EUNIS INFORMATION SECURITY

Outcomes of the EUNIS Workshop on Information Security

27-28 January 2020, University of Malaga.

In two half days around 25 information security experts presented and exchanged experiences. They discussed topics as varied as the dangers of unencrypted email traffic (POP3, IMAP, SMTP), the disastrous impact of Emotet attacks, and the lack of awareness among users. Below you’ll find an overview of the outcomes.

Conclusions re security policy and measures

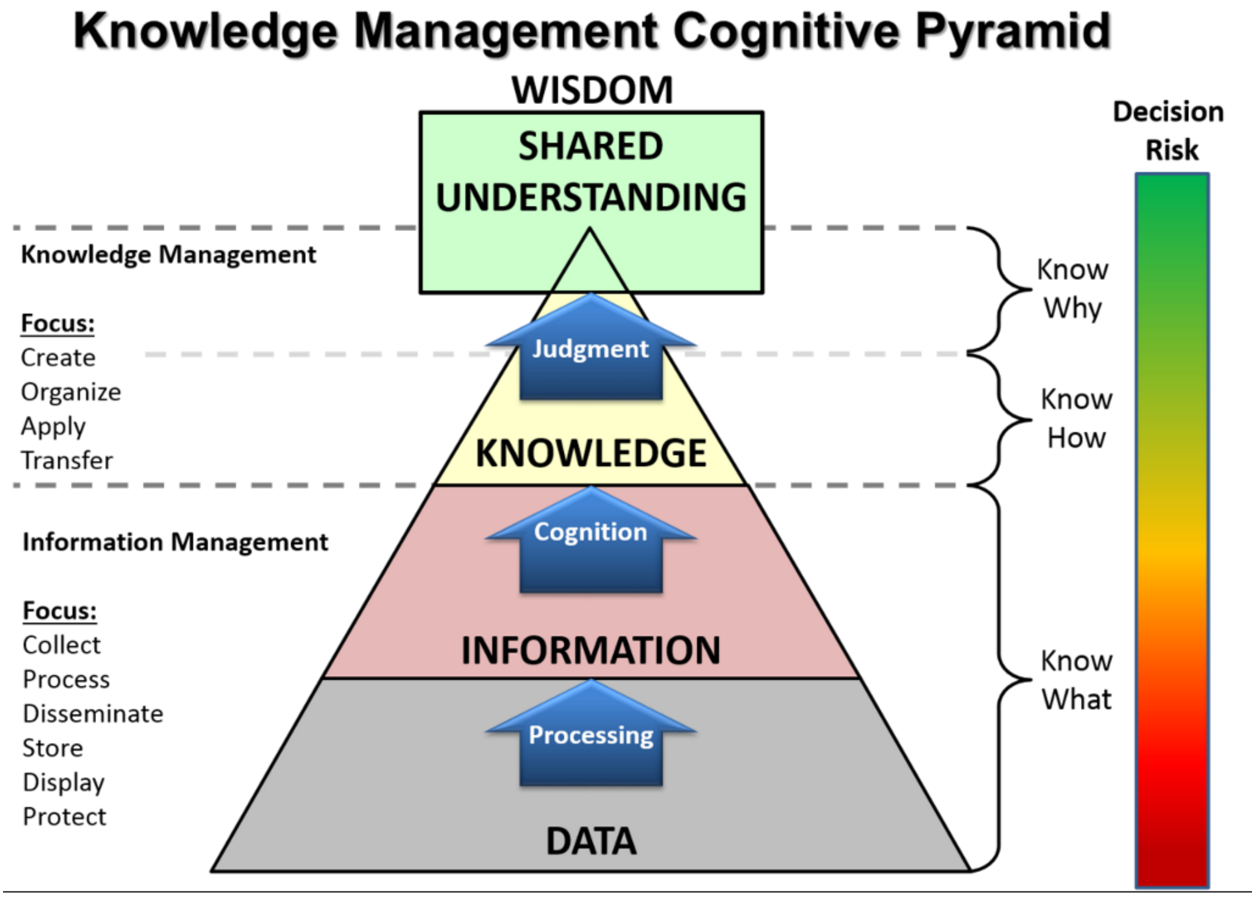
- Risk management is crucial to mitigate emerging conflicts between freedom of research and it security; between research personnel and espionage; between international cooperation and cybersecurity
- Clearer mandatory policies and guidelines needed and monitored. This requires update of the law, top management directives, increase of information security officers at universities, audits and awareness guidelines. IT security being “autocratic” can be justified if it offers convincing benefits.
- A solid ISMS is crucial and implementation has clear phases: mapping of systems, services and work processes; valuations and classification of information; Business Impact Analysis (BIA); Risk Assessment and measures management; Continuity planning (DRP + ISCP). Essential: a dependencies overview for services and linkage between information security and data protection.

Conclusions re governance, emergency training and GDPR

- Strategy of information security should be developed in dialogue between HEIs and ministry, setting priorities and clear goals.
- Invest in staff training as more personnel capacity is required, more expertise is needed in HEIs and at ministries. Currently guidelines are often not known, spreading information over all departments is difficult and IT solutions are duplicated.
- Emergency plans and procedures are required, as well as training how to act. There is potential for easy access to emergency procedures, using Apps and online learning content, gamification
- GDPR compliance helps: one rule for everybody, big private tech companies and public organisations, you have the choice to give consent using your data (that you can withdraw at any time), otherwise you have to get a legal obligation
- Problem with Learning/Campus Management Systems is that they are not based on consent but on legal obligation. This needs to be addressed in the statutes of public institutions

Insightful discussion on the DIKW Pyramid

The DIKW pyramid refers loosely to a class of models for representing purported structural and/or functional relationships between data, information, knowledge, and wisdom. "Typically information is defined in terms of data, knowledge in terms of information, and wisdom in terms of knowledge". https://en.wikipedia.org/wiki/DIKW_pyramid



Presentations and demonstrations on various vulnerabilities and responses

- Development of CERT/CSIRTs since 1989 to today enabled networking through FIRST, TF-CSIRT etc. Various information and services are offered by the Open CSIRT Foundation (OCF), including training of SIM3 auditors. Latest offering is the Security Incident Management Maturity Model (SIM3) and its new online tool. http://opencsirt.org/csirt-maturity/sim3-online-tool/
- How vulnerability management at the University of Münster is organized and implemented with OpenVAS at University of Münster. Which prerequisites are required? What are the results
- The IT security related services (CERT) services offered by DFN-CERT (the computer emergency response team of German NREN DFN) to German HEIs, such as DFN-CERT Portal and DFN-PKI
- Live hacking demonstrations that show how easily a hacker can compromise a PC when having physical access to it. Devices shown: hardware keylogger, USB rubber ducky, Bash Bunny, LAN Turtle. CrazyRadio PA USB dongle
- Demo of an automated checking mechanism to determine if a service is ready to go operational, checking on risk assessment, data processing agreement, penetration tests, et cetera. The API will be in production by January 2020.

If you are interested in more information please join the EUNIS Information Security Special Interest Group e-mailing at: thorsten.kuefer@eunis.org or asbjorn.thorsen@eunis.org.