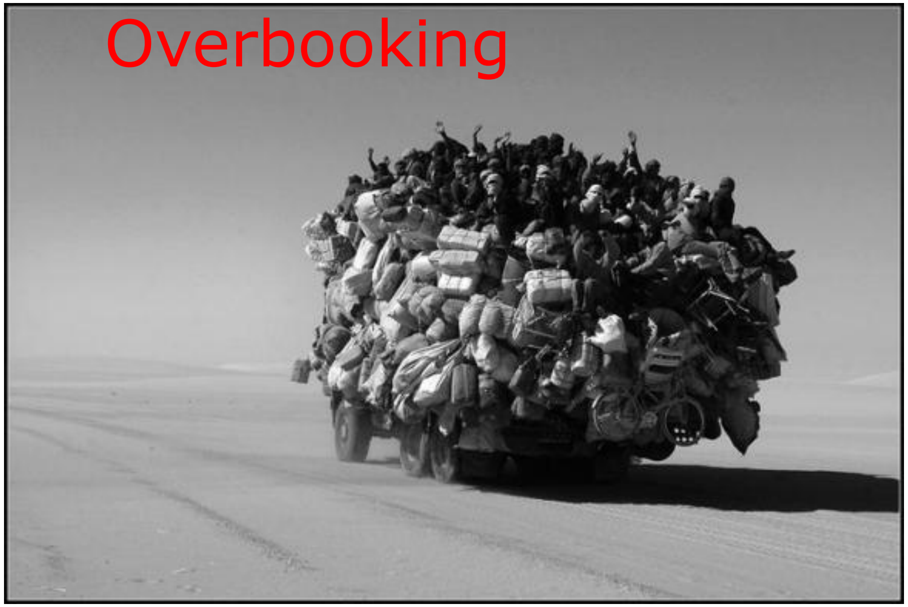
- Data in multiple jurisdictions, some of which may be risky.
- Lack of compliance with EU Data Protection Directive
  - Potentially difficult for the customer (data controller) to check the data handling practices of the provider
  - Multiple transfers of data exacerbated the problem
- Subpoena and e-discovery
- Confidentiality and Non-disclosure
- Intellectual Property
- Risk Allocation and limitation of liability

Isolation failure

- Storage (e.g. Side channel attacks see http://bit.ly/12h5Yh)
- Memory
- Virtual machines
- Entropy pools (http://bit.ly/41sIiN)
- Resource use (e.g. Bandwidth)

RESOURCE EXHAUSTION

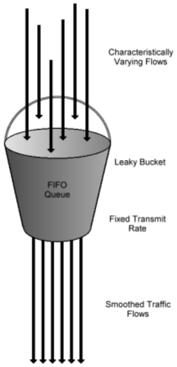
Overbooking



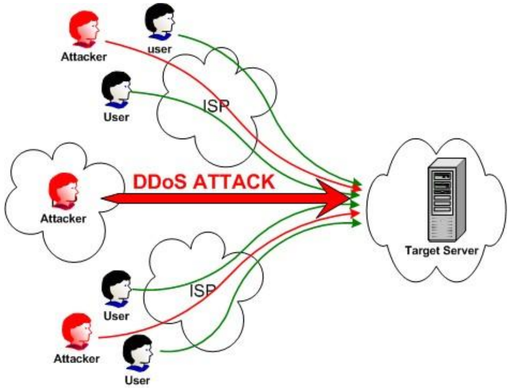
Underbooking

Caused by:

Resource allocation algos



Denial of Service



Freak events

Key management

- Key management is (currently) the responsibility of the cloud customer
- Key provisioning and storage is usually off-cloud
- One key-pair per machine – doesn’t scale to multiple account holders/RBAC
- Credential recovery sometimes available through management interface (protected by UN/PWD by)
- Copies of VM images may contain keys if not well-managed

Recommendations

Cloud Information Assurance Framework

Increasing transparency through a minimum baseline for:

- comparing cloud offers
- assessing the risk to go Cloud
- reducing audit burden for CP and security risks

Cloud Computing

Information Assurance Framework

November 09

Cloud Information Assurance Framework

An example

- **Network architecture controls**
- Well-defined controls are in place to mitigate DDoS (distributed denial–of-service) attacks e.g.
  - Defence in depth (traffic throttling, packet black-holing, etc..)
  - Defences are in place against ‘internal’ (originating from the cloud providers networks) attacks as well as external (originating from the Internet or customer networks) attacks.
- Measures are specified to isolate resource usage between accounts for virtual machines, physical machines, network, storage (e.g., storage area networks), management networks and management support systems, etc.
- The architecture supports continued operation from the cloud when the customer is separated from the service provider and vice versa (e.g., there is no critical dependency on the customer LDAP system).

Research recommendations

BUILDING TRUST IN THE CLOUD

- Certification processes and standards for clouds
- Return on security investments (ROSI) the measures cloud computing can enable to improve the accuracy of ROI for security;
- Techniques for increasing transparency while maintaining appropriate levels of security:
- Tagging, e.g., location tagging, data type tagging, policy tagging
- Privacy preserving data provenance systems, e.g., tracing data end-to-end through systems;
- End-to-end data confidentiality in the cloud and beyond:
    - Encrypted search (long term)
    - Encrypted processing schemes (long term)
    - Encryption and confidentiality tools for social applications in the cloud
- Higher assurance clouds, virtual private clouds, etc;

Research recommendations

DATA PROTECTION IN LARGE-SCALE CROSS-ORGANIZATIONAL SYSTEMS

- The following areas require further research with respect to cloud computing:
- Data destruction and lifecycle management
- Integrity verification - of backups and archives in the cloud and their version management
- Incident handling - monitoring and traceability
- Dispute resolution and rules of evidence
- International differences in relevant regulations, including data protection and privacy
    - Legal means to facilitate the smooth functioning of multi-national cloud infrastructures
    - Automated means to mitigate problems with different jurisdictions.
    - …..

Governments recommendations

- Public clouds are (usually) not suitable for critical government applications.
- Clearly define international differences in DP legislation.
- Should there be breach notification requirements on cloud providers.
- .....

Governments and the Cloud

UK

DK

...

- Gov Agencies and Public Organizations around the globe are moving non-critical applications towards a "cloud approach".

- In Europe we have some fast adopters, i.e. Denmark and UK, announcing/planning to move into the cloud.

Australia

USA

- In the short-medium term (1 to 3 years) an increasing number of Public Organizations, in EU Member States, will consider/adopt cloud computing.

Japan

Singapore

Agenda

- About ENISA
- Our position on Cloud computing
- Activities in Cloud computing
- Highlights of ENISA’s 2009 Cloud computing report
- **Ongoing and future work**

2010-11 – Security and resilience in Gov clouds: achieving an informed decision

Government towards the Cloud:
impact on service security & resilience

ENISA aims to:

- analyze and evaluate the impact of cloud computing on the resilience and security of GOV services.
- provide recommendations and good practices for European Members State planning to migrate to cloud computing

CAMM Common Assurance Maturity Model

MISSION

Provide an **objective** framework to **transparently** rate and benchmark the capability of a selected solution to deliver **information assurance maturity** across the **supply chain**

Contact us

Marnix Dekker – marnix.dekker@enisa.europa.eu

Daniele Catteddu - daniele.catteddu@enisa.europa.eu

Giles Hogben – giles.hogben@enisa.europa.eu

European Network and Information Security Agency

http://enisa.europa.eu