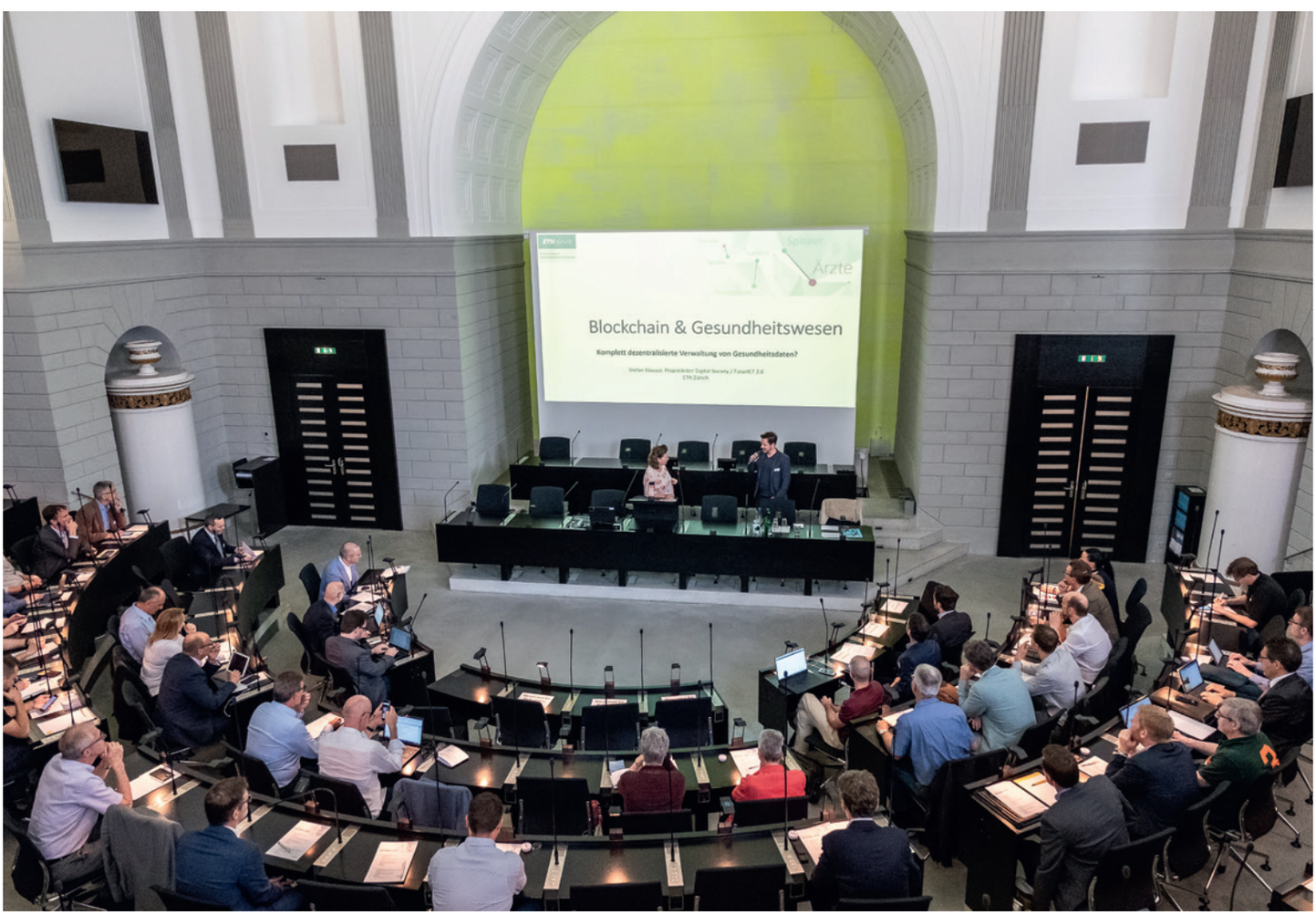
Spannendes MediData EDI-Podium 2018 – Blockchain, Cyberkriminalität, Digitale Transformation und die Zukunft der Gesundheit

Klarer Blick nach vorne – unser Gesundheitswesen besser gestalten

Am zwölften MediData EDI-Podium im Luzerner Kantonsratssaal trafen sich rund hundert Teilnehmende aus allen Bereichen des Gesundheitswesens für den aktiven Dialog über aktuelle Themen der Zeit. Welche Gefahren drohen uns durch kriminelle Machenschaften in der Cyber-Welt? Wie halten wir mit der digitalen Revolution Schritt und wie nutzen wir sie? Wie organisieren wir das Gesundheitswesen 2030? Sind Computer klüger als Menschen?

Das EDI-Podium ist eine jährliche Veranstaltung von MediData mit Sitz in Root D4. Vertreterinnen und Vertreter von Leistungserbringern, Kantonen, Versicherern und Verbänden aus der ganzen Schweiz nutzten erneut die Gelegenheit zu einem Erfahrungs- und Wissens-Austausch unter Spezialisten.

Dieses Jahr vermittelten Top-Referenten eine Vielzahl von Impulsen zum Thema «Informationssicherheit, Blockchain, Digitale Transformation und die Zukunft der Gesundheit». Virtuos führte Nicole Westenfelder, Journalistin und Moderatorin, durch das Programm, das die Teilnehmenden sichtlich fesselte.



Das Dutzend voll gemacht: Daniel Ebner, CEO, freut sich, eine grosse Schar von BesucherInnen zum 12. EDI Podium begrüssen zu können.

