Erfolgreiche Premiere: Die ersten Thementage „IT-Sicherheit und Datenschutz in der Forschung“ an der Universität Konstanz

24. - 25. April 2017

Christoph Becker und Stefan Brütsch

Die systematische Suche nach neuen Erkenntnissen sowie deren Dokumentation und Veröffentlichung – also die Forschung – ist eines der Kerngeschäfte der Universität. Dabei hat sich die Informations- und Telekommunikationstechnik für die Gewinnung und Verarbeitung von Forschungsdaten zu einem der wichtigsten Arbeitsmittel der Wissenschaftler und Wissenschaftlerinnen entwickelt. Viele Forschende sind deshalb bei ihrer täglichen Arbeit in höchstem Maße von zuverlässig funktionierenden, technisch abgesicherten und bedarfsgerecht ausgebauten IT-Systemen und Datennetzen abhängig.
Die darin verarbeiteten Forschungsdaten sind jedoch Sicherheitsbedrohungen unterschiedlichster Art ausgesetzt. Forschungsdaten können besonders schützenswert sein, wenn diese noch nicht publiziert worden sind, personenbezogene Daten enthalten oder einer vertraglichen Geheimhaltung unterliegen. Unzureichende Schutzmaßnahmen gegen unbefugte Einsichtnahme, Veränderung und Löschung dieser Daten können unter Umständen Forschungsvorhaben erheblich zurückwerfen, das Ansehen der Universität in der Öffentlichkeit (insbesondere gegenüber Partnern aus Wissenschaft und Industrie) schädigen oder gar zu hohen Schadensersatzansprüchen und Bußgeldern führen.
Darüber, ob und wie diese Informationen angemessen geschützt werden, entscheidet oft das individuelle Verhalten der IT-Benutzenden, die oft mit menschlichem Fehlverhalten, technischem Versagen oder vorsätzlichen Handlungen wie Sabotage und Spionage konfrontiert sind. Aufgrund der ständigen Bedrohung ist die Aufrechterhaltung der Informationssicherheit eine permanente Aufgabe, welche ein ausgeprägtes Sicherheits- und Risikobewusstsein und die aktive Mitwirkung jedes Einzelnen erfordert, um die richtigen Entscheidungen zur

richtigen Zeit treffen zu können.
Um die wissenschaftlichen Mitarbeiter und Mitarbeiterinnen dabei zu unterstützen, luden das Justiziariat und das IT-Securitymanagement am 24. und 25. April 2017 alle Interessierten zu zwei Thementagen unter dem Veranstaltungstitel „IT-Sicherheit und Datenschutz in der Forschung“ ein. Die in dieser Form erstmalige Veranstaltung an der Universität Konstanz stieß auf großes Interesse. So verfolgten bis zu 60 Personen die Hauptveranstaltungen an den Thementagen.
Mit einer Kombination aus Vorträgen von Referenten aus der Wissenschaft, der Wirtschaft und vom Verfassungsschutz sowie Präsentationen und einem Datenschutzseminar bot die Veranstaltung ein umfassendes Informationsangebot.

Tag 1

Den Auftakt machte Prof. Dr. Wolfgang Hommel, Professor für IT-Sicherheit von Software und Daten an der Universität der Bundeswehr München. In seinem Vortrag „Gehackt werden sowieso nur die anderen – in fünf Schritten zur vollwertigen digitalen Sorglosigkeit“ präsentierte er sehr anschaulich anhand von aktuellen Gefahren – wie den sog. „Erpressungstrojanern“ – die derzeitig noch stark verbreitete Sorglosigkeit vieler IT-Nutzer und ihre oft verheerenden Folgen. Abgeschlossen wurde der Vortrag mit herrlich satirischer Note mit einer Zusammenfassung maßgeblicher Handlungs- und Denkweisen für mehr Sicherheit und Privatsphäre: Gesundes Misstrauen gegenüber neuen Technologien und Organisationen, ständige Weiterbildung und sachgemäßer Umgang mit Sicherheitsvorfällen.
Im Anschluss daran sprach Prof. Dr. Rainer W. Gerling, IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft, über „Hacker und Spione: Bedrohungen der IT-Sicherheit“. In seinem Vortrag beleuchtete er das aktuelle Lagebild der IT-Sicherheit in Deutschland und erläuterte, wie ein moderner IT-Angriff abläuft. Prof. Gerling veranschaulichte dabei den Teilnehmenden, wie attraktiv auch Hochschulen für Datendiebe sein können. Zusätzlich wies er auf die Problematik bei Sicherheitsvorfällen durch Schadsoftware hin, insbesondere, da diese in der Regel schwer bis gar nicht aufzuklären seien. Prof. Gerling gab Ausblicke auf zukünftige Entwicklungen in der Abwehr von Bedrohungen für die IT-Sicherheit und appellierte an jeden Nutzenden, dass für dessen Informationssicherheit die eigenen Handlungsweisen von entscheidender Bedeutung sind.
Die Gefahren durch zwischenmenschliche Manipulation, mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen - das sogenannte „Social Engineering“ - griff der dritte Referent, Herr Sebastian Neeff, in seinem Vortrag mit dem Titel „Datenschutz und IT-Sicherheit fängt bei mir an: Was kann ich selbst tun?“ auf. Aufgrund seiner Funktion als Geschäftsführer einer Beraterfirma mit dem Fokus auf IT-Sicherheit berichtete er von eigenen Erfahrungen und Erkenntnissen aus der freien Wirtschaft und gab den Teilnehmenden Denkanstöße sowie praktische Verhaltenstipps aus seiner Berufspraxis. Dabei untermauerte er die vom Vorredner Prof. Gerling angesprochenen Gemeinsamkeiten zwischen Wirtschaft und Hochschulen im Hinblick auf die Bedrohung durch Datenspionage.
Der letzte Sprecher der Hauptveranstaltung, Herr Karl-Friedrich Fecht vom Landesamt für Verfassungsschutz Baden-Württemberg, bot den Teilnehmenden einen anderen Blickwinkel: In seinem Vortrag „(Cyber-) Spionage und Sabotage in der Forschung“ rückte er die konkrete Bedrohung durch Spionage in den Fokus. Universitäten stellten durch ihr Know-how, insbesondere im Bereich der Naturwissenschaften wie Chemie oder Biologie, sowohl für fremde Nachrichtendienste als auch für ausländische Unternehmen ein begehrtes Ausforschungsziel dar. In seinem Vortrag beleuchtete Herr Fecht die Methoden und Ansatzpunkte ausländischer Nachrichtendienste im Bereich der Forschungsspionage und gab Erfahrungen aus der täglichen Arbeit des Verfassungsschutzes wieder.

