## Smart City Demonstrator

### Gebäude

## Themen Smart Home (Wohnhaus)

Kinderzimmer (oben links): Kinder chatten sicher, Startup Privalino (Video)

Arbeitszimmer (oben rechts): Phishing und Schutz vor betrügerischen Nachrichten (Video)

Kaffeemaschine: „Was verstehen Sie unter dem Begriff Smart Home?“, Studie Prof. Vogt

Staubsaugerroboter: Von Staubsauger bis Glühbirne - Forschung zu Smart Home Geräten, Prof. Hollick – wird am Montag als Demo präsentiert von Jiska Classen

Lampe: Smart Home - Smarte Nutzerschnittstelle?, Studie Prof. Vogt

**Kinder chatten sicher**

Kinder sind im Internet zahlreichen Gefahren wie Cyber-Grooming, Sexting und Cyber-Mobbing ausgesetzt. Das Startup Privalino entwickelt einen kindersicheren Instant Messenger, der Kinder zwischen 6 und 10 Jahren in der Online-Kommunikation schützt.

**Phishing und Schutz vor betrügerischen Nachrichten**

Ob privat oder auf der Arbeit - über Social Engineering versuchen Betrüger das schwächste Glied der Sicherheitskette anzugreifen, den Menschen. Die Usability- und Sicherheitsexperten der TU Darmstadt haben deswegen eine Online-Schulung entwickelt.

**„Was verstehen Sie unter dem Begriff Smart Home?“**

Diese und viele weitere Fragen wurden in einer Interviewstudie der TU Darmstadt 42 Nutzern gestellt. Ziel der Studie war es zu ergründen, was Nutzer sich unter Smart Homes vorstellen und was sie erwarten würden sowie welche Privatsphäre- und Sicherheitsbedenken bestehen. Die Nutzer beschrieben ein Smart Home als eine vernetzte Steuerung von Haushaltsgeräten aus der Ferne und erwarten sich mehr Sicherheit und Effizienz in ihrem Leben. Bedenken bestanden bezüglich der Speicherung persönlicher Vorlieben oder Bank- und Gesundheitsdaten.

**Von Staubsauger bis Glühbirne - Forschung zu Smart Home Geräten**

Staubsauger-Roboter − ein praktischer Helfer im Haushalt oder Gefahr für die Privatsphäre? Um durch die Wohnung zu navigieren, legen sie eine Art „Landkarte“ an − und senden diese per WLAN an den Hersteller. Aus den gesammelten und den Nutzerdaten lassen sich viele Informationen ableiten, z.B. Arbeitszeiten, finanzielle Mittel, und durch den Netzwerkzugang (IP, WLAN-Name) auch der Wohnort − manche Modelle senden sogar eine genaue GPS-Position. Eine große Gefahr, wenn diese Daten in die falschen Hände geraten ...

Forscher der TU Darmstadt analysieren Smart Home Geräte und finden Privacy-Schwachstellen.

**Smart Home - Smarte Nutzerschnittstelle?**

Ein Smart Home soll den Alltag komfortabler, sicherer oder energieeffizienter gestalten. Vorgänge im Haus, wie z.B. das Regeln von Licht und Temperatur, sollen automatisch ablaufen. Dennoch möchten viele Nutzer sehen, was in ihrem Smart Home passiert und Vorgänge auch aktiv steuern. Aber wie sollte die Steuerung eines Smart Homes aussehen? Per Smartphone oder lieber über Sprache oder Bewegung? In einer Studie wurden Anforderungen an Nutzerschnittstellen für Smart Homes gemeinsam mit Nutzern erarbeitet und analysiert.

## Thema Finance (Bank)

Grafik auf dem Bildschirm: Blockchain, Prof. Faust + Projekt S7 in CROSSING Phase II

**Blockchain-Forschung: Schneller, sicherer, günstiger (Kette auf Monitor)**

Die Blockchain-Technologie ist die Grundlage für Krypto-Währungen wie Bitcoin. Doch ihre weitere Verbreitung wird durch mangelnde Skalierbarkeit und zahlreiche Sicherheitsschwachstellen gefährdet. So unterstützt z.B. Bitcoin nur wenige Transaktionen pro Sekunde und es kommt immer wieder zu spektakulären Angriffen, bei denen hohe Summen gestohlen werden.