Hacker – ein enormes Gefahrenpotenzial

Marc Ruef, Head of Research, Member of the Board von scip AG, eröffnete das Podium zum Thema «Cyberkriminalität» mit dem Statement «Virtueller Tod am Krankenbett». – Heute würden Patientendaten weitherum angeboten wie gestohlene Daten über Bankkunden. Hacker schaffen aber noch weitere Gefahren. Sie greifen in die Patientenversorgung ein. Den Verbrechern gelingt es, Anzeigen von Überwachungsgeräten zu manipulieren, Alarme auszuschalten, wenn kritische Parameter zum dringenden Eingreifen rufen würden, oder Infusionen zu verändern und damit Leib und Leben von Patienten zu gefährden. Der erfahrene Sicherheitsexperte ist besorgt, wie relativ einfach bestimmte medizintechnische Geräte fremdgesteuert werden können und damit auf Vitalparameter und weitere Patientendaten Zugriff genommen wird. Als Motive für die kriminellen Handlungen nannte Ruef Anerkennung, Verteidigung, Macht und Geld.

Sechs hauptsächliche Angriffsziele

Der Referent wies auf sechs wesentliche Gebiete hin, in denen ein Darknet, ein Internet dunkler Machenschaften, besteht und wo Daten und verbotene Produkte angeboten werden:

- Drogen: Hier wird die ganze Bandbreite von (teilweise gefälschten oder qualitativ minderwertigen) Medikamenten und Drogen angeboten.
- Waffen: Verschiedene illegale, gestohlene oder modifizierte Waffen können erworben werden.
- Services: Dienstleistungen aller Art bis hin zum Auftragsmord können bestellt werden. Länderweise bestehen sehr grosse Preisunterschiede.
- Pornografie: Material unterschiedlichster Ausprägung steht zur Verfügung.
- Software: Illegal kopierte, frühzeitig publizierte oder modifizierte Software wird gehandelt.
- Filme, Musik, Bücher, Comics und andere publizistische Erzeugnisse: Sie werden unter Ausschaltung von Urheber- und Lizenzrechten weitergereicht.

Geldgier ist der grösste Auslöser für Cyberkriminelle. Der Experte schätzt den Anteil des Drogenbereichs auf 15% aller Darknet-Geschäfte, Betrug und Manipulation von Märkten erreichen je 9% und das neue Element Bitcoin schafft es erstaunlicherweise bereits auf über 6%. An Preis-Beispielen nannte Ruef 38 Dollar für einen Scan eines Schweizer Passes, 7800 Dollar für ein Baby aus China und 400 000 Dollar für einen ausgewachsenen Gorilla. Der Phantasie und Skurilität sind kaum Grenzen gesetzt. Begehrte Handelsobjekte sind insbesondere auch Zugriffsdaten zu Android-Services oder Unternehmens-Servern.

Gegensteuer und Bewusstseinsbildung

Researcher und Behörden bemühen sich natürlich, den ungebetenen Aktionen Paroli zu bieten, stossen aber an ihre Grenzen. Technologie, Psychologie und Recht reichen allesamt häufig nicht aus, erfolgreich Gegensteuer zu geben. Unternehmen wie die scip AG beraten internationale Kunden, die auf das breite Know-how im Bereich der Informationssicherheit zurückgreifen. Die Spezialisten und Teams der scip AG überzeugen in ihren Fachbereichen von technischen Sicherheitsüberprüfungen über konzeptionelle Unterstützung bis hin zu umfangreichen Forschungsaufträgen. Sie analysieren spezielle Bedürfnisse ihrer Kunden im Rahmen vielschichtiger Projekte.

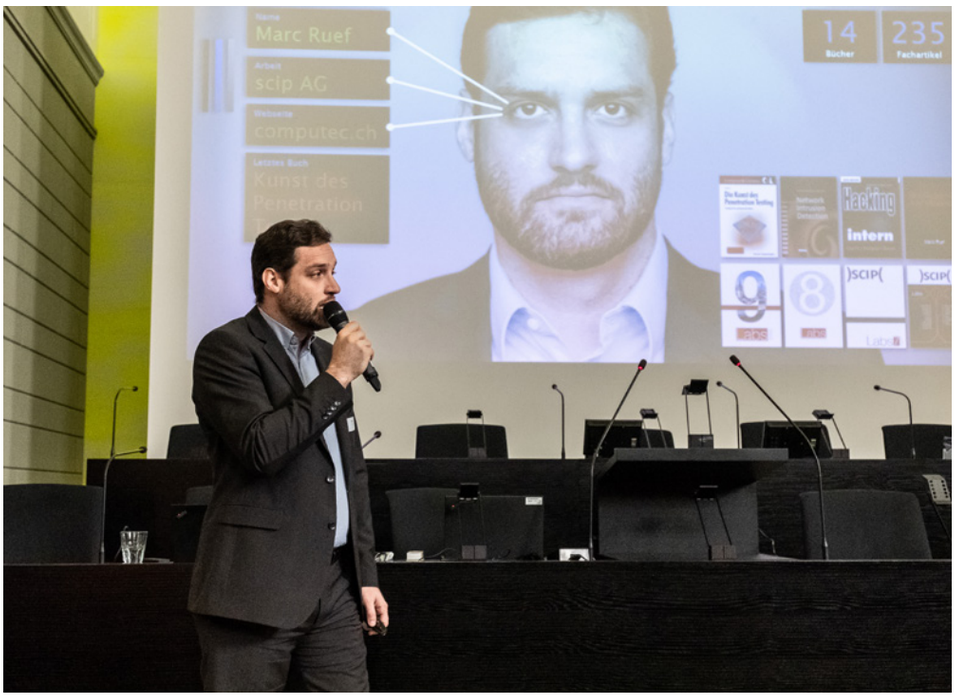
Die erfahrenen Fachleute weisen insbesondere Hersteller von Medizintechnik-Geräten auf das relative einfache Hacken hin. Die Praxis zeige allerdings, so Ruef, dass bei den betroffenen Firmen statt Technikern eher Anwälte auf den Plan gerufen würden und es bis zu 2½ Jahre daure, bis die festgestellten, oft gravierenden Mängel behoben seien. Es bleibe also noch viel zu tun, bis das Bewusstsein für eine höchstmögliche Datensicherheit stark genug entwickelt ist.

