



Die Digitalisierung verändert unser Leben in nahezu allen Bereichen. Treiber hinter diesem Prozess ist die Informatik, die sich dadurch auch selbst stark wandelt. Viele unterschiedliche Teilgebiete erlangen im Zuge der Digitalisierung eine besondere Relevanz. Hierzu zählen z. B. das Internet der Dinge oder die Analyse großer und teilweise öffentlich verfügbarer Datenmengen. Gleichzeitig erfordert die zunehmende Vernetzung aber auch neue Entwicklungen im Bereich der IT-Sicherheit.

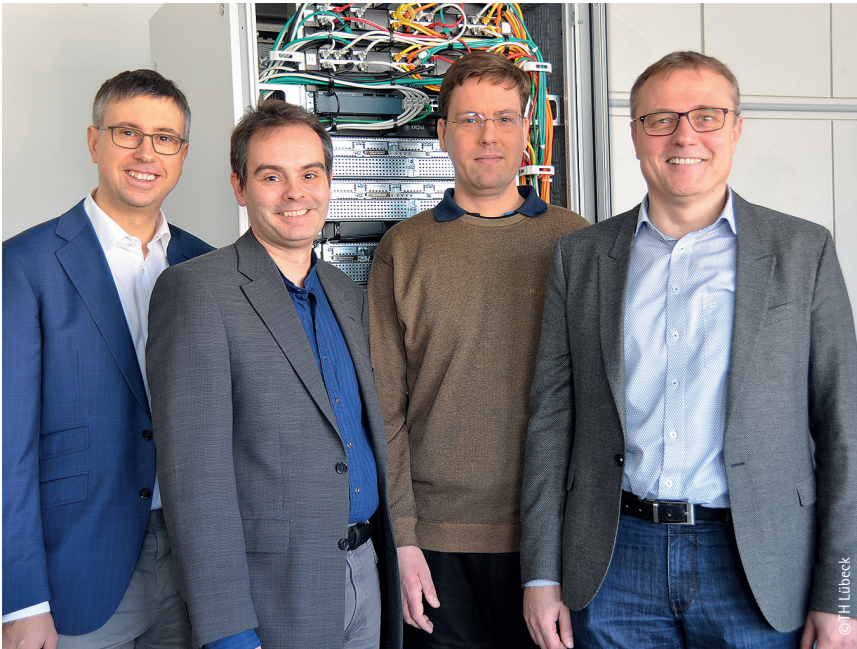
„Wenn Dinge miteinander reden, über was reden sie dann und warum?“ Diese Frage beantwortet Herr Prof. Dr.-Ing. Horst Hellbrück in seinen Forschungsarbeiten. Dass Dinge anfangen zu reden, ist kein Zufall, sondern eine Folge der Entwicklung der Technik. Seit Jahren werden Alltagsgeräte mit elektronischen Schaltkreisen ausgestattet, so dass sie komplexere und teilweise neue Aufgaben übernehmen. Das einfache Schnurtelefon ist so zum Smartphone geworden und wird für vieles aber kaum noch zum Telefonieren verwendet. Die Elektronik wird so günstig und leistungsfähig, dass auch Alltagsgeräte programmiert und damit ihre Funktionalität gesteuert werden. So werden z. B. die Straßenlampen einer ganzen Stadt in die Lage versetzt, miteinander zu kommunizieren. Durch dieses flächendeckende Netz las-

sen sich dann weitere Dinge anbinden, ob es die Mülltonnen sind, die den Füllstand melden oder die Stromzähler, die den Verbrauch melden.

Schwerpunkte sind die angewandte Forschung zu modernen Strukturen und Anwendungen in den Anwendungsfeldern: Maritime Technik, Medizintechnik, Industrie 4.0, Internet der Dinge. Durch Dienstleistungen des Kompetenzzentrums CoSA, wie z. B. Messungen, Machbarkeitsstudien, Wissenstransfer und Schulungen profitieren auch kleine und mittelständische Unternehmen vom Forschungsstandort Lübeck.

Am Beispiel des sozialen Netzwerks Twitter und der Frage, ob der Ausgang der Bundestagswahl 2017 bereits im Vorfeld absehbar war, demonstriert Prof. Dr. Nane Kratzke wie Datenanalyse in sozialen Netzwerken nicht nur den Betreibern solcher sozialer Netzwerke offensteht, sondern auch in einem Jedermann-Ansatz selber durchgeführt werden kann. In einem Dreimonatszeitraum wurden Twitterinteraktionen um 364 Politiker aller Fraktionen des Bundestags und der AfD „mitgeschnitten“ und analysiert. Aus den etwa 10 Gigabyte an gesammelten Daten konnten ca. 1,2 Mio. Interaktionen mit Bundespolitikern erfasst werden, die von ca. 120.000 Usern erzeugt wurden. Von diesem 120.000 Usern

