European Data Protection Supervisor

IT security incidents and the role of the DPO

Achim Klabunde

DPO Meeting@CEDEFOP

07.11.2014

IT Security in Regulation 45/2001

- Regulation 45/2001 Article 22 concerns the security of processing.
  - Other articles such as Article 21 (confidentiality of processing), Article 35 (Security in the context of telecoms networks) or Article 36 (confidentiality of communications) are also relevant
- The most important part of Article 22 lays in 22.1 and 22.2
  - In 22.1: “ensure a level of security appropriate to the risks”
  - In 22.2: “measures shall be taken as appropriate in view of the risks”

Practical requirements

- The need for measures, or security controls, has to be analysed in light of the risks to the organisation.
- this analysis should give an organisation a clearer view on what it should implement to reduce risks to a level acceptable
- This implies several things:
  - A risk management process is defined and implemented within the organisation.
  - The selection of security controls is part of this risk management process.
  - As risks change, so will the security controls necessary to mitigate those risks. This is a continuous process that requires constant attention of IT developments.

Risk management

- Risk management process and security controls is a demanding task in terms of resources and expertise
- strengthen your relationship with your Local Information Security Officer (LISO) or similar function,
- the security incident management process. When an issue occurs on an IT system and affect security, an organisation should have in place a process to deal with security implications of the issue (LISO would typically be involved as well).
- As security incidents may affect personal data, it would be interesting for DPOs to be informed when personal data is indeed affected.
- For example: how many of you have been informed about the Heartbleed bug?

Heartbleed

- The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library and was discovered in April 2014. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).
- The world was affected by this bug; EU institutions included. CERT-EU pushed information to the institutions with instructions on how to assess and fix the issue on the 10/04/2014 and with details on the 23/04/2014.
- We would suggest that you check in your organisation the steps taken to assess the potential issues created by the Heartbleed bug and the steps implemented to mitigate the risks.
- Other famous incidents this year:
  - GOTOFAIL
  - SHELLSHOCK
  - POODLE

Timeline

- **February 2014: Gotofail**
- **April 2014: Heartbleed**
- **September 2014: Shellshock**
- **October 2014: POODLE**
- **Is climate change increasing the frequency of hazardous events?**

Thank you for your attention!

=> Q&A <=

For more information:

www.edps.europa.eu

edps@edps.europa.eu

@EU_EDPS