Im Universitätsspital ist Sicherheitsproblematik besonders komplex

Im Alltag von Thomas Friedli, Chief Information Security Officer & ICT-Riskmanager des Inselspitals, spielt Cyber Security eine enorme Rolle. Mit dem Referat zum Thema «Wenn Hacker bei der Patientenbehandlung ‹unterstützen›» unterstrich er die gefährliche Tragweite der Machenschaften krimineller Kreise.

Friedli zeigte anhand einer Studie von WhiteScope aus dem Jahr 2017, dass alleine schon mehr als 8000 Schwachstellen in der Software von Herzschrittmachern vorhanden sind. Eine ebenfalls 2017 erstellte Studie weltweit kam zum Ergebnis, dass viele implantierte Defibrillatoren unterschiedlicher Hersteller Sicherheitslücken in der Kommunikationssoftware aufweisen.

Weiter berichtete Trend Micro im Mai 2017 von über 36 000 Medizintechnik-Geräten, welche alleine in den USA über die IoT-Suchmaschine «Shodan» zu finden waren. Ebenfalls im Mai 2017 kam eine Studie zur Erkenntnis, dass nur ein Drittel der Hersteller von medizinischen Geräten sich der potenziellen Risiken, die ihre Produkte beinhalten, bewusst ist. Und noch gefährlicher: Nur gerade 17 Prozent dieser Hersteller leiteten daraufhin signifikante Schritte ein, um Angriffe zu verhindern respektive um Risiken von Hacker-Angriffen zu minimieren. Friedli mahnte: «Man kann das Risiko nicht weg ignorieren.»



Marc Ruef, Head of Research scip AG, sprach mit viel Herzblut über die grossen Gefahren von Hackerangriffen im Gesundheitswesen.

Das Gesundheitswesen ist zum Haupt-Angriffsziel geworden

Geraten auch Spitäler vermehrt in den Fokus von Cyber-Kriminellen oder richten sich die Augen der Verbrecher eher auf Banken und andere Branchen? – Mitnichen: Im Jahr 2014 stand der Gesundheitssektorstand noch nicht auf der Rangliste der häufigsten angegriffenen Branchen – jedenfalls nicht unter den Top 5. Das hat sich rasch geändert. Bereits im ersten Quartal 2016 war die Gesundheitsbranche das beliebteste Angriffsziel von Cyber-Kriminellen (noch vor der Finanzwirtschaft und der Fertigungsindustrie).

Davor bleibt auch unser Land nicht verschont: 2016 registrierte die Gesundheitsbranche 64 % mehr schwere Cyber-Angriffe als 2015. «Dieselbe Studie zeigt leider auch, dass rund 50 % der Angriffe durch ‹Insider› ausgeführt werden wie ehemalige Angestellte oder frustrierte Mitarbeitende, welche Daten verkauften oder Systeme manipulierten», erläuterte Friedli, «und die Studie zeigt weiter, dass die meisten Sicherheitslücken bei den Medizintechnik-Systemen zu finden sind.»

Unumgänglich: eine umfassende Sicherheitsstrategie

Sich kompetent zu rüsten, Sicherheitslücken zu schliessen und eine umfassende Datenschutzstrategie zu fahren, ist mehr denn je angezeigt, weil auf die Spitäler, insbesondere Uni- und Zentrumsspitäler, grosse digitale Herausforderungen zukommen. Die Top Trends im Spital sind Virtual Reality und Augmented Reality, Künstliche Intelligenz sowie IoT(Internet of Things). Die Datenvielfalt und -menge wird also schon in absehbarer Zeit weiter massiv und verstärkt ansteigen. Die Angriffsflächen werden nicht kleiner und der Appetit der Gauner sicherlich auch nicht.

Internet of Things Botnet

Der Experte verdeutlichte: «Das IoT wird erst vereinzelt auf Schwachstellen hin untersucht; die ersten Botnets sind jedoch schon da!» So infizierte Mirai Botnet IoT-Geräte für eine «Zombie Armee». Dabei gelang es, während dieses Tests 100 000 Medtech-Systeme in nur 24 Stunden zu infiltrieren. 83 % der IoT-Geräte sind anfällig. Eine Infektion ist ausserdem schwer festzustellen, da der Schadcode im Memory liegt. DDos-Attacken von infizierten Geräten wurden bereits mehrfach ausgeführt.»

Unter DDoS (Distributed Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören. Im Gegensatz zur einfachen DoS-Attacke erfolgt der Angriff bei DDoS von vielen verteilten Rechnern aus. Der Angriff kann dabei auf Netzwerkebene, auf Anwendungsebene oder eine Kombination davon erfolgen. In der Regel werden für solche Attacken sogenannte Botnets (eine riesige Anzahl «gekaperter» Systeme, die vom Angreifer ferngesteuert werden können) oder schlecht konfigurierte Drittsysteme (z.B. Open DNS Resolver) verwendet, die durch manipulierte Anfragen dazu gebracht werden, grosse Antworten an die «falsche» Adresse – nämlich die des kriminellen Zielsystems – zu schicken.

