ENISA's role in enhancing Europe's Information Security Strategy and Capabilities

Udo Helmbrecht
Executive Director, ENISA

IFIP International Information Security and Privacy Conference
Crete, 4th June 2012
Agenda

• ENISA in the POLICY LANDSCAPE
• FUTURE RISK AND STRATEGIES
• SUPPORTING MEMBER STATES & EC
  • CLOUD COMPUTING
  • CERTs
  • EXERCISES
  • PRIVACY & TRUST
ENISA IN THE POLICY LANDSCAPE
ENISA

• Established in 2004

• Centre of Excellence: Writing reports that analyse data on security practices in Europe and on emerging risks (e.g. cloud computing, exercises, national contingency plans)

• Supporting the European Commission & Member States in their policy initiatives (e.g. setting up and training CERTs, seminars for national exercises)

• Facilitating cross-border cooperation (e.g. supporting cyber security exercises)

• Ensuring a coherent pan-European approach (e.g. supporting the implementation of article 13a)
# European Commission

<table>
<thead>
<tr>
<th>Commissioner</th>
<th>Directorate-General</th>
<th>European Union Agencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neelie Kroes</td>
<td>Information Society and Media (DG CONNECT)</td>
<td>ENISA</td>
</tr>
<tr>
<td>Cecilia Malmström</td>
<td>Home (DG HOME)</td>
<td>FRONTEX, EUROPOL, CEPOL, EMCDDA, EASO</td>
</tr>
<tr>
<td>Viviane Reding</td>
<td>Justice (DG JUST)</td>
<td>EUROJUST, FRA (Fundamental Rights)</td>
</tr>
<tr>
<td>Maroš Šefčovič</td>
<td>Inter-Institutional Relations and Administration</td>
<td>Informatics (DG DIGIT)</td>
</tr>
</tbody>
</table>

**European Union Agencies**

- ENISA
- FRONTEX
- EUROPOL
- CEPOL
- EMCDDA
- EASO
- EUROJUST
- FRA (Fundamental Rights)
European Strategy for Internet Security

- fostering close co-operation and early warning between MS’ competent authorities and private sector
- ensuring adequate capacities and structures for prevention, detection, mitigation and response at national and EU level
- stimulating efforts to improve security of products, networks and services
- ensuring a strong EU response to cybercrime
- supporting R&D investments and strengthen the competitiveness of EU’s security industry
- reinforcing cooperation with international partners
FUTURE RISKS AND STRATEGIES
Development of attacks

- Computer virus
- Phishing
- Spying
- Botnet
- Attacks on CIIP
- Attacks on Cloud Services

Effectiveness of malware

Time

Today
New virtual world (I)

- No national borders
- No uniform legal system
- Divergent approaches
  - personal data protection vs. data retention
- Difference of perception across countries/regions
  - i.e. privacy as human right in EU or consumer right in US
- Not a level playing field for EU online service providers
- Policy framework re-active instead of proactive
New virtual world (II)

• A new currency: personal data
• Contradictory expectations and practice
  • Privacy - fundamental human right in the EU
  • Users concerned about privacy
    • 93% of participants in recent ENISA study
  • Users willing to disclose more personal data for discounts
    • up to 87% of participants, in some cases, for 0.5 € discount in the study

• New business value chains
  • What is a fair price of a user’s profile?
  • How this price may vary if considered as part of a group (‘bargaining power of individual‘)?
  • What is the effect on consumers & competition?

SUPPORTING MEMBER STATES & EC
Supporting Member States

Cyber-security topics

Council, EP, Commission

CERT

CERT

CERT RO

CIIP

Data Breaches Notification
Cloud computing

- Content of Service Level Agreement (SLA).
- How continuous monitoring is implemented.
- Many customers do not monitor security measures continuously.
- security parameters are less well covered.

2009: Risk analysis
2009: Assurance framework
2011: Security and resilience in governmental clouds
2011: Security parameters in cloud SLAs

ENISA supporting CERTs

• Support MS in establishing and developing CERTs to a baseline set of capabilities.
• Providing good practice in cooperation with CERTs.
• Analyse barriers for cross-border cooperation.
• Support cooperation between CERTs and crucial stakeholders.
Cyber Atlantic 2011

• Announced in April during the Hungary Ministerial Conference
• Table top, centralised, discussion based
• Exploratory nature, how do we engage each other

20 MS involved, 17 actively playing, 100 experts with the support of ENISA and US DHS

Delivered on 03.11.2011, Brussels

Neelie Kroes, European Commission
Janet Napolitan
US Department of Homeland Security
Key Findings - Cyber Atlantic 2011

- exercises need to test holistically technical, law enforcement, policy/political aspects
- modern communication and conferencing facilities are needed for crisis cooperation of large groups
- exchange SOPs, trainings, and exercises among EU and US
“Everyone has the right to the protection of personal data concerning them”.

