OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG
IST INSTITUT FÜR SOZIALFORSCHUNG UND TECHNIKFOLGENABSCHÄTZUNG

CANVAS

Workshop
on Ethics and Cybersecurity
in Health Care

Fachtagung im Rahmen des EU-geförderten Projekts CANVAS

24. & 25. April 2018

TechBase Regensburg

Sehr geehrte Damen und Herren,

das Organisationsteam des Workshops on Ethics and Cybersecurity in Healthcare begrüßt Sie herzlich in Regensburg. Am 24. und 25. April möchten wir mit Ihnen gemeinsam erkunden, wie der Einsatz von Informations- und Kommunikationstechnologie im Gesundheitswesen so gestaltet werden kann, dass sowohl die Sicherheit der technischen Systeme und der darin gespeicherten Daten gewährleistet ist als auch europäische Grundwerte geschützt werden.

Der Einsatz von Informations- und Kommunikationstechnologie im Gesundheitswesen bringt neue Wertekonflikte mit sich, lässt bereits bestehende Konflikte sichtbarer werden und/oder erhöht deren Dringlichkeit. Stakeholder wie PatientInnen, Angehörige, Pflegende, Leistungserbringer, Krankenkassen sowie die gesamte Gesellschaft sind mit konkurrierenden oder gar widersprüchlichen Zielen konfrontiert wie Effizienzsteigerung, Kostenreduzierung, Verbesserung der Behandlungsqualität oder der sicheren Informationssammlung, -speicherung, -verarbeitung und -übertragung. Gleichzeitig sollen im Gesundheitswesen grundlegende moralische Werte und/oder moralische Werte, die für die Beziehung zwischen PatientInnen und behandelndem Personal konstitutiv sind, geschützt werden. Solche Ziel- und Wertekonflikte werfen moralische Bedenken auf, da entschieden werden muss, welche Ziele und Werte vorrangig zu behandeln sind.

Wenn Informations- und Kommunikationstechnologie im Gesundheitssektor eingesetzt wird, soll bspw. sichergestellt werden, dass PatientInnen selbst bestimmen, wann welche Informationen an wen weitergegeben werden – Passwortschutz und Verschlüsselung sind Maßnahmen zur Erreichung dieses Ziels. In Notfällen besteht jedoch die Gefahr, dass wichtige medizinische Informationen nicht mehr zugänglich sind. Darüber hinaus könnte es sehr hilfreich sein, dem behandelnden Personal medizinisch relevante Patienteninformationen leicht zugänglich zu machen, um die Qualität und Effizienz der Behandlung zu verbessern. Das Ziel, die Privatsphäre und die Autonomie der PatientInnen zu schützen, kann dem jedoch entgegenstehen. Zudem wird in der einschlägigen Literatur oft erwähnt, dass es zur Gewährleistung von Cybersicherheit notwendig sein könnte, die Privatsphäre zu gefährden. Dies gibt Anlass zu besonderer Besorgnis, denn es liegt auf der Hand, dass sowohl der Schutz der Privatsphäre als auch die Sicherheit der Informationssysteme und der darin organisierten PatientInnendaten entscheidende Ziele im Gesundheitswesen sein müssen. Ohne Privatsphäre ist das für die medizinische Behandlung notwendige Vertrauen gefährdet und ohne die Gewissheit, dass Patientendaten nicht manipuliert oder gestohlen werden, ist die Behandlung selbst gefährdet.

Das von der EU im Rahmen von Horizon 2020 geförderte Projekt CANVAS, über das Sie auf den nächsten Seiten noch mehr lesen können, hat zum Ziel, Informationen über die ethische Gestaltung von Cybersicherheit zu sammeln, zu bündeln und EntscheiderInnen in Europa zur Verfügung zu stellen. Ein Werkzeug sind hierbei Workshops, die an verschiedenen Standorten stattfinden und nicht zuletzt dazu dienen, möglichst viele Stakeholder zusammenzubringen und zu vernetzen. Wir freuen uns, dass Sie dabei sind.

Dieser Workshop wäre nicht möglich ohne die Hilfe zahlreicher Institutionen und Personen: Das Zentrum Digitalisierung Bayern ebenso wie das INDIGO-Netzwerk unterstützen die Veranstaltung sowohl ideell wie auch materiell. Der IT Sicherheits-Cluster Bayern e.V. hilft uns bei der Organisation, das Team der TechBase bietet uns einen angemessenen Rahmen für den Workshop. Schließlich stellt die Integrata-Stiftung die Ressourcen für den e-Care-Preis zur Verfügung. Vor allem aber lebt ein Workshop von den Beiträgen der Vortragenden, von den Menschen, die moderieren und von Ihnen, die durch Diskussionen den Workshop lebendig werden lassen. Ihnen allen möchte ich im Namen des CANVAS-Konsortiums und des Workshop-Organisationsteams herzlich danken.

Prof.. Dr. Karsten Weber

Regensburg, April 2018

Inhaltsverzeichnis

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG
IST INSTITUT FÜR SOZIALFORSCHUNG UND TECHNIKFOLGENABSCHÄTZUNG

CANVAS

1. Contructing an Alliance for Value-driven Cyber-security (CANVAS)

Das CANVAS-Konsortium

CANVAS findet im Rahmen des EU-Programms Horizon 2020 als Collaboration and Support Action statt. Das Projekt begann im September 2016 und läuft für 3 Jahre mit einem Budget von 1,57 Mio. € (davon 1 Mio. € von der Europäischen Kommission). Das Konsortium umfasst elf Institutionen aus sieben Ländern, die in gemeinsamer Zusammenarbeit eine europäische Allianz für wertebasierte Cybersicherheit aufbauen. Das umfasst zum einen wissenschaftliche ExpertInnen

- der Vrije Univesiteit Brussel (Belgien)
- der Otto-Friedrich-Universität Bamberg (Deutschland)
- der Ostbayerischen Technischen Hochschule Regensburg (Deutschland)
- dem ADAPT Center der Dublin City University (Irland)
- der Technischen Universiteit Delft (Niederlande)
- der Universitat Rovira i Virgili Tarragona (Spanien),
- der Université de Lausanne (Schweiz) und
- der Berner Fachhochschule Biel (Schweiz)

Darüber hinaus bringen sich das führende IuK-Sicherheitsunternehmen F-Secure aus Helsinki (Finnland) und das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (Deutschland) ein. Koordiniert wird CANVAS vom Ethik-Zentrum der Universität Zürich (Schweiz) unter der Leitung von Dr. Markus Christen (Grant No.: 700540-CANVAS-H2020_DS-2014-2015/H2020-DS-2015-1).

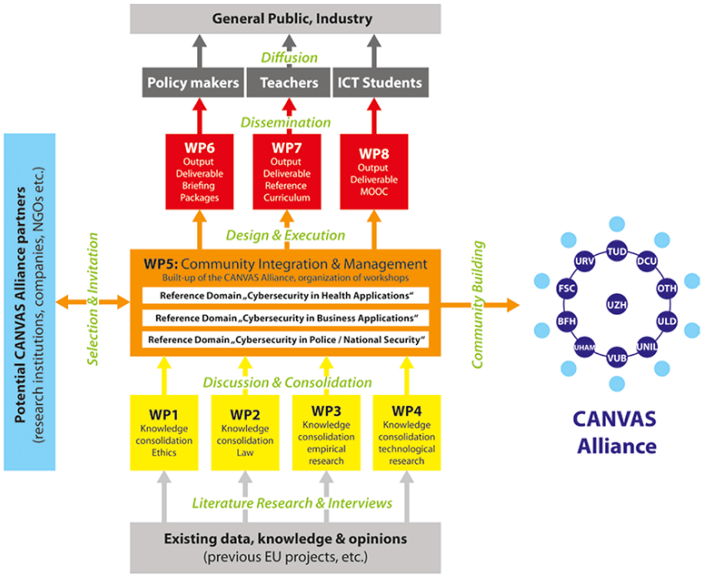
Ziel

Das Ziel von CANVAS ist es, Möglichkeiten zu finden, Cybersicherheit durchzusetzen, ohne dabei fundamentale Grundrechte und europäische Werte zu verletzen. Um dies zu bewerkstelligen, finden sich wissenschaftliche ExpertInnen zusammen, um in einem gemeinsamen Netzwerk mit Stakeholdern aus Wirtschaft und Politik alle relevanten Aspekte zusammenzutragen und Strategien auszuarbeiten, mit denen dies gelingen kann. Dieses Konsortium soll über die Projektzeit hinaus erhalten bleiben, um beständig an Lösungswegen zu arbeiten und einen breiten Diskurs um eine wertbasierte Cybersicherheit voranzutreiben.

Workpackages & Deliverables

CANVAS erfolgt in verschiedenen Arbeitspaketen. Im ersten Schritt wurden bereits existierendes Wissen und Daten über vier Bereiche in White Paper zusammengetragen:

- Ethik und Cybersicherheit (WP 1)
- Recht und Cybersicherheit (WP 2)
- Empirische Forschung über die Einstellungen zu Cybersicherheit (WP 3)
- Aktuelle technische Herausforderungen für die Cybersicherheit (WP 4)



Daran anknüpfend sind eine Reihe von Workshops geplant (WP 5). CANVAS wird sich dabei auf drei soziale Bereiche konzentrieren, die jeweils unterschiedliche Wertekonflikte beinhalten:

- Gesundheitsbereich
- Finanzwesen
- Strafverfolgung bzw. nationale Sicherheit

Die Ergebnisse dieser Arbeitsgruppen werden genutzt, um die Diskussion um wertebasierte Cybersicherheit mit verschiedenen Akteuren aufrechtzuerhalten und voranzutreiben.

Konkret geplant sind:

- Informationsmaterial für Stakeholder aus der nationalen und EU-Politik
- Referenzmaterialien für Schulungen über wertebasierte Cybersicherheit
- Erstellung eines MOOC (Massive Open Online Course) über wertebasierte Cybersicherheit

Weitere Informationen zu CANVAS unter:

https://canvas-project.eu/canvas/

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG
IST INSTITUT FÜR SOZIALFORSCHUNG UND TECHNIKFOLGENABSCHÄTZUNG

CAWAS

2. Netzwerk Internet und Digitalisierung Ostbayern (INDIGO)

Das Netzwerk Internet und Digitalisierung Ostbayern basiert auf einem Zusammenschluss von sechs ostbayerischen Hochschulen und verfügt über hohe wissenschaftliche Expertise im Handlungsfeld Internet und Digitalisierung. Der Verbund bündelt die (Forschungs-) Kompetenzen zahlreicher Wissenschaftler*innen aus verschiedenen akademischen Disziplinen in thematisch strukturierten Arbeitseinheiten, die sich u.a. mit IT-Sicherheit, Big Data, Mobilität, Industrie 4.0, Medien, ethischen Fragestellungen und Medizintechnik befassen.

Zielsetzung des Netzwerks INDIGO

INDIGO wurde 2014 zu dem Zweck gegründet, die Region Ostbayern als Wissenschafts- und Wirtschaftsstandort zu stärken sowie Wirtschaft, Politik und Gesellschaft auf dem Weg zu einer zukunftsweisenden Nutzung des Internets wie auch der globalen Digitalisierung kontinuierlich zu begleiten. Hierbei fördert das Netzwerk insbesondere die fachübergreifende Kooperation auf dem Gebiet der angewandten Forschung und Grundlagenforschung im Bereich Internet und Digitalisierung zwischen den beteiligten Hochschulen.

Aktivitäten des Netzwerks INDIGO

Förderung von Forschungskooperationen

Das Netzwerk INDIGO unterstützt u.a. durch die Einrichtung von Arbeitseinheiten und die Förderung des Dialogs zwischen verschiedenen Fachdisziplinen die hochschulübergreifende Zusammenarbeit zwischen den beteiligten Wissenschaftler*innen im Themenfeld Internet und Digitalisierung.

Förderung des wissenschaftlichen Nachwuchses

Durch die Einrichtung geeigneter Veranstaltungsformate schafft das Netzwerk INDIGO Austausch- und Vernetzungsmöglichkeiten für den wissenschaftlichen Nachwuchs, um hochschulübergreifend einen fachlichen Dialog zu Themen im Bereich Digitalisierung und die Entwicklung innovativer Forschungsprojekte zu ermöglichen.

Organisation von Veranstaltungen

Die INDIGO-Veranstaltungen sind ein wesentlicher Bestandteil der Netzwerkaktivitäten und befassen sich mit zentralen Fragen rund um das Thema Digitalisierung. Sie dienen vor allem dem Austausch zwischen den beteiligten Wissenschaftler*innen und der Vernetzung mit Akteuren aus Wirtschaft, Gesellschaft und Politik. Die nächste Jahreskonferenz wird am 23. November 2018 an der TH Deggendorf zum Thema „Mobilität“ stattfinden. Weitere Veranstaltungsformate sind beispielsweise Themen-Workshops und Doktorandentreffen.

Vernetzung und Kommunikation

Das Netzwerk INDIGO dient als Wissens- und Informationsdrehscheibe für Mitglieder und Kooperationspartner. Durch geeignete Vernetzungs- und Kommunikationsaktivitäten soll sowohl die Zusammenarbeit im Netzwerk gestärkt als auch ein Bewusstsein für die vorhandene wissenschaftliche Expertise und die Belange der INDIGO-Hochschulen in Gremien der Wissenschaftsförderung sowie in Wirtschaft, Gesellschaft und Politik geschaffen werden.

Mitglieder des Netzwerks INDIGO

- OTH Amberg-Weiden
- TH Deggendorf
- HAW Landshut
- Universität Passau
- OTH Regensburg
- Universität Regensburg

Struktur des Netzwerks INDIGO

- Direktorium
- Steuerkreis
- Geschäftsstelle
- Themencluster und Arbeitseinheiten

Wissenschaftliche Leitung:
Prof. Dr. Burkhard Freitag (Universität Passau)

Netzwerkmanagerin:
Christine Schnellhammer, M.A.
christine.schnellhamer@uni-passau.de
+49 (0) 851 509 1588

Geschäftsstelle:
INDIGOnetzwerk
Innstraße 43 (ITZ)
94032 Passau

Sekretariat:
Karin Pretzl
+49 (0) 851 509 1589
karin.pretzl@uni-passau.de

Weitere Informationen zum Netzwerk INDIGO unter:
www.indigo-netzwerk.de

3. Bayerischer IT-Sicherheitscluster e.V.

Im Bayerischen IT-Sicherheitscluster e.V. arbeiten Unternehmen der IT-Wirtschaft, Unternehmen, die IT-Sicherheitstechnologien nutzen, Hochschulen, weitere Forschungs- und Weiterbildungseinrichtungen sowie Juristen an gemeinsamen Zielen. Schwerpunktthemen im Bereich der IT-Sicherheit sind dabei IT-Security und Functional Safety.
Der Verein hat es sich zur Aufgabe gemacht, die Wettbewerbsfähigkeit und die Marktchancen der Mitgliedsunternehmen zu erhöhen. Aus den Kompetenzen und Interessen der einzelnen Mitglieder sowie aus den jeweils im öffentlichen Fokus stehenden IT-Security-Themen entwickeln sich die Arbeitsfelder des Bayerischen IT-Sicherheitsclusters.

Lösungen des Clusters

Spezielle Lösungen für KMU wurden in den Netzwerken des Bayerischen IT-Sicherheitsclusters entwickelt:

- ISIS12: In 12 Schritten zu einem ISMS
- ISA+Informations-Sicherheits-Analyse: Mit 50 Fragen zur Informationssicherheit
- iDSMS7: integriertes DatenSchutzManagement-System in 7 Schritten

Arbeitskreise

- Datenschutz
- Vertriebskooperationen
- Industrial IT Security
- Informationssicherheitsbeauftragte

Foren

- Automotive Safety
- Datenschutz
- IT-Security

Ziele

- Bündelung der IT-Sicherheits-Kompetenz in Bayern
- Förderung der Erforschung, Entwicklung, Anwendung und Vermarktung von Produkten der IT-Security und Functional Safety
- Unterstützung im Bereich Aus- und Weiterbildung (u.a. Ausbildung zum Informationssicherheits-Beauftragten)
- Initiierung und Begleitung von Kooperationen zwischen Wissenschaft und Wirtschaft im Bereich der IT-Sicherheit
- Unterstützung der Zusammenarbeit von Einrichtungen und Initiativen zur Förderung der IT-Sicherheit in Unternehmen
- Unterstützung von Gründern

Kooperationen

- Initiierung und Leitung von Netzwerken, welche spezielle Lösungen für den Mittelstand und Organisationen entwickeln, z.B. ISIS12, I-SA+Informations-Sicherheits-Analyse, Datenschutzmanagementsystem iDSM7
- Initiierung von Arbeitsgruppen und Workshops
- Kooperationsworkshops, z.B. Vertriebskooperationen
- Plattform für Networking
- Kostenfreie oder vergünstigte Teilnahmemöglichkeit an Veranstaltungen und Weiterbildungen, wie den hochschulzertifizierten Lehrgang zum Informationssicherheitsbeauftragten (ISB)
- Organisation von Gemeinschaftsständen auf Messen, z.B. it-sa

Umsetzung

Die Mitglieder arbeiten in den Netzwerken und Projektgruppen der einzelnen Arbeitsfelder gemeinsam an Produkten, Innovationen, Förderanträgen oder Marketingaktionen. Das Clustermanagement begleitet und unterstützt die thematische Arbeit und bietet allen Mitgliedern gezielte Kontaktvermittlung, die Präsentation ihrer Kompetenzen und umfangreiche Informationen.

Organisation und Management

Das 2006 gegründete Bayerische IT-Sicherheitscluster ist seit Juli 2013 als Verein organisiert. Der Vorstand besteht aus sechs Personen, die mit den Schlüsselaufgaben Clustermanagement, Mitgliederwerbung, Forschung und Weiterbildung sowie regionaler Repräsentation in den Großräumen München, Augsburg und Nürnberg betraut sind.

4. Das Zentrum Digitalisierung.Bayern (ZD.B)

Das Zentrum Digitalisierung.Bayern (ZD.B) erweitert die Kompetenzen im Bereich der Digitalisierung und der Nutzung digitaler Technologien in Bayern. Als Impulsgeber schafft es Synergien und beschleunigt den Wissenstransfer, indem es bayernweit Unternehmen, Start-ups, Hochschulen und Forschungseinrichtungen vernetzt. Das ZD.B hat das Ziel, die internationale Sichtbarkeit Bayerns zu erhöhen, und leistet einen wichtigen Beitrag, die Attraktivität Bayerns im Bereich der Digitalisierung zu stärken.

Die Themenplattformen bieten ein Austausch- und Aktivitätsforum zu zentralen Themen der Digitalisierung. Durch Vernetzungsaktivitäten, Veranstaltungen und die Initiierung von Projekten befördern sie den inhaltlichen Diskurs und beschleunigen den Wissenstransfer.

Wissenschaftliche Forschung an den Hochschulen und wirtschaftliche Innovation in den Unternehmen werden durch die ZD.B-Maßnahmen gefördert und eng miteinander verknüpft. Dies ist unverzichtbar, um dem dynamischen Tempo der Digitalisierung gerecht zu werden.

Bislang wurden folgende Initiativen auf dem Gebiet der Digitalisierung gestartet:

- **Neu geschaffene Professuren** erweitern die wissenschaftlichen Kompetenzen.
- **Nachwuchsforschungsgruppen** fördern junge besonders qualifizierte Wissenschaftler.
- Das **Doktorandenprogramm** vernetzt und fördert herausragende Hochschulabsolventen.
- **Innovationslabore für Studierende** ermöglichen es Studierenden, an innovativen Ideen zu arbeiten.

Das ZD.B unterstützt die Gründerinitiativen in Bayern und trägt zur **Optimierung des Ökosystems** bei. Insbesondere werden die neuen digitalen **Gründerzentren in den Regionen** in die Arbeit der Themenplattformen und Initiativen des ZD.B einbezogen. Zudem werden zukünftige Ideengeber und IT-Gründer bereits an den Hochschulen **frühzeitig** motiviert und mit fachlichen wie auch unternehmerischen Kenntnissen ausgestattet. Hierzu wird die **Entrepreneurship-Ausbildung** mit Schwerpunkt Digitalisierung an verschiedenen Hochschulen in Bayern verstärkt.

Ergänzend unterstützt das Cluster BICCnet Unternehmen bei der Internationalisierung ihrer Aktivitäten.