Die Anforderugen steigen gewaltig

Die Zahl der IoT-Geräte wird in den nächsten Jahren stark anwachsen. Es ist also höchste Eisenbahn, sich und die zu behandelnden Patienten ausreichend und systematisch zu schützen. Das beginnt vor allem bei der Medizintechnik. So ist es ohne ausreichenden Schutz möglich, innert 3 Minuten die Daten einer programmierten Spritzenpumpe zu knacken. Die Schwachstelle besteht darin, dass das Admin-Passwort meist fix hinterlegt und im Internet zu finden ist. Eine Manipulation könnte im Ausschalten oder Verändern der Dosierung bestehen.

Noch schneller ist eine Manipulation eines Patientenmonitors möglich. Hier sind nur gerade 2 Minuten nötig, um über die häufige Schwachstelle Human-Error Zugriff zu nehmen. Oft wird der Monitor an eine falsche Security Zone angeschlossen, was ein Ausschalten oder Verändern der Werte zulässt. Friedli nannte als weiteres Beispiel, bei dem die Informationssicherheit aufwändig zu realsieren sei, den Da Vinci-Roboter, weil hier Steuerung und Überwachung im gleichen Raum erfolgen. Solch ausgeklügelten Operationstechniken gehört allerdings die Zukunft. Sicherheitsexperten sind sehr gefragt.

Ein Ablaufdatum für Medtech-Produkte

Thomas Friedli zog ein Fazit: «Warum erhalten medizintechnische Systeme nicht auch ein Ablaufdatum wie sämtliche medizinischen Produkte? Dann dürften diese nicht mehr eingesetzt werden, falls kein aktuelles Betriebssystem installiert oder keine Sicherheits-Updates gemacht wurden. Und warum entwickeln Hersteller von Medtech-Geräten nicht endlich sichere Software auf aktuellen Betriebssystemen? Wollen wir in Zukunft sichere Medizin anbieten können, müssen wir einige Punkte kritisch hinterfragen. Dazu gehört auch, dass Regulierungen/Normen so gestaltet sein sollten, dass aktuelle Betriebssysteme und das regelmässige Einspielen von Sicherheits-Updates als zwingende Voraussetzung bei der Herstellung und beim Betrieb von Medizintechnik-Geräten gefordert wird.»

Blockchains verändern die Welt

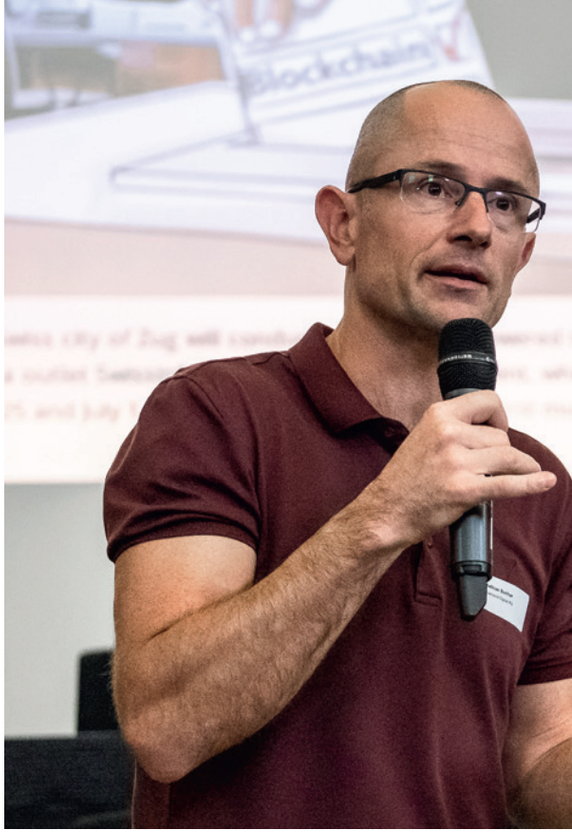
Blockchain – das Wort ist in aller Munde. Doch was ist Blockchain? Was kommt auf uns zu? Was wird Blockchain verändern? – Stefan Klauser, Projektleiter Digitale Gesellschaft, ETH Zürich, Professur für Computational Social Science COSS, präsentierte mit dem Referat «Das Potenzial von Blockchain im Gesundheitswesen».

«Spitäler müssen sich gut rüsten gegen die Cyberkriminalität», ist Thomas Friedli, Information Security Manager des Inselspitals, überzeugt.

Bei Blockchains handelt es sich um spezielle Datenbanken, die Transaktionsdaten zwischen Partnern verwalten, die Informationen, Produkte oder Dienstleistungen untereinander austauschen. Dies erfolgt ohne eine zentrale Kontrollinstanz und mit vollkommener Transparenz. Blockchain funktioniert daher wie ein umfassendes Journal von Transaktionen: Sobald zwischen einem Absender und einem Empfänger eine Datei übermittelt worden ist, wird im digitalen Journal eine neue Position, ein Datenblock, eingetragen. Und das Entscheidende ist: Tausende von Kopien dieser Transaktion liegen nun auf Computern rund um den Erdball. Jeder Datenblock wird an die früheren angekettet, daher auch der Ausdruck «Blockchain». Gespeichert sind die Ketten auf privaten Computern ebenso wie auf Servern von Unternehmen.

Sobald eine neue Transaktion eingetragen wird, erscheint diese Position überall und wird von den Speichern, auf denen die Interaktionen gespeichert sind, authentifiziert. Erst jetzt ist eine Transaktion auch gültig. Jedes Detail ist für immer unveränderlich festgehalten und von einer Riesenzahl von Computern authentifiziert.