**EU legislation reform**

- **Data Protection**
  - The directive (1995) to be replaced
  - the new regulation for data protection
    - Personal data protection by design and by default
    - Right to be forgotten
    - sanctions

- **Data retention reform**

- **Technologies perspective**

- **Consumers/users perspective**
Privacy and data protection activities at ENISA since 2010

★ Activities since 2010
★ Data Breach Notification in Europe
★ Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments
★ Privacy, Accountability and Trust – Challenges and Opportunities
★ Bittersweet cookies. Some security and privacy considerations

★ Activities 2011
★ Study on the use of cryptographic techniques in Europe
★ Report on trust and reputation models
★ Study on monetising privacy. An economic model for pricing personal information
★ Study on data collection and storage in the EU
★ Technological guidelines for implementation of Art. 4
  • All available at: http://www.enisa.europa.eu/act/it/library

★ On-going activities 2012
★ Art.4, privacy seals, Annual Privacy Forum, etc.

http://www.enisa.europa.eu/act/it/library
Privacy related activities - some findings

★ Findings, challenges, issues
  ★ Applicable legislation
  ★ Conflicting legislation
  ★ Conflicting behaviour
  ★ Likability and profiling in practice
    • 27 MS perspective and global reality of Internet

★ Topics for consideration
  ★ Profiling and tracking, period of storage, right to be forgotten
    • Data should not be stored forever
    • Data minimization
  ★ Personal data as a commercial asset; transfer of personal data between providers and outside EU
  ★ Solutions brought by the proposed reform of data protection in the EU
Study on the use of cryptographic techniques in Europe

- Focus on how personal data is protected
  - in eGov services deployed in MS

- Findings & recommendations
  - Good recommendations/specifications
    - Sometimes poorly deployed
    - Lack of coordination
  - Best practice needs to be promoted
  - Clear guidelines / policies need to be developed
  - EU-wide initiative needed
    - to specify a common minimum standard for cryptography of unclassified data in e-government services
Study on data collection and storage in the EU

★ Case studies covering all 27 MS
  ★ Social networking
  ★ Transportation sector
  ★ Telecommunications sector
    • analysis on deployment of
      – the principle of minimal disclosure and
      – the minimum duration of the storage of personal data

★ Findings and recommendations
  ★ MS should identify and eliminate conflicting regulatory provisions relating to the collection and storage of personal data
  ★ Data Protection Authorities should provide clear guidelines to data controllers at national and pan-European level
Report on trust and reputation models

★ Identified risks
  • exposing personal data, the linking of user identities across multiple sites
  • facilitating the targeting of advertising, risking price discrimination
  • website providers sharing the reputation data
  • the level of trust placed in the reputation score exceeding the level of trustworthiness of the reputation model

★ Recommendations covering
  • Mitigating security risks posed by reputation systems, trustworthiness of reputation scores, consumer communications, applicable legislation, linkability
Study on monetising privacy. An economic model for pricing personal information (I)

★ Questions

• Do some people pay a premium for privacy?
• What is the effect on consumers & competition?
• Does product personalization lead to lock-in?
• Does it pay for firms to differentiate along the privacy concern of individuals?

★ Model developed and experiments during 2011

• Lab experiment, 440+ participants ; field experiment and hybrid experiment
  – the largest laboratory experiment in the field of privacy economics to date
  – 2,300+ participants with 139 transactions and observations in the field & hybrid experiments
Study on monetising privacy. An economic model for pricing personal information (II)

★ Findings
• Privacy-friendly firms get a greater share of market if no price differentiation
• Privacy-unfriendly firms obtain greater share market if they practice lower prices, but privacy friendly firms stay above 10%

★ Recommendations
• users should be provided with options that allow them to disclose less personal data
• easy-to-understand comparison of the data protection practices is needed
• portability of profiles for consumers required to reduce lock-in
Data Breach Notifications – technological guidelines (I)

★ Target
  ★ Competent authorities (DPAs and others)
  ★ Telecom operators (and other sectors players)

★ Objectives
  ★ Practical and usable definition of a breach
  ★ Criteria for determining a breach
  ★ National and pan-European approaches
  ★ Appropriate technological protection measures
  ★ Identification and assessment of risks of breaches
  ★ Procedures of notification
Data Breach Notifications (II)

★ Review of ePrivacy Directive (2002/58/EC), Art.4
★ ENISA activities in 2011
  ★ Consultation workshop on DBN (24th January)
  ★ Technological guidelines for implementation of Art. 4
★ ENISA activities in 2012
  ★ Establish ‘formal’ exchange/collaboration with Art29 TS
  ★ Pilot in some MS
New activities. Data security in data retention reform

★ Context

★ Assistance to MS and EU institution
  • DG Home request on
    – Data security in Data retention reform

★ Scope, objectives

★ Comment on draft documents

★ Provide recommendations regarding data security

★ Identify best practice in 3-5 MS
  • With help from external experts, lessons from other areas

★ Data retention in the context of the new data protection regulation
  • Good protection of personal data
  • minimum security requirements across MS
Organisers
- ENISA, DG INFSO and University of Cyprus

Program Committee chair
- Bart Preneel, KU Leuven

Call for papers
- submission 25th of June; notification 11th of August
- www.privacyforum.eu
Conclusions

• Identification of risks associated with new technologies affecting the daily life of citizens
• Cyber crisis cooperation at EU and international level and development of capabilities
• Facilitating Public-Private cooperation
• Improving transparency of security incidents
• Enabling communities to improve NIS: capacity building with regard to the CERT community and application of good practice for CERTs
• Ensuring a strong EU response to cybercrime
• Stimulating R&D investments and strengthen the competitiveness of EU’s security industry
• Promote personal data protection
Contact

European Network and Information Security Agency
Science and Technology Park of Crete
P.O. Box 1309
71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu