Karlsruhe Institute of Technology

SEVEN THESES ON IT SECURITY

Competence Center for Applied Security Technology

PRIVACY PROMOTES SECURITY

It's no surprise to anyone that countries hide their military bases on Google Maps, or that you can't film or photograph in security areas at airports. Equally the protection of certain information is important for private individuals. Thieves are interested in whether or not I am on vacation, others are interested in how I can be blackmailed. That's why our IT infrastructure must allow everyone to set the limits of their own privacy in a meaningful way.

DATA THAT IS STORED MUST ALSO BE PRO-TECTED

Whether it's a data center or a smartphone, anyone who stores data assumes responsibility – especially if it's data from third parties. It should always be clear how each stored data set is protected against unwanted access. The loss of mobile devices must also be taken into account.

SECURITY INCIDENTS MUST BE REPORTED

Every company expects its employees to report lost building keys. Likewise, service providers must be obliged to inform customers about unauthorized access to their data. After all, customers assume that their password or credit card details are confidential. It may even be necessary to inform the public, if, after a break-in, generally accepted security assumptions are no longer correct. This also applies if no customer data is affected.

SECURITY MUST BE COMPREHENSIBLE

Experts need to understand the security of a system based on a published security concept. To this end, the desired security features and the measures to achieve them must be clearly identifiable. Ideally, standard solutions are used for the implementation of a security concept.

A DATA PROTECTION SEAL FOR SOFTWARE

A manufacturer who affixes the CE marking on his products declares conformity with certain standards. Such conformity marks must also exist for software products. The requirements for these marks, in particular those concerning the security of the processed data, must be formulated in a binding manner and adhered to by the software manufacturer. These requirements must include data economy, encrypted storage of confidential information and the use of encrypted communication channels.

E-MAILS MUST BE END-TO-END ENCRYPTED AND SIGNED

Secure e-mail communication means that a message can only be read by the recipient and is signed by the sender. It must be signed and encrypted before it is sent and may only be decrypted by the authorized recipient. This is the only way to ensure that confidential communication can't be tapped during transmission. E-mails that are stored in the clear may be stolen.

GOOD SECURITY MEASURES ARE EASY TO USE

It is paramount that IT security solutions are easy to use. If a security solution is too cumbersome, it won't be used. For example, most of the tools for secure e-mail communication are too complicated for laymen. We consider it as the authorities' duty to support citizens and companies in their "digital self-defense".

Oh, by the way, …

… you have the right to obtain information from companies regarding the personal data stored about you (Sec. 15 DS-GVO).