Aus diesem Grund gelten Transaktionen, die über eine Blockchain abgewickelt werden – im Vergleich zu herkömmlichen Transaktionssystemen – als praktisch fälschungssicher und daher vertrauensbildend, weil die Kontrolle über durchgeführte Transaktionen in der Hand von vielen liegt und nicht bloss in der Hand eines Akteurs



MediData – für eine gesunde Entwicklung im Schweizer Gesundheitswesen

MediData ist ein massgebender Informatik-Dienstleister – mit der Vision, sich für eine gesunde Entwicklung im Schweizer Gesundheitswesen einzusetzen und dank digitalisierter Prozesse die Zusammenarbeit zwischen Leistungserbringern, Versicherern, Kantonen sowie Patienten voranzutreiben. Das MediData-Netz ist die umfassendste Datenaustauschplattform für Healthcare Professionals in der Schweiz – für den effizienten und sicheren Austausch medizinischer und administrativer Daten.

www.medidata.ch

wie beispielsweise einer Bank. Interessant ist jedoch, dass die Transaktionsteilnehmer anonym bleiben können – es sei denn, sie möchten sich zeigen. Das bedeutet, dass Zahlungen via Blockchain nicht direkt und persönlich erfolgen, sondern über einen elektronischen Briefkasten, «Wallet» genannt. Die Adresse eines Wallets kann nicht einfach einer Person oder einer Firma zugeordnet werden, alle können zudem mehrere Wallets betreiben.

Prozesse wirtschaftlicher, schneller und einfacher abwickeln

Mit Blockchains geraten wir in die Lage, bestehende und auch neu zu bestimmende Prozesse wirtschaftlicher, schneller und einfacher abzuwickeln. Das wohl bekannteste Beispiel für eine Blockchain ist jenes mit der Internetwährung Bitcoin. Die Bitcoin-Blockchain ist die grösste öffentliche Blockchain. Noch sind Kryptowährungen wie Bitcoins oder Ether die auffallendsten Blockchain-Anwendungen, aber es werden viele andere folgen, gerade auch im Austausch von Gütern. Das liegt insbesondere daran, dass durch die digitale Konstruktion einer Blockchain die Unveränderbarkeit der Daten sichergestellt ist. So kann also nachvollzogen werden, wann, warum und wie eine neue Position in all den beteiligten Computern und Servern gespeichert wurde. Digitale Besitzrechte sind eindeutig feststellbar und Original und Kopie eines Datensatzes können ebenso klar voneinander unterschieden werden.

Stefan Klauser erwähnte interessante Beispiele für Blockchain-Anwendungen. Dazu könnte eine lückenlose Rückverfolgung einer Transport-Kühlkette gehören, bei der – etwa für Medikamente – nachgewiesen werden kann, dass keinerlei Störungen oder Unterbrüche zwischen Start- und Zielort stattgefunden haben. Eine bereits praktizierte Umsetzung ist weiter die über Bitcoins abgegoltene Beteiligung von Informationslieferanten für Studienprojekte, die zur sicheren Authentifizierung und Abwicklung via Blockchain realisiert ist. Hierbei, und das ist ein weiteres wichtiges Element, kann (wie bei andern angezeigten Fällen sensibler Daten) der eigentliche Inhalt der Transaktion so gestaltet sein, dass er nur für einen definierten Nutzerkreis ersichtlich ist. Das ist gewissermassen der «Fünfer und das Weggli» – erstklassig abgesicherte Transaktion und Schutz der persönlichen Identität.

Blockchain kann für die Gesellschaft und die Konsumenten viel verändern. Stefan Klauser, Projektleiter Digitale Gesellschaft an der ETHZ, präsentiert Use Cases.

Den Einsatz der Blockchain-Technologie im Gesundheitswesen sieht der Referent positiv. Er kann sich insbesondere eine Anwendung im Rahmen des elektronischen Patientendossiers vorstellen. Risiken ergeben sich nach seiner Einschätzung bei zentral verwalteten Daten, das sei hier gerade nicht gegeben, weshalb die Risikoabschätzung positiv ausfalle.

Die Stadt Zug setzt Zeichen

Anhand eines bereits umgesetzten und erfolgreichen Projekts zeigte Dr. Mathias Bucher, Dozent für Blockchain Technologie, CEO Diamond Digital AG, die entscheidenden Details mit seinem Referat «Blockchain Technology and its Application for Digital Identities».

Fortschrittlich ist die Stadt Zug. Hier startet im Juli die Blockchain-basierte digitale ID für alle Einwohner. Nach der erfolgreichen Testphase und der finalen Entwicklung bietet Zug allen EinwohnerInnen die Möglichkeit, dieses moderne IT-Tool zu nutzen. Die digitale ID basiert auf einer

Fortschrittliches Zug: In dieser Stadt wurde die Blockchain-Identität eingeführt. Dr. Mathias Bucher, Dozent für Blockchain-Technologie und CEO der Diamond Digital AG, stellt die Lösung vor.

App und ist mit einer Ethereum-Blockchain verknüpft. Die EinwohnerInnen können sich in wenigen Schritten über die Website der Stadt und eine App registrieren. Anschliessend geht man kurz bei der Einwohnerkontrolle persönlich vorbei, um sich seine Daten bestätigen zu lassen.

Digitale Personendaten sind üblicherweise auf zentralen Servern gespeichert – und können gestohlen werden. Die Stadt Zug geht daher einen anderen Weg und stellt die NutzerInnen ins Zentrum. Sie allein verwalten die persönlichen Daten ihrer Identität, weil diese weder zentral noch im Internet gespeichert werden, sondern verschlüsselt auf dem eigenen Mobiltelefon. Ohne Einwilligung der Benutzer verlassen keine Daten das persönliche Mobile. Jeder ist so sein eigener Datenschutz-Beauftragter.

Sicherheit hoch drei

Die digitale ID der Stadt Zug besteht aus drei Elementen:

- Erstens: ein **digitales Schliessfach**. Dieses befindet sich auf dem Mobiltelefon der Benutzer in einer App, biometrisch oder durch einen PIN gesichert. In dieser App wird die digitale ID nach dem Registrierungsprozess abgespeichert.

