Karlsruher Institut für Technologie

SIEBEN THESEN ZUR IT-SICHERHEIT

Kompetenzzentrum für angewandte Sicherheitstechnologie

SICHERE E-MAIL IST VON ENDE ZU ENDE VERSCHLÜSSELT

Sichere E-Mail-Kommunikation bedeutet, dass die Nachricht nur vom Empfänger gelesen werden kann und vom Absender signiert ist. Sie muss signiert und verschlüsselt werden, bevor sie versendet wird und darf erst vom berechtigten Empfänger wieder entschlüsselt werden können. Nur so wird sichergestellt, dass vertrauliche Kommunikation nicht unterwegs abgehört werden kann. Wird E-Mail unverschlüsselt gespeichert, ist sie dort einem Diebstahlrisiko ausgesetzt.

GUTE SICHERHEITS-MASSNAHMEN SIND EINFACH HANDHABBAR

Die einfache Benutzbarkeit von IT-Sicherheitslösungen darf nie vergessen werden. Ist eine Sicherheitslösung zu umständlich, wird sie nicht benutzt. Beispielsweise sind die meisten Werkzeuge für die sichere E-Mail-Kommunkation für Laien zu kompliziert zu bedienen. Wir sehen die Behörden in der Pflicht, Bürger und Firmen bei ihrer „digitalen Selbstverteidigung" zu unterstützen.

CE-KENNZEICHNUNGS-PFLICHT. AUCH FÜR SOFTWARE!

Hersteller von Elektronikgeräten verpflichten sich mit dem CE-Siegel, nur Produkte zu verkaufen, die gewissen Standards genügen. Ebenso muss es solche Verpflichtungen auch für Software geben. Die Ansprüche, insbesondere auch an die Sicherheit der verarbeiteten Daten, müssen verbindlich formuliert und von den Softwareherstellern eingehalten werden. Die Anforderungen müssen Datensparsamkeit, verschlüsselte Speicherung vertraulicher Informationen und die Verwendung verschlüsselter Kommunikationskanäle enthalten.

SICHERHEITSVORFÄLLE MÜSSEN MELDEPFLICHTIG SEIN

Jedes Unternehmen erwartet von seinen Angestellten, dass sie verlorene Gebäudeschlüssel melden. Umgekehrt müssen Dienstanbieter verpflichtet sein, Kunden über unbefugten Zugriff auf ihre Daten zu informieren; schließlich nehmen diese an, dass ihr Passwort oder ihre Kreditkartendaten geheim sind. Gegebenenfalls muss sogar die Öffentlichkeit darüber informiert werden, wenn nach einem Einbruch allgemein anerkannte Sicherheitsannahmen nicht mehr gelten – dies gilt auch dann, wenn keine Kundendaten betroffen sind.

SICHERHEIT MUSS NACHVOLLZIEHBAR SEIN

Fachleute müssen die Sicherheit eines Systems anhand eines veröffentlichten Sicherheitskonzepts nachvollziehen können. Dafür müssen die gewünschten Sicherheitseigenschaften und die Maßnahmen, mit denen sie erreicht werden, klar erkennbar sein. Optimalerweise werden für die Umsetzung des Konzepts Standardlösungen verwendet.

DATEN, DIE MAN VORHÄLT, MUSS MAN AUCH SCHÜTZEN

Ob Rechenzentrum oder Smartphone – wer Daten speichert, übernimmt Verantwortung; insbesondere, wenn es sich um die Daten von Dritten handelt. Stets sollte für jeden gespeicherten Datensatz klar sein, wie er vor unerwünschtem Zugriff geschützt ist. Der Verlust von mobilen Geräten muss dabei auch beachtet werden.

PRIVATSPHÄRE FÖRDERT SICHERHEIT

Für niemanden ist es überraschend, dass die USA ihre Militärstützpunkte auf Google-Maps ausblenden lassen oder dass man in Sicherheitsbereichen an Flughäfen nicht filmen oder fotografieren darf. Ebenso ist für Privatpersonen der Schutz gewisser Informationen wichtig. Diebe interessieren sich dafür, ob ich gerade im Urlaub bin; andere dafür, wie ich erpressbar bin. Daher muss es unsere IT-Infrastruktur jedem ermöglichen, die Grenzen seiner Privatsphäre selbst und sinnvoll zu setzen.

Ach übrigens, …

… gegenüber Unternehmen mit Sitz in Deutschland haben Sie bereits ein Recht auf Auskunft, welche Daten über Sie vorgehalten werden (BDSG § 34).

… im deutschen Recht gibt es bereits die Verpflichtung zur Datensparsamkeit (BDSG § 3a).

