bunden mit einer soliden wissenschaftlichen Ausbildung. Ab August 2014 können sich Studieninteressierte einschreiben.

Ab dem kommenden Wintersemester bietet die Fachrichtung Informatik der Universität des Saarlandes für Abiturienten den auf sechs Semester angelegten Bachelor-Studiengang „Cybersicherheit" an. Vom ersten Vorlesungstag an beschäftigen sich die Studenten mit Cybersicherheit, sind Angreifer, Verteidiger und Forscher in einer Person. Sie lernen, wie man Smartphones gegen Spionage-Apps wappnet, Computernetzwerke gegen Angriffe aus aller Welt schützt. Um ein noch besserer Verteidiger zu werden, erforschen sie auch Angriffe. Sie versuchen dabei, den Ganoven auf die Schliche zu kommen, die Passwörter knacken und in Datenbanken eindringen.

Weitere Informationen: *http://cybersicherheit.uni-saarland.de*

BlackBerry übernimmt Secusmart

Secusmart und der Smartphone-Pionier BlackBerry Ltd. informierten am 29.07.2014 über die Übernahme von Secusmart durch BlackBerry Ltd. Secusmart bleibt als GmbH in Deutschland erhalten. Durch das Zusammengehen erhält Secusmart Zugang zum globalen Markt für sichere mobile Kommunikation und wird zukünftig von dem weltweiten Vertriebs- und Support-Team der BlackBerry „Security Unit" profitieren. Der Abschluss der Transaktion wird, vorbehaltlich der notwendigen regulatorischen Genehmigungen, erwartet.

Dr. Hans-Christoph Quelle, CEO Secusmart GmbH: „Als Abhörschutzunternehmen haben wir durch diesen strategischen Schritt ganz neue Möglichkeiten „Security made in Germany" weltweit Behörden, Mobilfunkbetreibern und Unternehmen anzubieten. Die Geheimnisse unserer bestehenden und zukünftigen Kunden bleiben auch weiterhin zuverlässig geschützt: Herzstück der Secusmart-Technologie ist und bleibt ein Krypto-Chip, integriert in eine handelsübliche Micro-SD Karte. Ende zu Ende Verschlüsselung ist das einzige Mittel, um die Sprach- und Datenkommunikation vor Spionage Dritter zu schützen. Wie auch in der Vergangenheit hat kein Secusmart-Mitarbeiter Zugriff auf die Verschlüsselungsalgorithmen oder die Geheimnisse unserer Kunden."

Ausbau des sicheren intelligenten Energienetzes stagniert

Die Smartmeter-Regulierungsprojekte der Bundesregierung werden bislang nicht zügig zum Abschluss geführt. Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) kritisierte am 21.07.2014 die Verzögerungen und fordert die politisch Verantwortlichen jetzt zum Handeln auf.

Die Energiewende ist in aller Munde und beherrscht die Schlagzeilen. Rund 20% der in Deutschland erzeugten Elektrizität wird mittlerweile aus erneuerbaren Ressourcen gewonnen. Wesentliche Grundlage der Energiewende ist die dezentrale Erzeugung und Verteilung von Elektrizität, die umfangreiche Maßnahmen zur intelligenten Steuerung erfordert. Eine der dafür notwendigen intelligenten Komponenten sind Smartmeter, die intelligenten digitalen Stromzähler, die u.a. auch dynamische Tarife ermöglichen. Um eine Integration bzw. Steuerung in intelligenten Energienetzen abzusichern, ist anspruchsvolle IT-Sicherheit nötig. Das haben auch alle Beteiligten erkannt – aber bei der zeitnahen Umsetzung hapert es.

Seit ca. 3 Jahren werden die Mindestsicherheitsanforderungen für Smartmeter-Infrastrukturen in Deutschland standardisiert. Ein Abschluss sollte gemäß Koalitionsvertrag Mitte 2014 in Sicht sein. Dies wurde jedoch nicht realisiert, obwohl das zugehörige Gesetz bereits mit der Novellierung 2008[1] verabschiedet wurde. Das Bundesministerium für Wirtschaft und Energie hat bisher keine verbindlichen Standards veröffentlicht bzw. diese in die Gesetzgebung eingebracht.

Auch eine Adaption der bisher noch nicht verabschiedeten Sicherheitsstandards auf andere Komponenten im künftigen Energienetz, wie beispielsweise intelligente Ortsnetzstationen oder Energie-Managementsysteme, fehlt. Verbindliche Normen zur Absicherung des intelligenten Energienetzes gibt es daher nicht. Dies behindert und verzögert den raschen Aufbau der für die Energiewende benötigten sicheren kritischen Infrastruktur.

Ein erhebliches Risiko besteht, wenn die bisher verbauten und teilweise unsicheren Komponenten weiter in Deutschland zum Ausbau des intelligenten Energienetzes eingesetzt werden. Hackern wird dadurch die Chance eröffnet, die Energieversorgung und damit große Bereiche der Wirtschaft und des öffentlichen Lebens mit einem „Klick" nachhaltig stören zu können.

Es ist nun schnelles Handeln aller Verantwortlichen notwendig, um die Versorgungssicherheit der deutschen Bevölkerung und der Industrie mit Elektrizität weiterhin zu gewährleisten.

BMWi und BMBF: Forschungsinitiative ‚Zukunftsfähige Stromnetze'

Das Bundesministerium für Wirtschaft und Energie (BMWI) und das Bundesministerium für Bildung und Forschung (BMBF) haben am 06.08.2014 den Startschuss für die Forschungsinitiative „Zukunftsfähige Stromnetze" gegeben. Insgesamt sind 83 Vorhaben mit einem Gesamtfördervolumen von etwa 157 Millionen Euro für eine Förderung durch die beiden Ministerien ausgewählt worden.

Angesichts der Herausforderungen der Energiewendedürfen Erzeugung, Netz und Transport sowie Verbrauch nicht isoliert betrachtet werden. Es ist eine ganzheitliche Betrachtung notwendig:

- Neue Leitungen: Nur mit neuen Leitungen kann die Distanz zwischen Erzeugungsschwerpunkten und Verbrauchszentren überbrückt werden. Deswegen wurden das Energieleitungsausbaugesetz (EnLAG) und das Netzausbaubeschleunigungsgesetz (NABEG) auf den Weg gebracht, mit denen der Bau von Leitungen mit dringendem Ausbaubedarf beschleunigt werden soll.
- Neue Technologien: Die Erprobung von Erdkabeln und der Einsatz von Hochspannungsgleichstromübertragung (HGÜ) soll dort möglich sein, wo es technisch sinnvoll und wirtschaftlich effizient ist. Außerdem muss die Forschung als Grundlage für die Erschließung technologischer Potenziale gestärkt werden (6. Energieforschungsprogramm der Bundesregierung).
- „Smart Grids": Netze, Erzeugung und Last müssen effizient und intelligent miteinander verknüpft werden.

Alle Beteiligten müssen an einem Strang ziehen – Netzbetreiber, die Planungs- und Genehmigungsbehörden vor Ort und Bürgeri-

1 „Erneuerbare-Energien-Gesetz vom 25. Oktober 2008 (BGBl. I S. 2074)