Folgende Themenplattformen sind zurzeit eingerichtet:

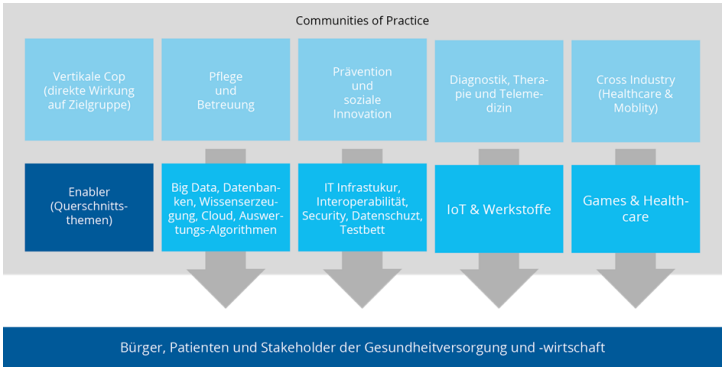
- Cybersecurity
- Digital Production & Engineering (Doppelplattform)
- Digitale Gesundheit/Medizin
- Digitalisierung im Energiebereich
- Vernetzte Mobilität
- Digitalisierung in Bildung, Wissenschaft und Kultur

* Jährliche Planung von Themen-Schwerpunkten und aufeinander abgestimmter Aktivitäten im Zusammenspiel mit Akteuren, Sprechern und Koordinatoren der Themenplattformen.

** Gilt nicht für die TP Digitalisierung in Bildung, Wissenschaft und Kultur

Die Themenplattform Digitale Gesundheit/ Medizin

Es ist das Bestreben der Themenplattform (TP) Digitale Gesundheit/Medizin des ZD.B, Forschungs- und Entwicklungsaktivitäten zu stimulieren, deren Ergebnisse zu einer messbaren Steigerung der Effektivität und Effizienz der Gesundheitsversorgung beitragen. Die intelligente Verknüpfung aller vorliegenden Daten zur Gesundheitsförderung und Prävention, zu Krankheitsverläufen und wissensbasierten Entscheidungsprozessen in Diagnostik, Therapie und Nachsorge sowie zur häuslichen Pflege ist dabei essenziell für Prozess- und Outcome-Optimierung.



Die Communities of Practice sind ein offenes Format, das partizipativ und bedarfsorientiert ausgestaltet wird. Die TP lädt alle interessierten Gruppen und Akteure dazu ein, sich aktiv in die CoPs einzubringen und an der Initiierung und Durchführung innovativer Maßnahmen und Projekten mitzuwirken. Von der Projektanbahnung bis hin zur Projektdurchführung unterstützt Sie die TP gerne bei der Vermittlung von Experten, Öffentlichkeitsarbeit, Beantragung von Förderungen etc.

Kommen Sie auf uns zu und bringen Sie sich aktiv ein!

Ihre Koordinatoren der Themenplattform Digitale Gesundheit/ Medizin:

Maria Marlene Bohrer-Steck, maria.bohrer-steck@zd-b.de
+49 (0)89 – 24 88 07 -136
Sebastian Hilke, sebastian.hilke@zd-b.de
+49 (0)9131 – 9161756

5. Programmübersicht 1. Tag (24. April 2018)

12:30 - 14:00 Uhr

- **Eröffnung:** Prof. Dr. Klaudia Winkler, Vizepräsidentin der OTH Regensburg
- **Grußwort:** Peter Steiert, Leiter der Abteilung 1: Kommunikation, Landesprüfungsamt für Sozialversicherung, Bayerisches Staatsministerium für Gesundheit und Pflege
- **Begrüßung:** Prof. Dr. Karsten Weber, OTH Regensburg, Tagungsorganisation und CANVAS-Konsortialmitglied
- **Vorstellung CANVAS:** Dr. Markus Christen, UZH Zürich, Konsortialführer CANVAS
- **Eröffnungsvortrag zu Cybersicherheit als Spannungsfeld des Datenschutzes:** Corina Scheiter, Referat technischer und organisatorischer Datenschutz beim Bayerischen Landesbeauftragten für den Bereich Gesundheit und Soziales: *Cybersecurity und Datenschutz: Freunde oder Feinde beim Umgang mit eHealth?*

14:00 - 14:15 Uhr

- **Pause**

14:15 - 15:15 Uhr

- **Keynote zu Cybersicherheit, Datenschutz und Ethik aus rechtswissenschaftlicher Perspektive:** Prof. Dr. Dirk Heckmann, Universität Passau: *Autonomes Fahren—E-Health—Cybermobbing: Vernetzung und Automatisierung als rechtliche und ethische Herausforderung*
- **Keynote zu Cybersicherheit, Datenschutz und Ethik in der medizinischen Praxis:** David Koeppe, Konzerndatenschutzbeauftragter Vivantes-Netzwerk für Gesundheit GmbH

15:15 - 15:45 Uhr

- **Kaffeepause**

15:45 - 16:45 Uhr

- **Keynote zu Telemedizin und Cybersicherheit aus der Praxisperspektive:** Dr. Christoph Götz, Leiter Gesundheitstelematik der Kassenärztlichen Vereinigung Bayern: *Telemedizin unter dem Brennglas von Cybersicherheit: Spezielle Herausforderungen und praktische Lösungsansätze*
- **Keynote zu den Möglichkeiten institutioneller Förderung von Cybersecurity:** Prof. Dr. Dr. h.c. Manfred Broy, Zentrum Digitalisierung Bayern: *Die Herausforderungen der Digitalisierung in der Medizin: Datennutzung, Datensicherheit und ethische Erwägungen*

16:45 - 17:15 Uhr

- **Fragen aus dem Plenum an alle Vortragenden**

17:15—17:30 Uhr

- **Pause**

17:30 - 18:00 Uhr

- **Preisverleihung eCare-Preis:** Vorstellung Integrata-Stiftung, Michael Mörike, Vorstand der Integrata-Stiftung Kurzvorträge der PreisträgerInnen & Laudatio auf die PreisträgerInnen, Prof Dr. Karsten Weber

18:00 - 20:00 Uhr

- **Stehempfang & Vernetzung**

5. Programmübersicht 2. Tag (25. April 2018)

09:00 - 10:30 Uhr

Session 1: mHealth

Einführung durch den Chair Prof. Dr. Horst Kunhardt, TH Deggendorf
Vortrag von Prof. Dr. Walter Swoboda, HAW Neu-Ulm: *Cybersecurity in mHealth-Anwendungen: Ein Fallbeispiel*

Session 2: Pflegetechnik und altersgerechte Assistenzsysteme

Einführung durch den Chair Prof. Dr. Christa Mohr, OTH Regensburg
Vortrag von Prof. Dr. Frank Teuteberg, Universität Osnabrück: *Das Modellprojekt Dorfgemeinschaft 2.0: Altersgerechte Assistenzsysteme in der gesundheitlichen Versorgung im ländlichen Raum*
Vortrag von Prof. Dr. Josef Hilbert, IAT Gelsenkirchen: *Auswirkungen von Big Data auf die Pflege*

10:30 - 11:00 Uhr

- **Kaffeepause**

11:00 - 12:30 Uhr

Session 3: Digitale Implantate

Einführung durch den Chair Prof. Dr. Sebastian Dendorfer, OTH Regensburg
Vortrag von Johannes Roos, Tuomi: *Digitale Implantate: Steuerung, Programmierung und Monitoring über die Cloud*
Vortrag von Enno Park, Cyborg e.V.: *Mein Implantat gehört mir*

Session 4: EGK und EPA

Einführung durch den Chair Prof. Dr. Georgios Raptis, OTH Regensburg
Vortrag von Prof. Dr. Thomas Wetter, Universität Heidelberg: *Wie die Informatik - zu Recht? - Grundfesten der Medizin erschüttert*
Vortrag von Holm Diening, Gematik: *Sicherheitsmechanismen der Telematikinfrastruktur*

12:30 - 13:30 Uhr

- **Mittagspause**

13:30 - 15:00 Uhr

Session 5: Big Data

Einführung durch den Chair Prof. Dr. Christoph Palm, OTH Regensburg
Vortrag von Eva Schlehahn, ULD Kiel: *Cybersecurity und Datenschutz im Gesundheitssektor: Konflikte und Synergien*
Vortrag von Max-R. Ulbricht: Technische Universität Berlin: *Einwilligungsmanagement für Fitness-, Vital– und Gesundheitsdaten*

Session 6: Kritische Infrastrukturen

Einführung durch den Chair Prof. Dr. Markus Bresinsky, OTH Regensburg
Vortrag von Prof. Dr. Rainer Bernnat, Strategy&: *Kritische Infrastrukturen im Gesundheitswesen: Auswirkungen der zunehmenden Digitalisierung*
Vortrag von Dr. Armin Will, Universitätsklinikum Schleswig-Holstein: Kritische Infrastrukturen und der Faktor Mensch: *Mehr IT-Sicherheit durch Problembewusstsein und Sensibilisierung der Mitarbeiter*

15:00 - 15:30 Uhr

- **Kaffeepause**

15:30 - 16:00 Uhr

- **Wrap Up**

6. Abstracts 1. Tag

Eröffnungsvortrag

Corinna Scheiter:

Cybersecurity und Datenschutz: Freunde oder Feinde beim Umgang mit eHealth?

Im Gesundheitswesen entstehen derzeit unter dem Begriff eHealth neue Möglichkeiten, medizinische Daten zu erfassen, automatisch auszuwerten und mit anderen zu teilen. Gerade für die medizinische Forschung, aber auch für die Früherkennung von Erkrankungen ergeben sich mit KI, Big Data und genetischen Analysen neue Ansätze.
Dies wirft jedoch auch einige Fragen im Hinblick auf den Datenschutz und die Datensicherheit auf. Insbesondere stellt sich die grundlegende Frage, ob alles, was technisch möglich ist, auch genutzt werden sollte oder ob (und welche) Grenzen benötigt werden.
Datenschutz wird oft als veraltet und Verhinderer von neuen Entwicklungen und Technologien angesehen. So scheinen Big Data-Ansätze, genetische Langzeitforschung, Selbstvermessung im direkten Gegensatz zu Prinzipien wie Datensparsamkeit, Zweckbindung, Nicht-Verkettbarkeit etc. zu stehen. Häufig ist zu hören, dass der Datenschutz durch Datenreichtum und Datensouveränität ersetzt werden sollte.
Cybersecurity bzw. IT-Sicherheit sind einerseits schon lange ein Teilaspekt des Datenschutzes (technisch-organisatorische Maßnahmen) und zudem wesentlich für den sicheren Betrieb von IT-Systemen und das Vertrauen der Nutzer in neue Technologien. Andererseits werden jedoch viele Entwicklungen kritisch beobachtet, da ein Mehr an Sicherheit häufig auch zu einem Mehr an Überwachung und Kontrolle führt (Videoüberwachung, Aufbrechen der Verschlüsselung aus Sicherheitsgründen, Hintertüren für Sicherheitsbehörden, Beseitigung der Anonymität, Datenspuren und Profilbildung, gläserner Bürger).
Es stellen sich daher einige Kernfragen:

- Wo ist die Grenze zwischen Sicherheit und Freiheit zu ziehen?
- Gibt es eine Pflicht zum gesunden Leben und zur Nutzung aller technischen Möglichkeiten (Selbstvermessung, genetische Analyse)?
- Dürfen Daten von Patienten auch ohne Kenntnis / Einwilligung genutzt werden, wenn dadurch anderen geholfen werden kann?
- Ist es überhaupt möglich, in komplexen technischen Systemen mit zunehmend automatisierten Entscheidungen (KI) die Kontrolle zu behalten?