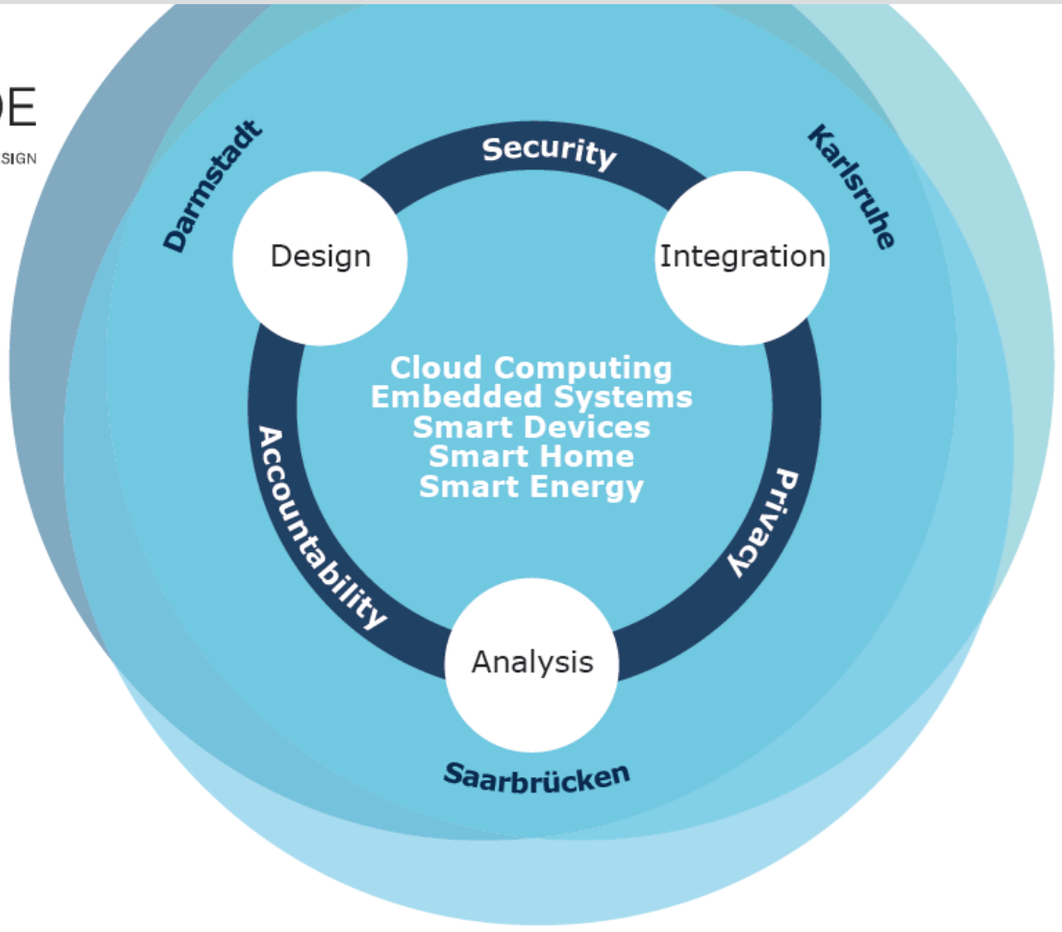
… HTTPS schützt vor dem Nachbarn, nicht vor Nachbarstaaten.

… das BSI erstellt nicht nur Empfehlungen für Hersteller von IT-Systemen (IT-Grundschutz), sondern berät auch Bürger (www.bsi-fuer-buerger.de).

… ein gutes Passwort ist leicht zu merken und schwer zu raten.

… eine Meldepflicht bei Datenschutzvorfällen besteht bereits, wenn bestimmte personenbezogene Daten betroffen sind (BDSG § 42a).

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN



KASTEL

CISPA
Prof. Dr. Michael Backes

EC SPRIDE
Prof. Dr. Michael Waidner

KASTEL
Prof. Dr. Jörn Müller-Quade

CISPA
Center for IT-Security, Privacy and Accountability

SPONSORED BY THE
Federal Ministry of Education and Research

Competence Centers for IT Security

Das BMBF fördert insgesamt drei Kompetenzzentren für Cybersicherheit. Die Schwesterzentren von KASTEL sind das Center for IT-Security, Privacy and Accountability (CISPA) in Saarbrücken und das European Center for Security and Privacy by Design (EC SPRIDE) in Darmstadt.