- Zweitens: die **Ethereum-Blockchain**, eine Art dezentrale Datenbank. Die App erstellt in der Blockchain eine eindeutige und unveränderbare Kryptoadresse und verknüpft diese mit dem digitalen Schliessfach auf dem Mobiltelefon des Nutzers. Diese Adresse ist einmalig und kann nicht gefälscht oder repliziert werden.

- Drittens: das **Zertifizierungsportal**. Dieses liegt bei der Einwohnerkontrolle der Stadt Zug. Nach dem Abschluss der Registrierung haben die User zwei Wochen Zeit, um bei der Einwohnerkontrolle persönlich vorbeizugehen. Hier überprüfen die Mitarbeitenden die Identitätsangaben, die über den Registrierungsprozess eingegeben wurden: Vorname, Name, Geburtsdatum, Heimatort/Staatsangehörigkeit, Nummer von Pass oder Identitätskarte. Für diese Überprüfung muss man sich mit dem Pass oder der Identitätskarte ausweisen. Mit der Bestätigung durch die Einwohnerkontrolle werden alle Identitätsangaben mit dem Kryptoschlüssel der Stadt Zug aus der Blockchain signiert und in Form eines digitalen Zertifikats verschlüsselt im digitalen Schliessfach der App auf dem Mobiltelefon des Nutzers gespeichert.

Kreative Umsetzungen folgen

Die digitale ID in Zug befindet sich in der Pilotphase. Verschiedene konkrete Anwendungen für entsprechende Dienstleistungen sind in Evaluation, so z.B. ein einfacher Zugang zu allen elektronischen Behördendienstleistungen, ein Blockchain-basierter Fahrradverleih, ein digitalisiertes Parking-Management oder das Ausleihen von Büchern ohne Bibliotheksausweis.

An der Entwicklung und Implementierung der digitalen ID der Stadt Zug beteiligt waren das Institut für Finanzdienstleistungen Zug (IFZ) der Hochschule Luzern – Wirtschaft, die Firmen Consensys-uPort (Zug) und ti&m (Zürich) sowie die IT-Abteilung der Stadt Zug. Die Kontaktstelle Wirtschaft des Kantons Zug leistete wertvolle Koordinationsarbeit.

Digitale Transformation – die Zukunft ist heute

Kamales Lardi, Founder & Managin Partner, Lardi & Partner Consulting GmbH / Expert in Digital Transformation, Business Model Innovation & Social Media und Autorin, begeisterte die Teilnehmendem für das Thema «Digital Transformation» mit Ihrem Referat «End of Business As Usual: Digital Transformation in the Business Landscape».

Weltweit findet eine währschafte digitale Disruption statt. Wie wir uns darauf einstellen können, weiss Kamales Lardi, Founder & Managing Partner, Lardi & Partner Consulting.

«Die weltweiten Ausgaben für die digitale Transformation werden 2019 die Summe von 1.7 Trillionen Dollar erreichen», begann die Referntin. Entscheidende Elemente sind dabei zu beachten:

- eine Konvergenz der Enabler: leistungsstärkere IT-Systeme, unlimitierte Archivkapazitäten, globale Vernetzung und Zugänglichkeiten, sinkende digitale Betriebskosten und Zunahme von Clouds
- bahnbrechende Technologien, die noch bestehende Begrenzungen aufheben werden: Künstliche Intelligenz, IoT, Blockchains, AR/VR
- vernetzte Konsumenten, die klare Präferenzen äussern, und Technologie-versiert, anspruchsvoll, miteinander verbunden, proaktiv und engagiert sind
- neue kompetitive Landkarte: wachsende Anzahl Startups, die Konsumentennähe entwickeln, vermehrte vertikale Integration und Industrie-übergreifender Wettbewerb, dies insbesondere durch globale Unternehmen wie Google, Amazon, Apple, Microsoft usw.
- sich wandelndes globales Eco-System: Medizintourismus, Herausforderung älter werdende Gesellschaft und damit verbundene Kosten, mobilere und digital unterstützte Fachkräfte, die gerade im Gesundheitswesen sehr umworben sind
- regulatorische Veränderungen: Notwendigkeit zum Schutz der Privatsphäre und des Datenschutzes, Sicherstellen der Cyber Security, Bewältigen neuer Krankheitsformen wie Facebook-Depression oder Spielsucht

Steigende Erwartungen, neue Business-Modelle

Die neuen technologischen Möglichkeiten lassen die Erwartungen der User ansteigen. Kamales Lardi erwähnte die «vier P»: Digitalisierung soll personalized, preventative, perdicitive und participatory sein. – Digitalisierung wird insbesondere auch disruptive Auswirkungen zeitigen. So werden sich die Konsumentenerfahrungen verändern. Die Konvergenz von digitalen und physischen Kontakten wird zu einer besseren Versorgung im Gesundheitswesen führen. Die Digitalisierung und der Einsatz neuer Technologien werden Produkte und Dienstleistungen hervorbringen, die den Bedürfnissen der Konsumenten besser entsprechen. Optimierte, automatisierte Verfahren werden die Effizienz von Geschäftsprozessen steigern und die Zukunft von Arbeitsplätzen und -kultur beeinflussen. Schliesslich, so Lardi, würden aufgrund disruptiver Markttrends neue Chancen und Business-Modelle entstehen. «Es ist ein End of Business as Usual.»