Die Antwort aus Sicht des Datenschutzes ist einfach und gleichzeitig schwierig: Der Nutzen neuer Technologien ist unstreitbar, gleichzeitig ist jedoch der Datenschutz als das Recht informationeller Selbstbestimmung ein Grundrecht, das gewahrt bleiben muss. Es dürfen somit nicht alle technischen Möglichkeiten genutzt werden; gleichzeitig muss sich der Datenschutz an neue Themen anpassen.
Cybersecurity bzw. IT-Sicherheit ist hierbei ein wichtiges Element, um einen Ausgleich der Interessen zu finden. Häufig kann sie helfen, eine datenschutzfreundliche Techniknutzung umzusetzen (z.B. Konfigurationsmöglichkeiten, Pseudonymisierung, Verschlüsselung). Nicht zuletzt deshalb wurden in der Datenschutz-Grundverordnung (DSGVO) die technischen Aspekte deutlich stärker gewichtet (Aufnahme der Kriterien Privacy by Desgin / Default etc.)

Keynote zu Cybersicherheit, Datenschutz und Ethik aus rechtswissenschaftlicher Perspektive

Prof. Dr. Dirk Heckmann:

Autonomes Fahren - E-Health - Cybermobbing: Vernetzung und Automatisierung als rechtliche und ethische Herausforderung

Der Vortrag befasst sich mit den Chancen und ethischen Herausforderungen in drei digitalisierten Lebensbereichen: der Vernetzung in einer digitalisierten Verkehrsinfrastruktur (autonomes Fahren), der Vernetzung im Gesundheitswesen (E-Health) und der Vernetzung in der privaten Kommunikation (Social Media). Der Referent greift insoweit auf Erkenntnisse zurück, die er durch seine Mitwirkung an der Ethikkommission für automatisiertes und vernetztes Fahren, im Ethikbeirat der AOK Nordost zur Bewältigung der digitalen Transformation im Gesundheitswesen sowie im ARAG-Projekt zur Bekämpfung von Cybermobbing gewonnen hat.
In all diesen Bereichen eröffnen die Digitalisierung, Automatisierung und Vernetzung erhebliche Chancen. Sie bergen aber auch Risiken und Nebenwirkungen. Hier stellt sich die Frage, wie die Rechtsordnung mit diesen Herausforderungen umgeht bzw. umgehen sollte. Welcher Regulierungsbedarf besteht und wo stößt Regulierung an ihre Grenzen? Welche Spielräume hat der Gesetzgeber bei der Gestaltung der digitalen Zukunft? In allen drei Beispielszenarien werden auch die Geschäftsmodelle benannt und näher erläutert, inwieweit unredli-

6. Abstracts 1. Tag

che Geschäftsmodelle unterbunden werden können bzw. sollten. Woraus ergibt sich die Unredlichkeit? Was sind die Maßstäbe und (Verfassungs-)Werte, an denen sich die Abgrenzung von Redlichkeit und Unredlichkeit orientiert?
Am Ende wird die These aufgestellt, dass Rechtsschutz durch Technikgestaltung und Technikwissen gewährleistet werden kann. Ein konkreter Regelungsvorschlag am Beispiel eines Gesetzentwurfs zur Verbesserung des Persönlichkeitsrechtsschutzes im Internet zeigt auf, wie die Regulierung in einer digitalen Gesellschaft und digitalen Wirtschaft gelingen kann. Umgekehrt zeigt sich auch, dass der Gesetzgeber bei der Regulierung im Gesundheitswesen (E-Health) versagt hat und dass es eines stärker differenzierenden Regulierungsmodells beim autonomen Fahren bedarf.

Literatur:

- Bundesministerium für Verkehr und digitale Infrastruktur (2017). *Automatisiertes und vernetztes Fahren*. Abschlussbericht der Ethikkommission. PDF unter: http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile [15.04.18]
- Heckmann, D. & Köhler, K. (2018): *Werte im Netz besser schützen: Der Alternativvorschlag zum Netzdurchsetzungsgesetz*. Online unter: https://www.arag.com/german/press/pressreleases/group/00448/ [15.04.18]

Keynote zu Cybersicherheit, Datenschutz und Ethik in der medizinischen Praxis

David Koeppe:

Cybersicherheit, Datenschutz und Ethik in der medizinischen Praxis

Cybersicherheit - gehandhabt unter dem Begriff „Informationssicherheit“ - liegt in einem Krankenhaus traditionell in der Zuständigkeit der IT-Abteilung und erfährt erst allmählich eine breitere Würdigung. Diese Notwendigkeit zur Akzeptanz resultiert einerseits aus den immer größer werdenden Bedrohungen, über die in den Medien auch zunehmend eindringlicher berichtet wird. Andererseits werden die einschlägigen gesetzlichen Vorgaben spürbar strenger - vor allem in Form der EU-Datenschutzgrundverordnung und der Vorgaben für die Kritischen Infrastrukturen.
„Ethik“ ist dagegen ein Begriff, der im Krankenhaus nahezu ausschließlich der Sphäre des ärztlichen Handelns entstammt. Mit Informationssicherheit wird er üblicherweise nicht in Verbindung gebracht, auch wenn es darin bei näherer Betrachtung durchaus ethische Aspekte gibt.
Das der Informationssicherheit nahestehende Thema des Datenschutzes kennt solche ethischen Dimensionen seit jeher, letztlich ist dessen Ziel die Wahrung von Privatsphäre und Menschenwürde. Durch die gesetzgeberischen Aktivitäten und dem insbesondere in jüngster Zeit entstandenen betrieblichen Umsetzungsdruck müssen Datenschutz und Informationssicherheit zunehmend als Gesamtkomplex betrachtet werden, schon alleine, um keine parallelen Prozesse und Datensammlungen vorhalten zu müssen, die inhaltlich starke Überschneidungen aufweisen. Die damit mindestens implizit auch der Informationssicherheit aufzudrängenden Fragen nach den Rechten und Freiheiten natürlicher Personen befördern zweifelsohne auch die Ethik in das meist noch als technisch wahrgenommene Thema.
Dies wird anhand von einigen betrieblichen Handlungsfeldern aufgezeigt. Dabei geht es um teils althergebrachte Wertefragen, die auch schon immer als solche betrachtet, jedoch üblicherweise nicht mit dem Ethik-Begriff als solchem in Verbindung gebracht wurden. Der gesteigerte Umsetzungsdruck, der heutzutage hinter der Informationssicherheit speziell im Krankenhaus steht, führt künftig zweifelsohne zu vermehrten Interessenkollisionen. Um diese sachgerecht handhaben zu können, müssen zu einem verträglichen Ausgleich geregelte Diskurse geführt werden. Diese sind sowohl in die betrieblichen Prozesse einzubetten als auch mit einem geeigneten, reflektierten Instrumentarium innerhalb der Informationssicherheit zu versehen. Ohne ein Augenmerk auf diese didaktische Begleitung laufen die Belange der Sicherheit Gefahr, an unverhältnismäßigen Widerständen zerrieben zu werden. Die Mittel hierfür zu finden und die Wege zu bereiten ist Gegenstand von CANVAS.

Keynote zu Telemedizin und Cybersicherheit aus der Praxisperspektive

Dr. Christoph Götz:

Telemedizin unter dem Brennglas von Cybersicherheit: Spezielle Herausforderungen und praktische Lösungsansätze

Der Vortrag beginnt mit einem kurzen Hinweis auf die Unausweichlichkeit und Strukturveränderung von Digitalisierung im Gesundheitswesen. Dieser Faktenlage wer-

6. Abstracts 1. Tag / 7. Abstracts 2. Tag

den dann Überlegungen und Wahrnehmungen zu Sicherheit und Aufwand gegenübergestellt. Nach einem kurzen Blick auf speziellen Schutzbedarf und Motivation für IT-Sicherheit werden die teils schwierigen Realitäten in der Gesundheitsversorgung angesprochen: Cyberangriffe, Herausforderungen oder allgemeiner Kompetenzmangel. Dabei sollen ausgewählte Beispiele die Herausforderungen im eHealth-Bereich mit Blick IT-Sicherheit verdeutlichen: Smart Analytics oder Personalisierte Medizin.
Ein Ausblick zu Möglichkeiten der Entwicklung neuer digitaler Sicherheitsprodukte, zu Einflussnahme auf politische Positionen und zu neuen Strukturideen für gesundheitstelematische Infrastrukturmaßnahmen schließt diesen Block ab. Der Vortrag endet mit einem Plädoyer für ein verstärktes Engagement der Fachberufe mit besonderem Blick auf den Nachwuchs.

Keynote zu den Möglichkeiten institutioneller Förderung von Cybersecurity

Prof. Dr. Dr. h.c. Manfred Broy: Die Herausforderungen der Digitalisierung in der Medizin: Datennutzung, Datensicherheit und ethische Erwägungen

Die Digitalisierung verändert alles. Ein zentraler Punkt dabei ist die Erfassung von Daten, auch großer Datenmengen und die umfassende Nutzung dieser Daten durch Data Analytics. Gerade im Gesundheitsbereich bietet dies enorme Chancen. Heute ist es beschämend, wie im deutschen Gesundheitssystem die Möglichkeiten, Gesundheitsdaten und medizinische Daten digital zu erfassen und den Medizinern gezielt zur Verfügung zu stellen, ungenutzt bleiben. Patientenakte und Gesundheitskarte sind zwei Stichworte für ein nicht funktionierendes System. Auch aus ethischen Gründen ist es unabweisbar, dass die digitalen Möglichkeiten gerade in der Medizin genutzt werden müssen, um Patienten viel genauere Diagnosen und Therapien zu ermöglichen und entscheidende Effizienzverbesserung in das Medizinsystem einzubringen. Die Gründe dafür, weshalb dies nicht passiert, sind vielfältig, aber im Großen und Ganzen nicht technischer Natur. Darüber hinaus gibt es natürlich die ethische Herausforderung der Privatheit der Daten und der Sicherheit, dass gerade Gesundheitsdaten nicht missbraucht werden. Hier stellt sich die Frage, ob dieses Problem eher technisch zu lösen ist oder durch einen angemessenen Rechtsrahmen.