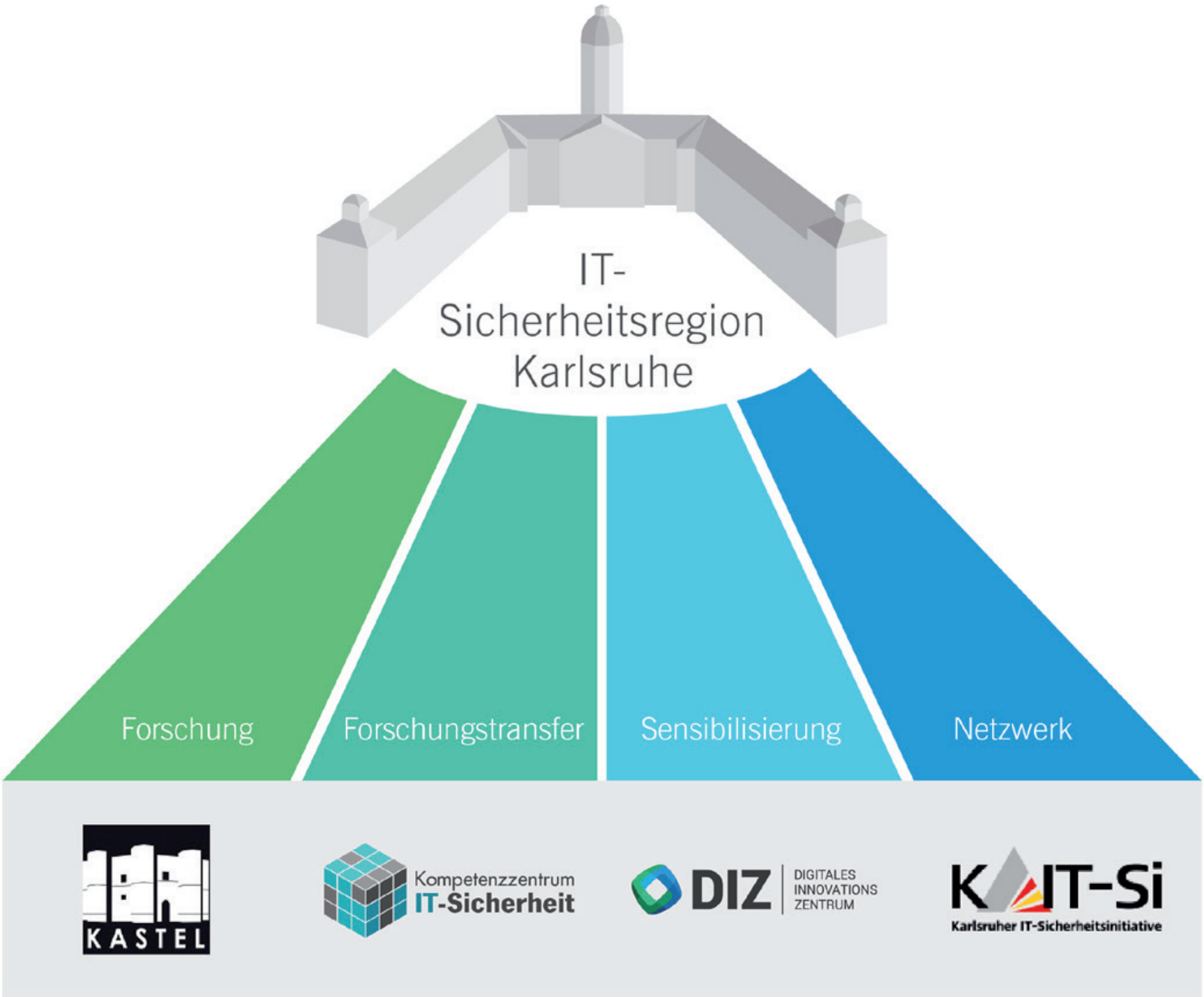
… there already is a legal obligation to minimize data (Sec. 5 par. 1c) DS-GVO).

… HTTPS protects against neighbors, not against neighboring countries.

… the BSI not only provides recommendations for manufacturers of IT systems (basic IT protection), but also advises citizens (www.bsi-fuer-buerger.de).

… a good password is easy to remember and hard to guess.

… there already is an obligation to report data protection incidents if certain personal data is affected (sec. 33 and 34 DS-GVO).


IT-
Sicherheitsregion
Karlsruhe
Forschung
Forschungstransfer
Sensibilisierung
Netzwerk
KASTEL
Kompetenzzentrum
IT-Sicherheit
DIZ
DIGITALES
INNOVATIONS
ZENTRUM
KA IT-Si
Karlsruher IT-Sicherheitsinitiative

KASTEL

The Competence Center for Applied Security Technology (KASTEL) is a merger of the major players in academic IT security research in Karlsruhe: The Karlsruhe Institute of Technology (KIT), the Fraunhofer IOSB and the FZI Research Center for Computer Science.

Twelve research groups from the fields of computer science, economics and law cooperate in KASTEL and develop a holistic approach that integrates the competencies and methods of various disciplines.