Durchstarten für die digitale Transformation

Der Zeitpunkt für den Start in die digitale Transformation sei jetzt. Es gelte, Innovationen zu orten und zu nutzen, die entscheidenden Elemente dynamisch zu entwickeln und die künftige Geschäftsentwicklung zu optimieren. Daraus folge eine Checkliste mit drei wichtigen Punkten:

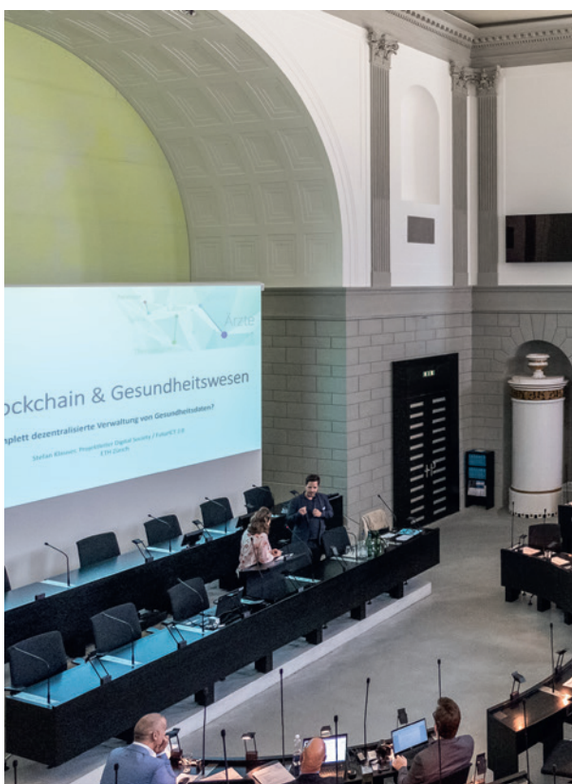
- **einen digitalen Gesundheitscheck erstellen**: Auswirkungen von Trends, disruptiven Technologien, Verbraucherverhalten bewerten, bestehende Abläufe und Herausforderungen überprüfen
- **Entwickeln einer digitalen Strategie und Roadmap**: Erforschen neuer Möglichkeiten zur Optimierung, Weiterentwicklung und Innovation, Kreation hochwertiger digitaler und physischer Konsumentenerfahrungen, Entwicklung einer Roadmap für Projekte zur digitalen Transformation
- **Aufbau und Optimierung**: Pilotprojekte zur Bewertung von Werten und Renditen, Aufbau und Einführen von Projekten auf der Basis bewährter Best Practices

Wie managen wir morgen unsere Gesundheit?

Zum Abschluss vermittelte Georges T. Roos Einblick in die Zukunft mit seinem Referat «Die Zukunft der Gesundheit. Die Perspektive eines Zukunftsforschers». Unmissverständlich lautete sein Einstieg: «Unsere Gesellschaft wird in 20 Jahren völlig anders aussehen.»

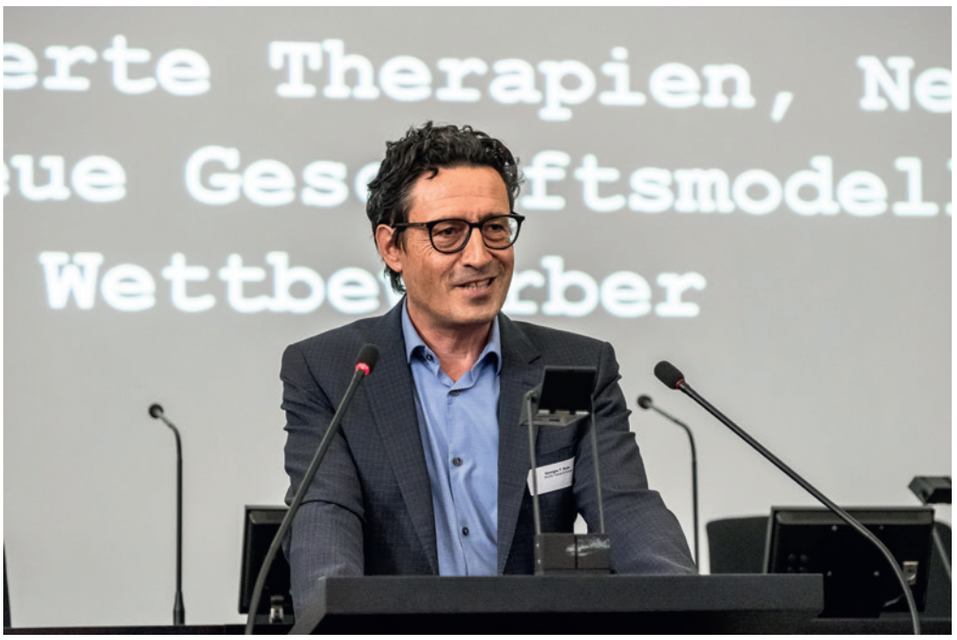
Wir befänden uns heute in der dritten Gesundheitsrevolution, bemerkte Roos:

- Die erste Gesundheitsrevolution vor 150 Jahren sicherte durch öffentliche Gesundheitsmassnahmen das Überleben und mündete in einer signifikant gestiegenen Lebenserwartung.
- Die zweite Gesundheitsrevolution sieht z.B. Prof. Ilona Kickbusch im Schaffen solidarisch organi-



sierter Finanzierungssysteme für das Gesundheitswesen, durch welche die Errungenschaften der Medizin allen Menschen (in den entwickelten Ländern) zugänglich gemacht wurden.
– Die dritte Revolution ist nun im Gang: Gesundheit ist zu einem zentralen persönlichen, politischen und ökonomischen Faktor geworden, der unseren sozialen Alltag auf vielfältige und widersprüchliche Weise durchdringt.