Session 1: mHealth

Prof. Dr. Walter Swoboda: Cybersecurity in mHealth-Anwendungen: Ein Fallbeispiel

Zu den Anfangszeiten der Computerwissenschaften waren via Terminal gesteuerte Mainframes die Regel. Mit Einführung der Personal Computer verschwand diese Architekturvariante, ist aber nun wieder in abgewandelter Form in Gebrauch. Internet-Auktionshäuser, soziale Netzwerke, Banken, Suchmaschinen: Sie alle arbeiten nach dem Client/Server-Prinzip, wobei aus ökonomischen Gründen der Schwerpunkt beim Server liegt, den Clients werden nur wenige Aufgaben und Daten übertragen. Diese asymmetrische Lastverteilung kommt auch in der Mehrzahl der mHealth-Applikationen zum Einsatz, allerdings aus anderen Motiven: Die verwendete Hardware muss klein und leicht sein, außerdem soll sie mit der zur Verfügung stehenden Energie sparsam umgehen, was mit einem distalen Datenkonzentrator und zentraler Rechenkapazität leichter zu realisieren ist. Das ist sicherheitsrelevant, da die notwendige Datenübertragung meist über öffentliche Kanäle erfolgt.
Digitales Sprachassistenten sind ideale Kommunikationsgeräte für Senioren, da sie weder ortsgebunden sind noch separat zu erlernende Schnittstellen benötigen [2,1,6]. Die sich ergebenden Möglichkeiten sind enorm und reichen von einfachen Erinnerungsanwendungen („Medikamente heute schon eingenommen?“), Kommunikation mit Angehörigen über soziale Netzwerke bis hin zu ausgeklügelten Trainingsprogrammen für Adhärenz und gezielter Krankheitsvorbeugung (z.B. bei Demenz) [7].
Praktisch jeder multinationale Anbieter von IT-Lösungen für den Consumer-Bereich bietet mittlerweile Lösungen an, die sich sogar auf eigene Hardware übertragen lassen und mittels zur Verfügung gestellter Programmierumgebungen angepasst werden können [4]. Alle diese Geräte haben den entscheidenden Nachteil, dass Daten aus Performance-Gründen mehr oder weniger ungeschützt übertragen werden. Es besteht ein erhebliches Security-Problem, unabhängig vom hier nicht betrachteten Umgang der Hersteller mit den Datensätzen.
Im Rahmen einer Feldstudie haben wir begonnen, einen digitalen Sprachassistenten ohne diese Einschränkungen zu entwerfen, der höchsten Sicherheitsanforderungen genügt, indem die verarbeiteten Daten auf dem Gerät verbleiben. Unsere Lösung basiert auf dem Single-Board-Computer Raspberry Pi [5], dem Betriebssystem

7. Abstracts 2. Tag

Raspbian und Jasper, einer digitalen Spracherkennungssoftware [3].
Das Pilotsystem läuft stabil und Tests zeigen gute Ergebnisse der Spracherkennung. Aufgrund seiner Modularität ist Jasper sogar leichter zu integrieren als kommerzielle Systeme und kann leicht durch zusätzliche Module ergänzt werden. Allerdings macht sich die geringe Rechenleistung bemerkbar: Vom Erkennen ganzer Phrasen wie bei den kommerziellen Lösungen ist das System weit entfernt. Erstaunlich ist die Güte der bei kommerziellen Lösungen eingesetzten Mikrofone; diese sind aus Kostengründen bei der Pilotlösung nicht verwendbar.
Um mhealth-Systeme sicher zu betreiben, ist hoher Aufwand nötig. Wenn Daten im geschützten Bereich verbleiben, muss die verwendete Hardware höheren Anforderungen genügen. Der erhöhte Ressourcenverbrauch gilt auch für eventuelle Verschlüsselungsalgorithmen bei Datenübertragung. Abhilfe durch leistungsfähigere Hardware ist nicht in Sicht: Künftige Applikationen werden die zur Verfügung stehende Performance schneller verbrauchen, als diese durch neue Entwicklungen zur Verfügung gestellt wird. Bei den PCs dauerte dieser Zustand über 30 Jahre und es ist davon auszugehen, dass er auch bei mhealth-Hardware ähnlich lange bestehen wird.
Um die Benachteiligung sicherer Systeme möglichst klein zu halten, muss künftig zwischen notwendiger Cybersecurity und eventuell vernachlässigbarem Formalismus unterschieden werden.

Literatur:

[1] Demiris, G., Rantz, M., Aud, M., Marek, K., Tyrer, H., Skubic, M. & Hussam, A. (2004). *Older adults' attitudes towards and perceptions of smart home technologies: a pilot study*. Medical Informatics and the Internet in Medicine, 29(2), 87-94
[2] Hargittai, E. (2002). *Second-level Digital Divide: Differences in People's Online Skills*. First Monday, 7(4)
[3] https://jasperproject.github.io
[4] Klosowski, T. (2017). *The Simplest Way to Build A Raspberry Pi-Powered Amazon Echo*. https://lifehacker.com/the-simplest-way-to-build-a-raspberry-pi-powered-amazon-1794218212
[5] http://www.raspberrypi.org
[6] Riggins, F. J. & Dewan, S. (2005). *The digital divide: Current and future research directions*. Journal of the Association for information systems 6(12), 13
[7] Wagner, N., Hassanein, K., & Head, M. (2010). *Computer Use by Older Adults: A Multi-Disciplinary Review*. Computers in Human Behaviour, 26(5), 870-882

Session 2: Pflegetechnik und altersgerechte Assistenzsysteme

Prof. Dr. Frank Teuteberg:

Das Modellprojekt Dorfgemeinschaft 2.0: Altersgerechte Assistenzsysteme in der gesundheitlichen Versorgung im ländlichen Raum

Der demographische Wandel stellt ländliche Regionen, in denen immer mehr Infrastruktur verloren geht, vor besondere Herausforderungen. Die medizinische und soziale Versorgung insbesondere auch der älteren Menschen kann immer schwieriger sichergestellt werden. Oft müssen weite Wege zum Arzt, zur nächsten Apotheke oder zur nächsten Einkaufsmöglichkeit zurückgelegt werden. Im Rahmen des Vortrags wird das Modellprojekt Dorfgemeinschaft 2.0 vorgestellt und berichtet wie altersgerechte Assistenzsysteme so gestaltet und nutzbar gemacht werden, dass konkrete Beiträge für mehr Teilhabe im Alter entstehen.
Das Projekt Dorfgemeinschaft 2.0 wird vom Bundesministerium für Bildung und Forschung im Rahmen des Demographiewettbewerbs „Innovationen für Kommunen und Regionen im demografischen Wandel (InnovaKomm)" gefördert. In dem Projekt (www.dorfgemeinschaft20.de; Laufzeit: 01.11.2015 bis 31.10.2020; Förderung durch BMBF; Projektvolumen: 5,82 Mio. Euro), an dem neben vielen Praxispartnern auch die beiden Osnabrücker Hochschulen beteiligt sind, geht es um telemedizinische Gesundheitsversorgung, intelligente Mobilität, Smart Home-Technologien, altersgerechte Mensch-Technik-Interaktion, datenbasierte Geschäftsmodelle, aber auch um „Satellitenstützpunkte" im ländlichen Raum, die den älteren Bürgern in wichtigen Fragen des Alltags und Lebens weiterhelfen und dazu beitragen sollen, dass sie möglichst lange unabhängig in ihrem gewohnten Umfeld leben können. Die Basis bildet ein „Virtueller Dorfmarktplatz", auf dem die Dienste in den Lebensräumen Wohnen, Mobilität, Versorgung, Gesundheit & Pflege sektorenübergreifend und patientenorientiert vernetzt und zugänglich gemacht werden.
Ausgehend von den Wünschen und Herausforderungen älterer Menschen wird im Vortrag anhand von Good-Practice-Beispielen aufgezeigt, wie durch Assistenzsysteme Menschen dabei unterstützt werden können ihr Leben im Alter selbstbestimmt zu gestalten.
Es werden Probleme und Herausforderungen (Vertrauen, Cybersicherheit, Datenschutz, Standards, Technologieakzeptanz, Partizipation, etc.) aufgezeigt, aber auch, welche positiven Schritte im Rahmen des

7. Abstracts 2. Tag

Projekts Dorfgemeinschaft 2.0 zur Entwicklung eines gesundheitsbezogenen Versorgungskonzepts in der Modellregion „Grafschaft Bentheim/Südliches Emsland“, unter maßgeblicher Einbindung kommunaler und regionaler Akteure, bereits stattgefunden haben.

Prof. Dr. Josef Hilbert:

Auswirkungen von Big Data auf die Pflege

Noch wird Big Data in der Pflege nicht genutzt. Deswegen können die Auswirkungen nicht erfahrungswissenschaftlich fundiert, sondern „nur“ plausiblisierend-spekulativ ausfallen.