Tag 2

Der zweite Tag startete mit einem Vortrag zum Thema „Sichere Nutzung von Cloud-Diensten“ von den beiden Konstanzern Prof. Dr. Marc H. Scholl in Kooperation mit Prof. Dr. Marcel Waldvogel. Darin wurden - am Beispiel des sich in Vorbereitung befindlichen Dienstes Nextcloud verschiedene Einsatzszenarien, Datenschutz- und Sicherheitsaspekte sowie Vor- und Nachteile im Vergleich zu anderen Datenspeichern diskutiert. Darüber hinaus erläuterten die Referenten, wie mithilfe der zusätzlichen Anwendung Boxcryptor[1] Daten unabhängig vom Speicherort sicher verschlüsselt

gespeichert und dennoch mit anderen Personen gemeinsam genutzt werden können.
Der nächste Vortrag fokussierte die vertrauliche Übermittlung von E-Mails und wurde von Herrn Christian Mack in Kooperation mit Herrn Rainer Rutka (beide KIM) gehalten. Unter dem Titel „Vertrauliche E-Mails: Verschlüsselung mit S/MIME“ wurden die Motivation, Funktionsweise und die Verwendung von E-Mail-Verschlüsselung auf allgemein verständliche Weise dargestellt.
Im letzten Vortrag des Tages, mit dem Titel „Zuverlässiges Dokumentenmanagement mit Alfresco“, stellte Herr Dr. Stefan Hohenadel (KIM) den Teilnehmenden die Grundfunktionen für das Verwalten von und die gemeinsame Arbeit an Dokumenten vor, was ihnen den Einstieg in die Arbeit mit dem Dokumentenmanagementsystem vereinfachen soll.
Den Abschluss der Thementage bildete das Seminar „Datenschutzrechtliche Bestimmungen für Wissenschaftler/innen“, welches Herr Andreas Lumpe von der ZENDAS (Zentrale Datenschutzstelle der Baden-Württembergischen Universitäten) angeboten hatte. Das Seminar sensibilisierte zunächst für die Frage, wann forschungsbezogene Daten einen Personenbezug aufweisen. Die Teilnehmenden erhielten zudem einen Überblick über datenschutzrechtliche Bestimmungen, die beim Umgang mit personenbezogenen Daten zu berücksichtigen sind, und erfuhren unter Einbeziehung praktischer Beispiele, welche Schritte zu unternehmen und Besonderheiten bei der Planung von Forschungsvorhaben zu beachten sind.

Fazit und Danksagung

Die Thementage waren in vielerlei Hinsicht ein Erfolg. Die Veranstaltungen führten den Teilnehmenden die Wichtigkeit des eigenen Handelns – sowohl im privaten als auch im beruflichen Kontext – vor Augen und gaben neue Impulse, die möglichen Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Forschungsdaten beim Einsatz von Informationstechnologie sowie die Risiken bei der elektronischen Erfassung, Speicherung und Verarbeitung personenbezogener Daten zu erkennen, zu bewerten und angemessen darauf reagieren zu können.

Bei der Gelegenheit möchten wir uns nochmals ganz herzlich bei allen Beteiligten bedanken, die geholfen haben, die Veranstaltung auf die Beine zu stellen. Besonderer Dank gilt den Referenten.

Fußnote:

1 Boxcryptor schützt, Daten in einer Cloud mit Ende-zu-Ende-Verschlüsselung