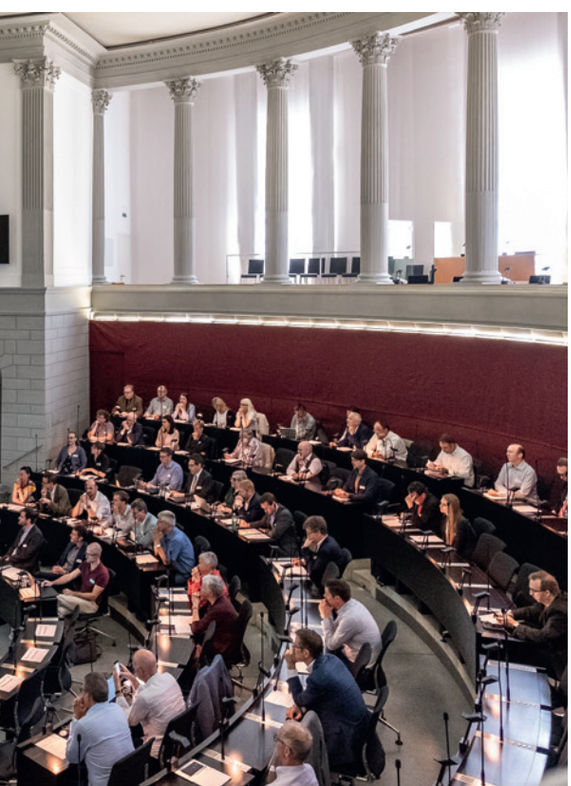
Entscheidende Beiträge an die Gesundheitsversorgung leisten die rasant wachsenden digitalen Möglichkeiten. Sie führen erstens dazu, riesige Datenmengen systematisch und immer günstiger auszuwerten, weil ein eigentlicher Preiszerfall bei der Sequenzierung abläuft. Dadurch entsteht ein gewaltiger Wissenszuwachs, gerade im Bereich der Gentechnologie, sei es doch mittlerweile bekannt, dass 4000 Krankheiten mit dem Erbgut zu tun hätten.



Tiefgreifende Umwälzungen, so Zukunftsforscher Georges T. Roos, ROOS Trends & Futures, kommen auf uns zu. Chancen und Gefahren sind zu orten, es wird höchst spannend.

Und plötzlich sind die Maschinen sehr intelligent

Ein weiterer Einflussfaktor ist, dass Maschinen angefangen haben, zu lernen und Sprachfähigkeit zu entwickeln. IBM Watson ist bereits imstande, innnerhalb einer Sekunde 800 Millionen A4-Seiten Text zu analysieren. Daraus werden Muster erkannt, Hypothesen gebildet und überprüft. Computer sind bereits fähig, aufgrund Künstlicher Intelligenz Debatten zu führen. Die digitalen Tausendsassas sind auch unheimlich exakt. Roos präsentierte ein Beispiel einer deutschen Restschuld-Versicherung, bei der regelmässig Rechtsfälle entstehen. So bewältigte während eines Monats ein Compter 23000 solch relativ standardisierter Fälle, im gleichen Zeitraum erledigten die Hausjuristen nur 750 Fälle. Die digitale Intelligenz ergab eine Trefferquote von 84 % gleichbleibender Beurteilung von an den Ombudsmann weitergezogenen Fällen, die Juristen schafften bloss 62 %.



Im Gesundheitswesen sind natürlich vorausschauende Beurteilungen oder direkte Einflussnahmen für die positive Entwicklung der Gesundheit oder die Linderung einer Krankheit von ausschlaggebender Bedeutung. Spezielle Applikationen sind heute schon in der Lage, einen Epilepsie-Anfall aufgrund relevanter Parameter sechs Stunden im Voraus zu prognostizieren. In der genetischen Medizin wird an der «molekularen Schere» gearbeitet, welche die Funktionsweise von Genen beeinflusst und sie ein- und ausschalten sowie blockieren oder aktivieren kann.

Höchst interessant sind weiter Roboter-unterstützte Bewegungshilfen und in Zukunft wird es wohl möglich sein, Prothesen durch Gedanken zu steuern, indem Signale des Gehirns aufgenommen und in Aktionen der künstlichen Gliedmassen umgesetzt werden. Im Januar 2014 haben Forscher der EPFL Lausanne und des BioRobotics Institute in Pisa eine Handprothese getestet, die berührungssensibel ist.

10 Tonnen Burger aus einer Rinds-Stammzelle

Weiteres Handlungsfeld Ernährung: Es erstaunt, dass es möglich ist, innert nur zwei Monaten 10000 kg Hamburger aus lediglich einer einzigen Stammzelle eines Rindes künstlich zu erzeugen und damit notabene nicht nur einen bedeutungsvollen Beitrag zur Hungerbekämpfung zu leisten, sondern auch Türen zu öffnen, die 4 % Treibhausgase zu reduzieren, die weltweit aus der Viehzucht entstehen.

Last, but not least haben auf internationaler Ebene fast alle Länder mit der deutlich längeren durchschnittlichen Lebenserwartung und den daraus resultierenden Gesundheitskosten zu kämpfen. Roos: «Wir werden zwar kalendarisch älter, sind aber dauernd verjüngt.» Tendenziell führt dies wohl zu einer späteren, aber eher verlängerten Pflegebedürftigkeit. «Das Gesundheitswesen wird noch mehr zum Big Business; in den USA dürften sich die Ausgaben bis 2030 vervierfachen und jährlich 20 Billionen Dollar beanspruchen.»

Die höchst interessanten und zum Nachdenken anregenden Botschaften, die kritischen Statements und die zukunftsorientierten Themen inspirierten zum angeregten Gedankenaustausch beim anschliessenden Network-Apéro.

Für die Agenda

Das nächste EDI Podium findet wieder in Luzern statt – am 28. Juni 2019.

Weitere Informationen

www.medidata.ch