Ausgangsbasis dafür sind

- die laufende Debatte mit Annahmen zu Chancen und Risiken
- eine erste Kartierung von Forschungs-, Entwicklungs- und Erprobungsaktivitäten
- empirisch fundierte Beiträge über den aktuellen Stand der Nutzung von Informations- und Kommunikationstechniken in der Sozial- und Gesundheitswirtschaft
- die Meinungen und Erwartungen von Experten und Beschäftigten zur zukünftigen Entwicklung

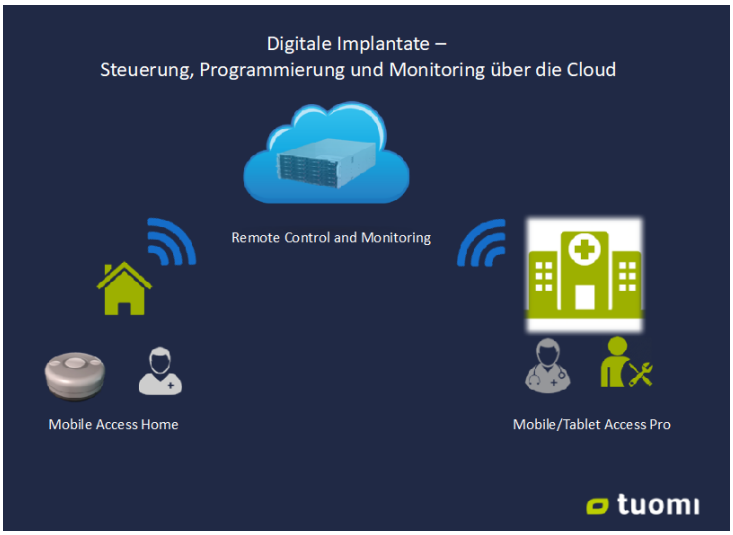
Wichtige Ergebnisse sind etwa, dass

- Gesundheit und Soziales ein großes, aktives und oft unterschätztes Einsatzfeld bei der Nutzung von Informations- und Kommunikationstechniken sind.
- in der Pflege sowohl im stationären als auch im ambulanten Bereich die Schwerpunkte bei der aktuellen Nutzung bei der elektronischen Dokumentation liegen und
- avancierte Nutzungen wie Robotik oder Künstliche Intelligenz (KI) (noch) sehr randständig sind.
- bei Beschäftigten eine große Technikaufgeschlossenheit herrscht, die bei aktiver Nutzung sich noch stärker ausprägt.
- Pflegerinnen und Pfleger kaum an der Entwicklung von Nutzungskonzepten für die digitalen Techniken beteiligt werden.

Spekulationen zur zukünftigen Nutzung von Big Data in der Pflege lassen sich vor diesem Hintergrund zu Szenarien verdichten:
Das Wunschszenario - es lässt sich sowohl aus Beschäftigtenbefragungen als auch aus den Absichten der ‚Macher‘ herleiten - ist, dass mit Hilfe von Big Data, KI und Robotik eine individualisierte, präventiv ausgerichtete Pflege entstehen wird. Sie ermöglicht beim Pflegepersonal nicht nur den Rückbau von körperlichen und psychischen Belastungen, sondern sie schafft auch neue Freiräume für den interaktiven Austausch mit Patienten und deren Angehörigen, Freundinnen und Freunden der Nachbarn.
Im Alptraumszenario ermöglicht die offensive Nutzung der IuK-Technologien in der Pflege Effizienzvorteile, die mehr Pflege-Patienten pro Pflegkraft möglich machen und von einer millimetergenauen Steuerung und Überwachung der Pflegeaktivitäten begleitet werden.

Session 3: Digitale Implantate

Johannes Roos: Digitale Implantate: Steuerung, Programmierung und Monitoring über die Cloud



Wenn über die Steuerung digitaler Implantate über die Cloud gesprochen wird, dann werden viele Menschen unsicher. Ein Artikel unter Heise Online wies noch vor kurzem auf die Gefahren hin, sobald Implantate gehackt werden können [1].
Die Angriffe der letzten Jahre auf IT Systeme haben dazu geführt, dass Gesetze und Regeln überarbeitet wurden. Die neue DSGVO fordert einen verantwortungsvollen Umgang mit personenbezogenen Daten. Information Security Management Systeme erhöhen die IT-Sicherheit in Organisationen.
In der Medizintechnik wie auch in anderen Segmenten stehen wir noch am Anfang der Entwicklung. Johnson & Johnson und St. Jude Medical mussten medizinische Geräte wegen massiver Sicherheitslücken vom Markt nehmen bzw. nachbessern.
Warum sollte man aber unbedingt Implantate in und über die Cloud verwalten? In den ersten Interviews und Gesprächen stellte sich schnell heraus, dass man mit einem solchem Ziel, sehr viele Aspekte erfüllen kann:

7. Abstracts 2. Tag

1. Verbesserung der Lebensqualität
2. Mehr Flexibilität im Leben der Patienten
3. Bessere Kontrolle über die eigenen Lebensumstände
4. Monitoring der Implantate aus der Ferne
5. Besser Unterstützung durch weltweite Kompetenz (Fachärzte beraten untereinander)
6. Geringere Kosten in der Versorgung der Patienten
7. Kontrolle und Verfolgbarkeit der Implantate im Produktlebenszyklus

Um bei der Umsetzung eines solchen Projektes ein hohes Maß an Sicherheit zu gewähren, ist eine tiefgreifende Planung unabdingbar. Vergleichen wir ein Cloud System mit einem hochkomplexen Gebäude, so würde man auch hier nicht mit dem Bau beginnen, bevor nicht wesentliche Teile der Architektur und der zu unterhaltenden Systeme im Detail geplant worden sind.
In einem Sicherheitskonzept einer IT Infrastruktur spielt Verschlüsselung eine wesentliche Rolle. Die Daten auf den Geräten, in der Cloud, der Datentransfer vom Implantat bis hin zum Lesegerät oder zur Weiterverarbeitung auf einem anderen Device müssen hoch verschlüsselt sein. Verschlüsselung ist eine grundsätzliche Maßnahme, die bereits bei der Entwicklung der Hardware mitberücksichtigt werden muss.
Gleiches gilt für den Datenschutz. Software sollte im Hinblick auf den Datenschutz bereits „privacy by design“ im Grundkonzept berücksichtigen.
Im weiteren Projekt werden folgende medizinischen Geräte unterschieden:

1. Das Digitale Implantat
2. Eine Kommunikationseinheit zwischen Implantat und mobile Device
3. Die Mobile Device App
4. Die Cloud Anwendung

Das Implantat sorgt im vorliegenden Anwendungsfall für die geregelte Medikamentenabgabe. Diese kann nach unterschiedlichen Kriterien gesteuert und überwacht werden.
Die Kommunikationseinheit verbindet das Implantat drahtlos mit dem mobilen Gerät.
Die mobile Geräte-App dient als zentrale Kommunikationseinheit zur Datenübertragung zwischen Cloud und Implantat, im Emergency-Fall gibt sie weitere Hilfen und bietet allgemeine Informationen wie z.B. den Termin der nächsten Wiederbefüllung.
Die Cloud Anwendung berechnet und simuliert die Medikamentenabgabe, verwaltet die Patientendaten oder wertet Statistiken aus. Neben den medizinischen Aspekten spielt die Logistik der Implantate eine wichtige Rolle. Der Lebenszyklus eines Produktes wird nachvollziehbarer, der unerlaubte Einsatz bereits benutzter Implantate wird auf Grund der eindeutigen weltweiten Identifizierung in der Cloud unmöglich.
Alle im Projekt eingesetzten Teile wie Implantat, Kommunikationseinheit, App und Cloud-Anwendung werden nach der neuen Medical Device Regulation (MDR) zertifiziert.

Literatur:

[1] Barthélémy, A. (2018). *Sicherheitslücken: Medizinische Geräte können gehackt werden*. Heise Online, 28.03.18. Online unter: https://www.heise.de/ newsticker/ meldung/Sicherheitsluecken-Medizinische- Geraete-koennen-gehackt-werden-4007227.html [13.04.18]

Enno Park:

Mein Implantat gehört mir

Bisher sind digitale medizinische Implantate und Prothesen geschlossene Systeme, die nicht oder nur geringfügig von Patienten selbst modifiziert oder programmiert werden können. Zumeist sind selbst für geringfügige Korrekturen an den Einstellungen aufwändige Besuche bei Orthopäde oder in Kliniken nötig, die sich oftmals über viele Termine und Kilometer hinziehen. Offene Systeme könnten erleichtern, dass Betroffene ihre Implantate oder Prothesen auf Wunsch selbst modifizieren und programmieren können. Dies entspräche einem Open-Source-Ansatz wie er in der IT seit langem bekannt und vor allem im Bereich von Serversystemen und Netzinfrastruktur Standard ist. Endnutzern bekannte Beispiele sind das Betriebssystem Linux oder der Browser Firefox, die nicht nur frei verwendet, sondern auch für neue Zwecke angepasst und nach Fehlern durchsucht werden können. Ein Open Source-Ansatz gesteht also den Nutzern/ Patienten im Sinne eines emanzipatorischen Menschenbildes mehr Autonomie und Eigenverantwortlichkeit zu. Ein freier Informationsfluss unterstützt hilft außerdem Patientengruppen dabei, sich intern gegenseitig zu unterstützen. Selbstverständlich können und sollen Do-It-Yourself-Ansätze nicht die bisherigen Strukturen ersetzen sondern nur ergänzen, schließlich kann längst nicht allen Patienten zugemutet werden, sich eingehend mit technischen Details zu befassen. Gerade bei jüngeren Patienten ist das Interesse allerdings sehr groß. Den Nutzern von Implantaten und Prothesen die Möglichkeit zu geben, ihre Geräte auf Wunsch selbst zu modifizieren, kann potenziell einiges an Kosten einsparen, fördert kreative Lösungen und „Hacks“ im Umgang mit Implantaten und Prothesen zu Tage und deckt Sicherheitslücken auf. Dabei sind Sicherheitslücken in körpernaher und

7. Abstracts 2. Tag

implantierter Technik umso kritischer je notwendiger Patienten auf diese Technik angewiesen sind. In der Medizintechnik fehlte bis zu einer Serie von spektakulären Hacks und Angriffen vielerorts das Bewusstsein für potenzielle Sicherheitslücken. Stichproben seitens des Cyborgs e.V. ergaben mehr oder weniger schwere Sicherheitslücken bei fast allen untersuchten Geräten. Allerdings ist das wahre Ausmaß des Problem nicht bekannt, da das Auftreten von Sicherheitslücken in digitalisieren Prothesen und Implantaten bisher nicht konsequent erforscht und statistisch erfasst wurde. Sollte sich der anfängliche Eindruck des Cyborgs e.V. bestätigen, besteht erheblicher Untersuchungs- und Handlungsbedarf. Die Herstellerfirmen im Gesundheitsbereich tendieren angesichts dieser Problematik derzeit weiterhin dazu ihre Systeme möglichst zu schließen und Quellcode oder Schaltpläne geheim zu halten. Diese Strategie hat allerdings in anderen Bereichen der Digitalisierung nicht vor Hacks und Angriffen geschützt. Viele IT-Experten empfehlen das Offenlegen von Quellcode und Konstruktionsplänen, damit nach dem Mehraugenprinzip Fehler gefunden und den Herstellerfirmen gemeldet werden können. Dieser Ansatz wäre auch in der Medizintechnik viel versprechend.