ließ sich (mit gewissen Unsicherheiten) für etwa die Hälfte eine politische Nähe zu einer Partei ableiten. Spannender ist jedoch, wie unterschiedliche Parteien soziale Netzwerke unterschiedlich nutzen. Linke Parteien scheinen zumindest Twitter intensiver als konservative Parteien zu nutzen. Kleinere Parteien nutzen Twitter interaktiver als große Parteien. Große Parteien sind wesentlich abhängiger von der Reichweite ihrer Spitzenkandidaten als kleine Parteien. Aber vor allem populistische Parteien profitieren ungemein von den Mechanismen sozialer Netzwerke. Populistische Inhalte werden von Followern fast dreimal häufiger geteilt als Inhalte etablierter Parteien – populistische Parteien und ihre Inhalte erscheinen in sozialen Netzwerken damit wesentlich prominenter als sie in Wahrheit sind. Man kann also soziale Netzwerke durchaus dazu nutzen, dem „Volk aufs Maul“ zu schauen, man muss allerdings dahinter liegende „Verstärkungs“-Mechanismen sozialer Medien verstehen, um solche Daten zu interpretieren. Ferner ist zu berücksichtigen, dass Teilnehmer in sozialen Netzwerken keinen repräsentativen Bevölkerungsdurchschnitt darstellen. Linke und populistische Strömungen sind meist deutlich überrepräsentiert, konservative Parteien eher unterrepräsentiert. Follower populistischer Parteien teilen Inhalte wesentlich aktiver und erscheinen damit „aufgeregter“.



v.l.: Die Professoren Andreas Schäfer, Nane Kratzke, Andreas Hanemann und Horst Hellbrück



Bei Followern konservativer Parteien scheint eher ein konsumierendes (unaufgeregtes) Verhalten zu überwiegen. Diese verzerrenden Effekte (groß/klein, links/rechts, populistisch/etabliert) muss man sowohl als Bürger, als Politiker und auch als Journalist wissen und berücksichtigen. Wir nehmen sie indirekt (und unbewusst) jeden Tag auch in den klassischen Medien, Tageszeitungen und Nachrichtensendungen im Fernsehen wahr. Sind wir uns alle dessen immer so bewusst?

In den letzten Jahren wurde aber auch durch eine ganze Reihe von gravierenden Vorfällen deutlich, welche Gefahren bei einer Vernachlässigung der IT-Sicherheit in einer immer stärker vernetzten Welt entstehen können. Ein Beispiel war der Datenskandal Ende 2018, als ein Hacker jede Menge persönliche Daten von Politikern, Künstlern und anderen prominenten Personen in einem virtuellen Adventskalender veröffentlichte.

Am Fachbereich E+I und auch speziell im Kompetenzzentrum CoSA befasst sich Herr Prof. Dr. Andreas Hanemann daher mit der Frage, wie man die IT-Sicherheit verbessern kann. Hierbei ist es sinnvoll zu beachten, dass gerade KMUs aus Schleswig-Holstein nur begrenzte personelle Ressourcen haben, um sich mit dem Thema zu beschäftigen. Anstatt eine perfekte theoretische Lösung zu konzipieren, die am Ende nur unzureichend umgesetzt wird, ist es daher besser, einen realisierbaren Ansatz zu entwickeln.

Eine wichtige Rolle können hierbei Tools spielen, mit denen man ohne großen Aufwand feststellen kann, inwiefern Handlungsbedarf besteht. Beispielsweise kann man mit den Werkzeugen Arachni Scanner und OWASP ZAP den Webauftritt eines Unternehmens auf Schwachstellen bei der Programmierung testen. Diese beiden Tools sind eine Empfehlung aus einer ausführlichen studentischen Untersuchung verschiedener Tools, die man für diesen Zweck einsetzen kann. Für einen Test der Konfiguration des zugrundeliegenden Servers bietet sich das Webtool von Qualys an. Hiermit wird u. a. untersucht, ob die beim Zugriff mit https durchgeführte Verschlüsselung dem Stand der Technik entspricht.

Das Wissen über die IT-Sicherheit wird nicht nur im Rahmen der Lehre an die Studierenden vermittelt. Zusätzlich werden in Zusammenarbeit mit OnCampus, der eLearning Tochtergesellschaft der TH Lübeck, auch über das Internet zugängliche Online-Lehrmodule angeboten, die für jede(n) offen stehen. Das sind zum einen die Kurse aus dem Programm „QualiCS“ (<https://www.oncampus.de/qualics>), die teilweise von Personen von CoSA erstellt wurden. Zum anderen ist es der MOOC (Massive Open Online Course) „Netzwerksicherheit“ (<https://www.oncampus.de/weiterbildung/moocs/netzwerksicherheit>), der die Themen ausführlich behandelt und dabei einem regulären Studienmodul entspricht.

## KONTAKT

Technische Hochschule Lübeck  
 Fachbereich Elektrotechnik und  
 Informatik  
 Mönkhofer Weg 239  
 23562 Lübeck



Prof. Dr.-Ing. Horst Hellbrück,  
 Leiter des Kompetenzzentrums CoSA



Prof. Dr. Andreas Schäfer,  
 Studiengangsleiter Informatik

### Forschungsschwerpunkte:

Sicherheit, Internettechnologien und Internet der Dinge, Medizintechnik und Industrie 4.0, Drahtlose Übertragungstechnik und Ortung, Mensch-Maschine-Kommunikation und Usability Engineering, Cloud Computing