Im Sonderforschungsbereich CROSSING an der TU Darmstadt arbeiten Forscher daran, die Blockchain-Technologie schneller, günstiger und sicherer zu machen durch den Einsatz moderner Kryptographie.

## Thema Critical Infrastructures (Bahnhof)

Scheinwerfer/Blinklicht am Zug: Sicherheit für Kritische Infrastrukturen, Prof. Katzenbeisser & Kooperation mit der DB

**Sicherheit für Kritische Infrastrukturen**

Die Digitalisierung schreitet auch im Eisenbahnsektor immer weiter voran. Die Leit- und Sicherungstechnik, z.B. Stellwerke und Signale, wird zunehmend von analog auf digital umgestellt – und ist damit ein potentielles Einfallstor für Cyber-Attacken.

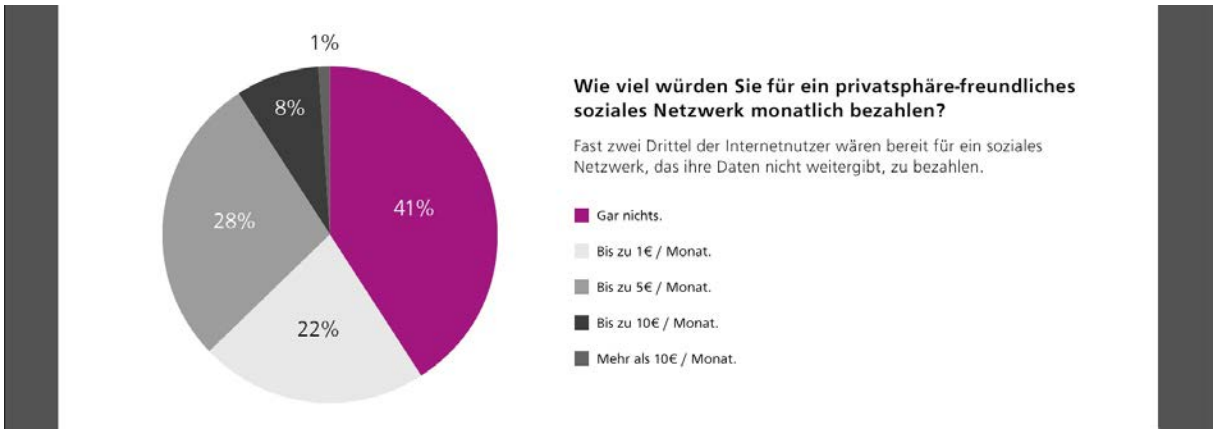
Um diese frühzeitig zu erkennen, abzuwehren und trotzdem einen sicheren Betrieb zu gewährleisten, arbeitet die TU Darmstadt in einer gemeinsamen Arbeitsgruppe eng mit der Deutschen Bahn zusammen. Ziel ist eine „defense in depth" im Eisenbahnumfeld.