Session 4: EGK und EPA

Prof. Dr. Thomas Wetter

Wie die Informatik - zu Recht? - Grundfesten der Medizin erschüttert

Die Praxis der Medizin der letzten etwa 60 Jahre war, verkürzt gesagt, dadurch bestimmt, dass Erkenntnisse durch klinische Studien gewonnen werden und dass Ärzte diese Erkenntnisse auf Patienten anwenden. Beides wurde nicht grundlegend in Frage gestellt, obschon bei klinischen Studien keine Wahrheiten sondern nur gesellschaftlich akzeptierte positive Risikoabwägungen das Ergebnis sind und obwohl der Bürger in vielerlei anderer als medizinischer Hinsicht selbstbestimmt entscheidet und handelt. Die aktuelle Praxis ist also patriarchalisch, mit einerseits den Biometrikern und andererseits den Ärzten in den Rollen der Patriarchen.

Ein Patriarchat mit wohlwollenden Patriarchen führt nicht per se zu schlechter gesellschaftlicher Zufriedenheit und unzureichendem Nutzwert. Wenn allerdings Entwicklungen eintreten, welche die Nachhaltigkeit eines patriarchalischen Modells in Frage stellen, muss über Alternativen, deren Praktikabilität und moralischen Wert nachgedacht werden. Dies geschieht hier zunächst ohne Rücksicht auf die Konsequenzen immer umfangreicherer und ubiquitärerer Datenhaltung als Voraussetzung für diese alternativen Verfahren. Erst in einem zweiten Schritt wird dieser Aspekt hinzugenommen.

Neben prospektiven experimentellen Wirksamkeitsstudien nach Methoden der Biometrie (im Folgenden: klinische Studien) fördern inzwischen retrospektive Analysen großer Datenmengen nach Methoden der Informatik medizinische Einsichten zu Tage. Es wird deren Nutzwert im Vergleich zu dem klinischer Studien untersucht sowie ob nach Vorliegen eines entsprechenden Ergebnisses eine klinische Studie der empfohlene nächste Schritt zur Absicherung ist, oder aber moralisch obsolet, da ein Menschenexperiment zu einer nicht mehr offenen Frage.

Neben von Menschen erbrachten Gesundheitsdienstleistungen spielen Angebote durch digitale Medien und Kommunikationstechnologie eine immer größere Rolle. Neben vielen unzureichenden, wenn nicht inhärent gefährlichen, gibt es in klinischen Studien als effektiv nachgewiesene Dienste, die aber in vielen Fällen wegen des Fernbehandlungsverbots der ärztlichen Berufsordnung nicht in Routine gehen dürfen. Es wird der Nutzwert solcher Dienste untersucht, sowie ob die Berufsordnung noch zeitgemäß ist, oder aber moralisch obsolet, weil sie den Bürgern wertvolle Dienste vorenthält.

Bei diesen Analysen werden Maximen der medizinischen Ethik, die Beauchamp and Childress [1] zu breiter Anerkennung gebracht haben, sowie eine utilitaristische Abwägung als zulässige Werkzeuge vorausgesetzt. Mittels dieser Werkzeuge werden Positionen hergeleitet, welche nach Einschätzung des Autors eine Chance auf gesellschaftliche Akzeptanz haben. Dabei werden Argumente verwendet, die so erstmals in Wetter 2016 erschienen [2].

Ändern sich diese Positionen, wenn die breite Nutzung von digital gespeicherten Patientendaten und damit die Notwendigkeit von deren Schutz gegen missbräuchlichen Zugriff in die Argumentation einfließen muss? Auch dies wird nach Beauchamp und Childress analysiert, wobei ein Zitat eines Pioniers der deutschen Medizininformatik, Carl-Theo Ehlers, andeuten soll, welches Ergebnis die Zuhörer erwarten können: „Es gibt eines, das wichtiger ist als Datenschutz: Patientenschutz."

Literatur:

[1] Beauchamp, T.L. & Childress, J.F. (2013). *Principles of Biomedical Ethics*, 7. editierte Auflage. Oxford / New York: Oxford University Press

[2] Wetter, T. (2016). *Consumer Health Informatics. New Services, Roles, and Responsibilities*. Cham: Springer International Publishing

7. Abstracts 2. Tag

Session 5: Big Data in Health Care

Eva Schlehahn:

Cybersecurity und Dattenschutz im Gesundheitssektor: Konflikte und Synergien

Bereits 2013 gab es eine Stellungnahme des damaligen Europäischen Datenschutzbeauftragten (EDSB) Peter Hustinx zur vorgestellten Cybersicherheitsstrategie der Europäischen Union und zu der zu dem Zeitpunkt gerade vorgeschlagenen NIS Richtlinie (EU) 2016/1148. Unter Bezugnahme auf die europäischen Zielvorstellungen für eine bestmögliche Prävention und Bewältigung von Störungen und Cyberangriffen wies der EDSB schon damals darauf hin dass ein hohes Maß an Netz- und Informationssicherheit einen wesentlichen Beitrag zur Sicherstellung des Schutzes der Rechte natürlicher Personen auf Achtung der Privatsphäre und den Datenschutz in der Online-Umgebung leisten kann. Jedoch wies der EDSB in seiner Stellungnahme auch auf die Gefahr hin, dass manche Maßnahmen der Cybersicherheit durchaus einen Eingriff in die Rechte natürlicher Personen auf Schutz ihrer Privatsphäre und ihrer personenbezogenen Daten darstellen können, was letztlich einen Grundrechtseingriff bedeuten würde. Insoweit fordert die Stellungnahme, dass sicherzustellen ist, dass Maßnahmen im Cybersecurity-Bereich mit Artikel 52 Absatz 1 der Charta der Grundrechte der EU vereinbar sind und nicht zu einem unangemessenen Eingriff in das Recht auf Privatsphäre führen.
Im Kontext dieses durch die Stellungnahme angesprochenen Spannungsfeldes zielt der Vortrag darauf ab, ein grundlegendes Verständnis der Konfliktfelder von Cybersecurity und europäischem Datenschutzrecht zu vermitteln. Hierzu werden die elementaren Perspektiven, Zielvorstellungen und Grundprinzipien des europäischen Datenschutzrechts erläutert, um sowohl die Unterschiede als auch Gemeinsamkeiten im Hinblick auf Cybersecurity herauszuarbeiten. Spezifische Risiken der Datenverarbeitung im Gesundheitsbereich, insbesondere im Kontext von Big Data, werden hierbei beispielhaft herangezogen, um aufzuzeigen inwieweit eine datenschutzrechtliche Betrachtung das klassische Angreifermodell der IT-Security ergänzen kann. Hierbei wird das Standard-Datenschutzmodell als eine beispielhafte, aber bereits bewährte Methodik des Datenschutzes zur umfassenden Bestimmung von technischen und organisatorischen Maßnahmen vorgestellt. Auf diese Weise zeigt der Vortrag, warum ein Zusammenspiel zwischen dem organisationsinternen Datenschutzmanagement und dem IT Sicherheitsmanagement helfen kann, Schutzlücken aufzudecken und Verarbeitungsprozesse zu verbessern.

Max-R. Ulbricht:

Einwilligungsmanagement für Fitness-, Vital– und Gesundheitsdaten

Daten aus sogenannten "Wearables", wie Fitness-Trackern und Smartwatches, bieten sowohl Individuen als auch Institutionen vielfältige Möglichkeiten. Anfangs von Sport-Enthusiasten oder Anhängern der sogenannten "Quantified Self"-Bewegung genutzt, um durch die detaillierte Auswertung aufgezeichneter Bewegungsdaten sowie Vitalparameter -- wie Herzfrequenz, Körpertemperatur oder Hautwiderstand -- entweder das sportliche Leistungsvermögen zu verbessern oder aber gar die gesamte Lebensführung daran auszurichten, um gesundheitliche Aspekte positiv zu beeinflussen, sind entsprechende Geräte mittlerweile nicht nur gesellschaftlich etabliert, sondern haben eine signifikante Marktdurchdringung erreicht.
Mit der erhöhten Akzeptanz dieser Gerätekategorie entstanden über die vergangenen Jahre verschiedenste Geschäftsmodell und Anwendungsszenarien, welche auf Basis der generierten Daten Mehrwerte schaffen sollen. Im Bereich der Krankenversicherungen beginnen beispielsweise einige Anbieter nicht nur damit, Neukunden mit teils erheblichen Rabatten beim Neuerwerb eines entsprechenden Gerätes zu locken, sondern darüber hinaus Bonuspunkte für übermittelte Datensätze auszuloben, welche sich in Prämien oder vergünstigte Tarife umwandeln lassen. Spezialisierte soziale Netzwerke sprechen vor allem im Bereich Sport und Fitness die Träger von Wearables an, sich mit Gleichgesinnten zu vergleichen, die erreichten sportlichen Ziele zu veröffentlichen, um damit sich selbst und andere zu motivieren. Auch ernsthafte medizinische Studien wie zur frühzeitigen Erkennung von unregelmäßigem Herzschlag zur Vorbeugung von Herzinfarkten oder die Vorhersage von epileptischen Anfällen werden inzwischen mithilfe von Daten aus Fitness-Trackern und Smartwatches realisiert.
All diesen Anwendungsfällen gemein ist das Erfordernis des Teilens der aufgezeichneten Daten sowohl mit dem Hersteller des Gerätes als auch mit dem Anbieter des jeweiligen Dienstes bzw. der Institution, die der Träger unterstützen oder deren Angebote er nutzen möchte. Darüber hinaus lässt sich als weiteres Paradigma im Bereich des Internets der Dinge, zu welchem Wearables gezählt werden, beobachten, dass durch die (Re-) Kombination verschiedenster Datenquelle neue, innovative Dienste und Dienstleistungen entstehen. Beispiel-