Further information on www.kastel.kit.edu

Publisher

Karlsruhe Institute of Technology (KIT)

Kaiserstraße 12

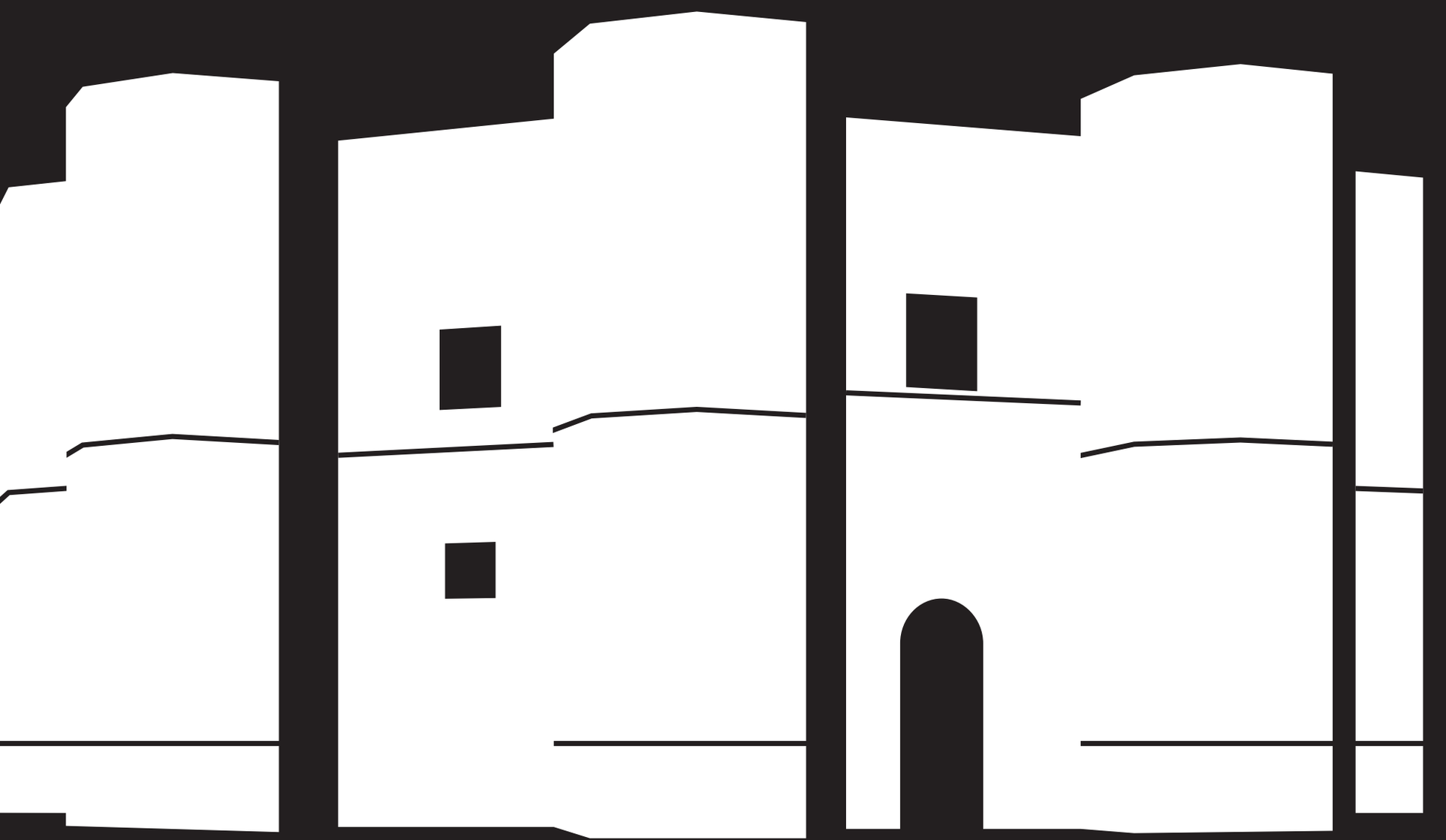
76131 Karlsruhe

Web: kit.edu

Cover picture: wikimedia.org, Niccolò Rigacci

SPONSORED BY THE

Federal Ministry
of Education
and Research



KASTEL