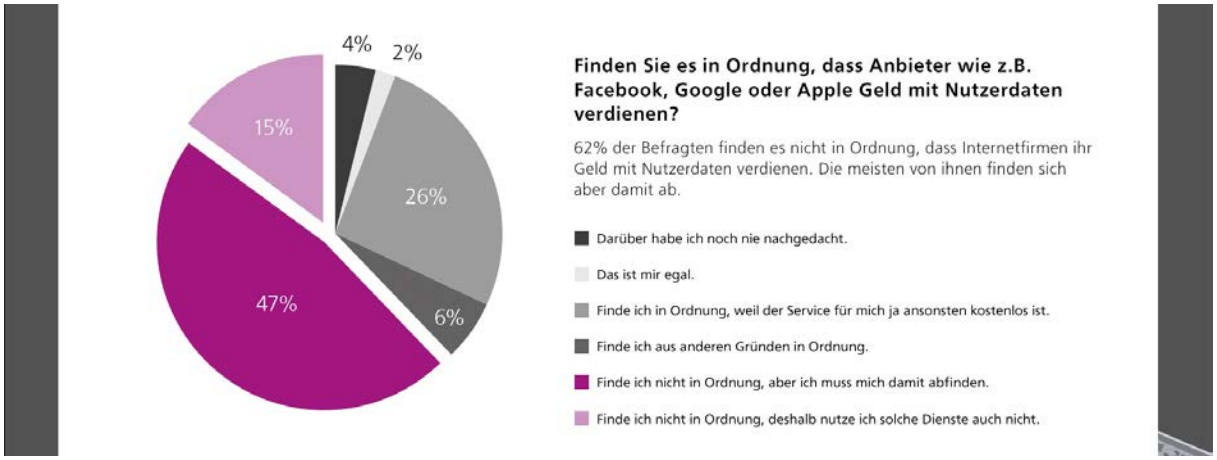
## Thema Privacy (öffentliches Gebäude) – 2 Marker

2 Gebäude, es öffnet sich jeweils direkt ein Slide mit den Studienergebnissen: Studie „Der Preis des Kostenlosen" – Service gegen Daten, ein fairer Deal? Von Prof. Buxmann, wird am Montag ebenfalls als Demo vor Ort sein

**Der Preis des Kostenlosen**

Täglich nutzen viele Millionen Menschen Angebote im Internet, für die sie keine Rechnung bekommen. Und doch zahlen sie dafür – mit ihren Daten. Wie hoch der „Preis des Kostenlosen" ist, erkunden CYSEC-Forscher des Fachgebiets Wirtschaftsinformatik der TU Darmstadt.