KASTEL

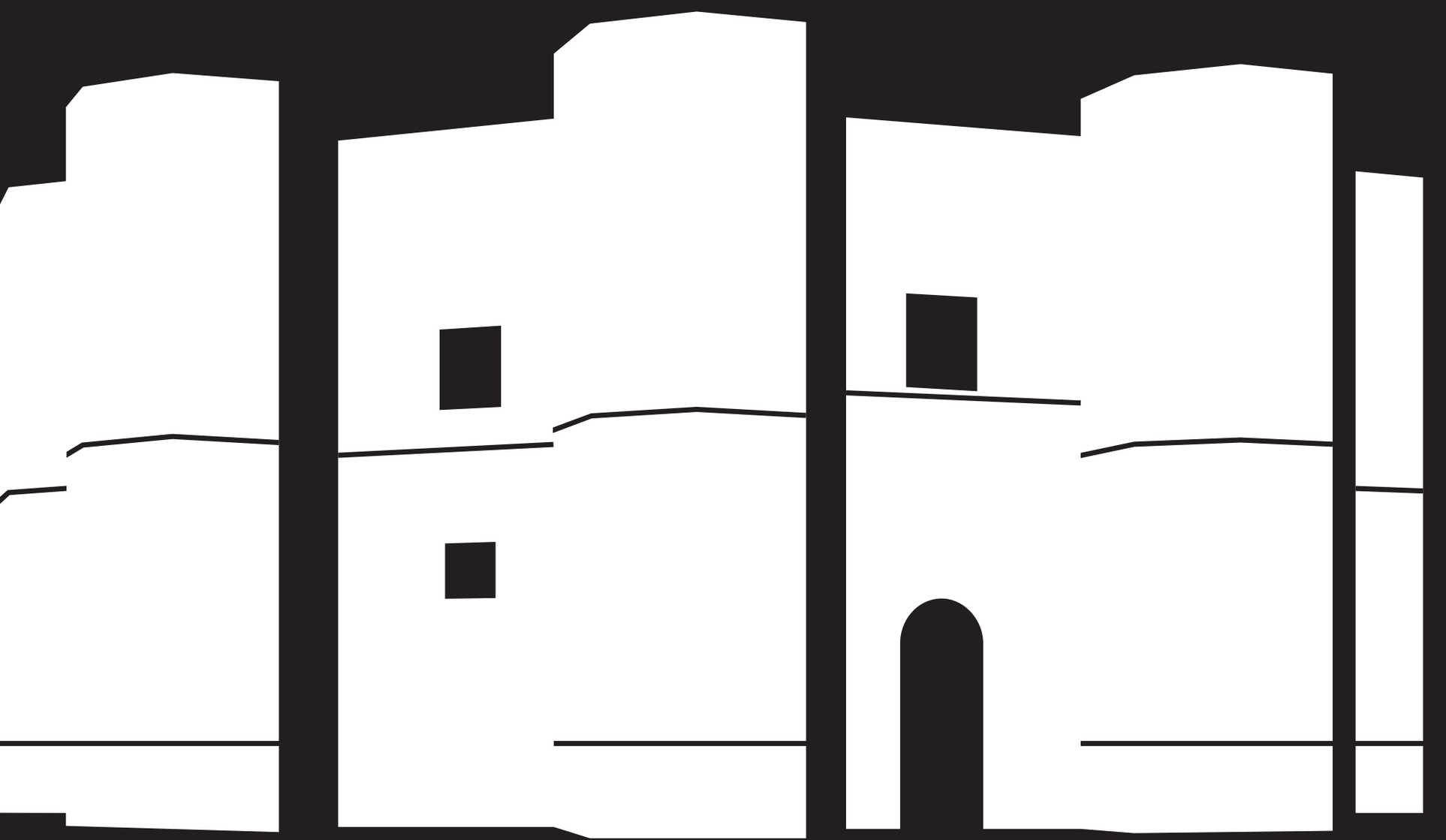
Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Kompetenzzentrum für angewandte Sicherheitstechnologie KASTEL ist am Karlsruher Institut für Technologie (KIT) angesiedelt. In KASTEL kooperieren zehn Lehrstühle aus den Fachbereichen Informatik, Wirtschaftswissenschaften und Rechtswissenschaften mit dem gemeinsamen Ziel, in einem durchgängigen Prozess sichere Anwendungen zu entwickeln.

Weitere Informationen auf www.kastel.kit.edu

KIT - Campus Süd
Institut für Kryptographie und Sicherheit,
Am Fasanengarten 5
76131 Karlsruhe
Tel.: +49 721 60855022
E-Mail: info@iks.kit.edu
Web: www.iks.kit.edu

Herausgeber
Karlsruher Institut für Technologie (KIT)
Kaiserstraße 12
76131 Karlsruhe
Web: kit.edu

Titelbild: wikimedia.org, Niccolò Rigacci



KASTEL