7. Abstracts 2. Tag

haft sei hier ein Dienst zur Verknüpfung von Fitnessdaten mit sozialen Medien genannt, welcher es ermöglicht, bei Abschluss einer sportlichen Aktivität die zugehörigen Kennzahlen automatisiert über einen Kurznachrichtendienst zu veröffentlichen.
Für die skizzierten Nutzungsszenarien oder auch die Verknüpfung verschiedener Dienste ist die informierte Einwilligung oftmals die einzig zulässige Legitimationsgrundlage zur Datenverarbeitung. An diese sind enge rechtliche Vorgaben geknüpft, welche theoretisch dafür sorgen, dass sich z.B. bei der Weiterentwicklung eines Dienstes mit neuen Funktionen die ursprünglich angegebenen Zwecke der Datenverarbeitung ändern. Dies hätte zur Folge, dass mit jeder neuimplementierten Funktionalität eine neue Einwilligung zu einem neuen Verarbeitungszweck von allen Nutzenden einzuholen wäre. Deshalb tendieren Anbieter dazu, mit einem "broad consent" genannten Ansatz, initial in alle denkbaren aber auch unvorhersehbaren Datenverarbeitungszwecken einwilligen zu lassen, was rechtlich zumindest fragwürdig bleibt. Es muss aus Anbieterperspektive ständig eine Abwägung zwischen Rechtskonformität einerseits und Nutzungskomfort sowie Innovationspotential anderseits stattfinden.
Das im Vortrag vorgestellte Forschungsvorhaben hat es zum Ziel, oben genanntes Dilemma durch die Entwicklung technischer Infrastrukturen und Artefakte aufzulösen oder zumindest weitgehend zu entschärfen. Es werden bereits prototypisch entwickelte Komponenten und mögliche Architekturen vorgestellt, welche es im Kontext des Internets der Dinge ermöglichen können, Einwilligungen zu antizipierten Datenverarbeitungszwecken sowie potentiellen, datenverarbeitenden Institutionen als Präferenzen festzulegen, mit erhobenen oder zukünftig anfallenden Daten zu verknüpfen sowie die Einhaltung der Präferenzen technisch durchzusetzen.

Session 6: Kritische Infrastrukturen

Prof. Dr. Rainer Bernnat:

Kritische Infrastrukturen im Gesundheitswesen: Auswirkungen der zunehmenden Digitalisierung

Die Versorgung der Bevölkerung mit Gesundheitsdienstleistungen gehört zu den „Kritischen Infrastrukturen“, damit auch in Krisensituationen die Versorgung gewährleistet werden kann. Die Einrichtungen des Gesundheitswesens, wie z.B. Krankenhäuser, sind nur in begrenztem Maße auf Extremsituationen eingestellt, obwohl sie gerade in diesen Situationen gefordert sein können, besonders hohe Leistung erbringen zu müssen. Wenn diese Einrichtungen hinsichtlich des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien (IKT) keine ausreichenden Schutzvorkehrungen aufweisen, kann sich dies unmittelbar auf die Versorgung auswirken und Menschenleben gefährden.
Der Einsatz von IKT in den einzelnen Branchen des Gesundheitssektors ist sehr unterschiedlich ausgeprägt. Die Anforderungen – aber auch die Möglichkeiten – in Bezug auf IKT variieren, je nachdem, ob es sich um eine ärztliche Einzelpraxis, eine Apotheke mit Materialwirtschaftsfokus, ein Krankenhaus mit mehreren tausend Mitarbeitern oder einen internationalen Pharmakonzern handelt, sehr stark. Allerdings existieren auch einige sektorweite bzw. branchenübergreifende IKT-Initiativen. Sie dienen insbesondere dazu, den gesamten Sektor besser zu vernetzen, Transparenz zu schaffen und die Versorgungssicherheit zu erhöhen. An den Beispielen „Stationäre Versorgung“ und „Ambulante Versorgung“ wird dies exemplarisch deutlich:

- Für die stationäre Versorgung ist ein hohes Maß an IKT-Abhängigkeit festzustellen. Die IT-Durchdringung ist hierbei bei den einzelnen Krankenhäusern noch sehr unterschiedlich, insbesondere in Bezug auf den Grad der Nutzung elektronischer Patienten- und Fallakten. Neue technische Möglichkeiten, bspw. die zunehmende Verbreitung digitaler Patientenakten, der steigende Kostendruck und der demographische Wandel, werden diese Abhängigkeit auch weiterhin verstärken. Hinsichtlich der Resilienz ist eine große Robustheit festzustellen, zu der maßgeblich die flächendeckende Verteilung von Einrichtungen der Grund- und Regelversorgung beiträgt. Für den Bereich der Spezialbehandlungen, wie etwa Isolierstationen, Transplantationskliniken und (Supra-) Maximalversorger, kann eine höhere Kritikalität beobachtet werden. Ein Ausfall einer dieser Kliniken beeinträchtigt die Sicherstellung der Versorgung in signifikantem Umfang.
- In der ambulanten Versorgung besteht dagegen ein geringer Grad an IKT-Durchdringung. Da die Prozesse der Diagnose und Therapie noch immer mit eingeschränkter digitaler Unterstützung erfolgen, bedeutet ein Ausfall der IT i.d.R. kaum eine Einschränkung bei der Versorgung. Abgesehen von geräteintensiver Medizin (z.B. niedergelassene Radiologen), beschränkt sich der Einsatz von IT hauptsächlich auf Arztinformationssysteme primär für administrative Zwecke (Abrechnung, Dokumentation, etc.). Mit der Einführung und Weiter-

7. Abstracts 2. Tag

entwicklung der Telematik-Infrastruktur wird die IKT-Abhängigkeit jedoch deutlich zunehmen. Die ambulante Versorgung kann aufgrund der dezentralen Verankerung als robust charakterisiert werden. Ein Ausfall einer einzelnen Arztpraxis hat keinen Einfluss auf die Sicherstellung der Versorgung im Sinne kritischer Infrastrukturen.

Der Gesundheitssektor war bisher nur wenigen Angriffen oder Ausfällen ausgesetzt, deren Auswirkungen die Sicherstellung der Versorgung substantiell beeinträchtigt haben. Bei einem Großteil der Vorfälle wurden die Vertraulichkeit, in Form von Angriffen auf Patientendaten bzw. andere sensible Daten, oder die Verfügbarkeit, in Form von eingeschleuster Software, verletzt. Es gibt ebenso Vorfälle, die das Schutzziel Integrität betreffen, beispielsweise durch Manipulation von Grenzwerten oder Konfigurationen in der Medizintechnik (z.B. bei Infusionspumpen). Diese Angriffe sind als besonders kritisch zu erachten, da sie direkten Einfluss auf die Gesundheit (und das Leben) der Patienten haben können.
Mit zunehmender Durchdringung von IT und Digitalisierung im Gesundheitswesen kommt der IT-Sicherheit im Gesundheitswesen eine zunehmend wichtige Rolle zu. Hieraus ergeben sich konkrete Handlungsnotwendigkeiten, z.B. im Bereich IT-Sicherheit im Rahmen der Zulassung von Medizinprodukten, im Bereich der Einführung konkreter Verordnungen für den Gesundheitssektor auf Basis des IT-Sicherheitsgesetzes oder im Bereich des IKT-bezogenen Forschungsbedarfs, vor allem hinsichtlich einer vertiefenden Analyse der Branche Medizintechnik und der Branche Arzneimittel und Impfstoffe.

Dr. Armin Will:

Kritische Infrastrukturen und der Faktor Mensch: Mehr IT-Sicherheit durch Problembewusstsein und Sensibilisierung der Mitarbeiter

Infrastrukturen stellen im Krankenhaus immer mehr das Rückgrat der Funktionsfähigkeit dar.
Die Aufrechterhaltung der Verfügbarkeit der IT-Infrastrukturen wird durch umfangreiche Sicherungsmaßnahmen der IT-Abteilungen geleistet. Vielfältige technische Maßnahmen und Werkzeuge kommen zum Einsatz. Für die „gängigen" Risiken (Stromausfall, Netzwerkstörungen, Programmfehler/Fehlbedienung etc.) reichen diese zentralen Maßnahmen aus. Bei Cybergefahren kann der zentrale technische Schutz (ISMS, Firewall, Virenschutz, Backup etc.) aber nur bedingt allen Risiken begegnen.
Der Faktor Mensch und sein individuelles IT-Sicherheitsbewusstsein trägt, ggf. sogar entscheidend, zur IT-Sicherheit des Gesamtsystems bei. Unzureichendes Wissen bei Anwendern der IT-Infrastruktur um die eingesetzte Technologie, die möglichen Gefahren und resultierende Folgeschäden stellen ein Risiko für die IT-Sicherheit dar. Dieses mangelnde IT-Sicherheitsbewusstsein machen sich Angreifer zunutze. Trojanische Pferde und Social-Engineering – insbesondere Phishing – sind prominente Beispiele, bei denen mangelhaftes IT-Sicherheitsbewusstsein eines Benutzers gezielt ausgenutzt wird.
Mit dem BMBF-Projekt ITS.APT - IT-Security Awareness Penetration Testing wird am UKSH – erstmals wissenschaftlich fundiert und abgesichert – der Fokus auf den Faktor Mensch als potentielle Schwachstelle der IT-Infrastruktur gelenkt: Wie stark sind Mitarbeiter gegenüber Cybergefahren sensibilisiert? Mittels individueller Resonanzmessung wird in ITS.APT das Verhalten der Probanden anhand der von ihnen ergriffenen Handlungsoptionen gegenüber simulierten Cybergefahren ermittelt. Dabei bleibt für den Probanden die Testsituation verborgen, da die Tests während seiner normalen Tätigkeit am PC – im laufenden Betrieb – erfolgen. Auf der Basis dieser individuell ergriffenen Handlungsoptionen und der Korrelation mit personalisierten Fragebögen, welche im Nachgang der Test den Probanden angeboten werden, lässt sich der Grad der IT-Security-Awareness der Mitarbeiter ableiten. Im Rahmen des Projektes erfolgen auf Basis der erhobenen Daten gezielt fokussierte Schulungen zur Stärkung des IT-Sicherheitsbewusstseins. In einem erneuten Testdurchgang wird der Erfolg der Schulungsmaßnahmen validiert.

Impressum

Institut für Sozialforschung und Technikfolgenabschätzung (IST)

Ostbayerische Technische Hochschule Regensburg (OTH)

Seybothstraße 2

93053 Regensburg

Prof. Dr. Karsten Weber

karsten.weber@oth-regensburg.de

Nadine Kleine M.A.

nadine.kleine@oth-regensburg.de

Weitere Informationen zum Institut für Sozialforschung und Technikfolgenabschätzung (IST):

www.oth-regensburg.de/ist