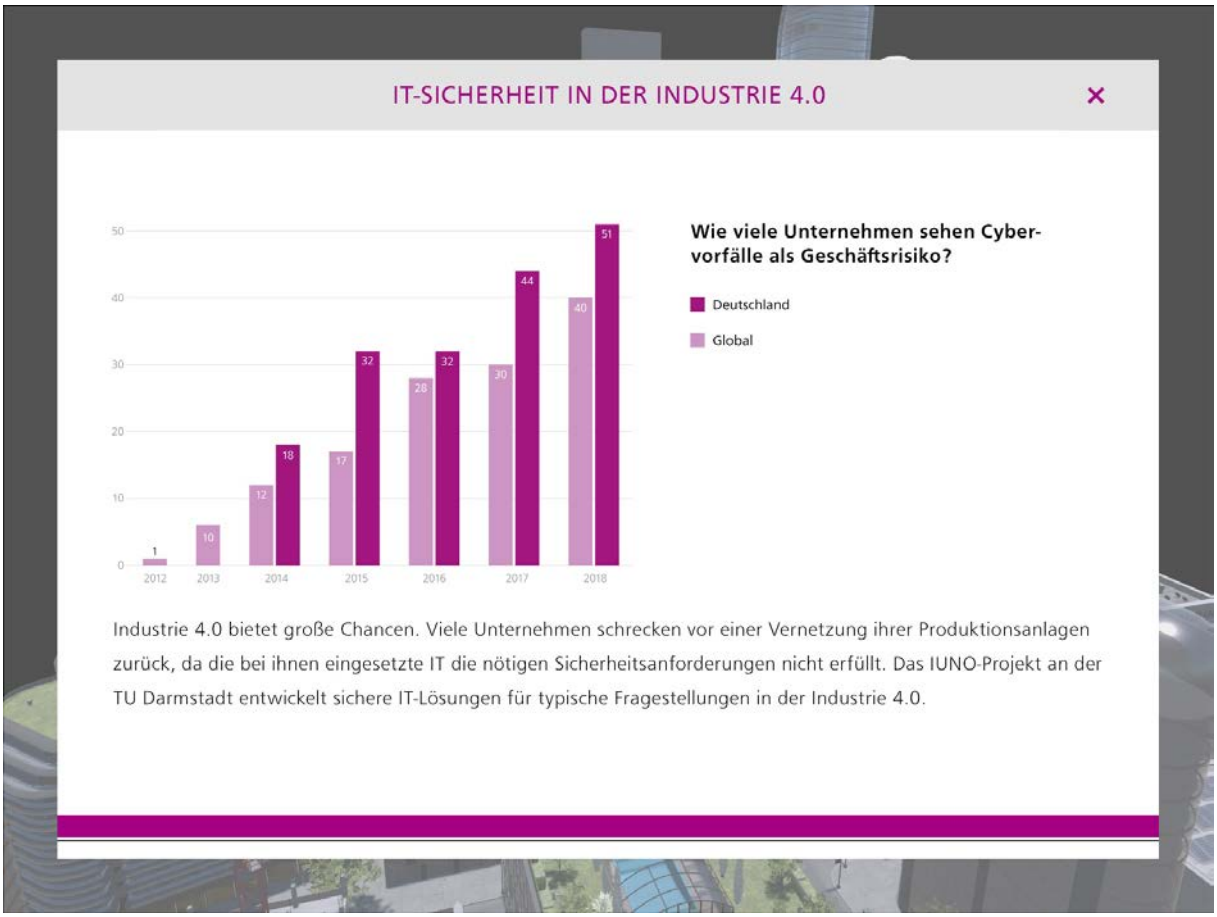



## Thema Industrie 4.0 (Fabrik)

Es öffnet sich direkt ein Slide mit einer Auswertung einer jährlich durchgeführten Studie Allianz Risk Barometer

**IT-Sicherheit in der Industrie 4.0**

Industrie 4.0 bietet große Chancen. Viele Unternehmen schrecken vor einer Vernetzung ihrer Produktionsanlagen zurück, da die bei ihnen eingesetzte IT die nötigen Sicherheitsanforderungen nicht erfüllt. Das IUNO-Projekt an der TU Darmstadt entwickelt sichere IT-Lösungen für typische Fragestellungen in der Industrie 4.0.



## Themen Health (Krankenhaus)


DNA / PCR-Maschine: Genomic Privacy, Rechnen auf verschlüsselten Daten, Prof. Katzenbeisser

Datenübertragung (Computerbildschirm): Long-Term Security, CROSSING / Prof. Buchmann

Uhr: Startup QuantiCor, Post-Quantum-Verschlüsselung

**Erbgut im Angebot - sensible Genomdaten schützen (sich drehender DNA-Strang)**

Je mehr wir über unsere Genomdaten wissen, desto besser können uns Ärzte künftig behandeln. Sie sind die Grundlage der personalisierten Medizin. Doch wie lassen sich diese sensiblen Daten nutzen, ohne dass sie missbraucht werden?

Forscher der TU Darmstadt entwickeln ein Verfahren, bei dem die Daten zwar verschlüsselt werden, aber dennoch nachträgliche Analysen möglich sind. So soll Vertrauen in die Infrastruktur der Genomforschung geschaffen werden – für Patienten, Ärzte, Forscher und IT-Dienstleister.

**Datensicherheit ein Leben lang - und darüber hinaus (Datenblätter/Ordner)**

Die Menge an Daten, die langfristigen Schutz bedürfen, wächst von Tag zu Tag. Krankenakten, Gesundheitsdaten oder Erbgut-Analysen betreffen nicht nur den Patienten selbst, sondern auch seine Nachkommen. Die Datensicherheit muss über einen sehr langen Zeitraum gewährleistet sein. Viele der derzeitig genutzten Sicherheitslösungen sind dafür nicht geeignet.

Im Sonderforschungsbereich CROSSING an der TU Darmstadt werden Techniken für ein effizientes und vertrauenswürdiges Archivierungssystem entwickelt.

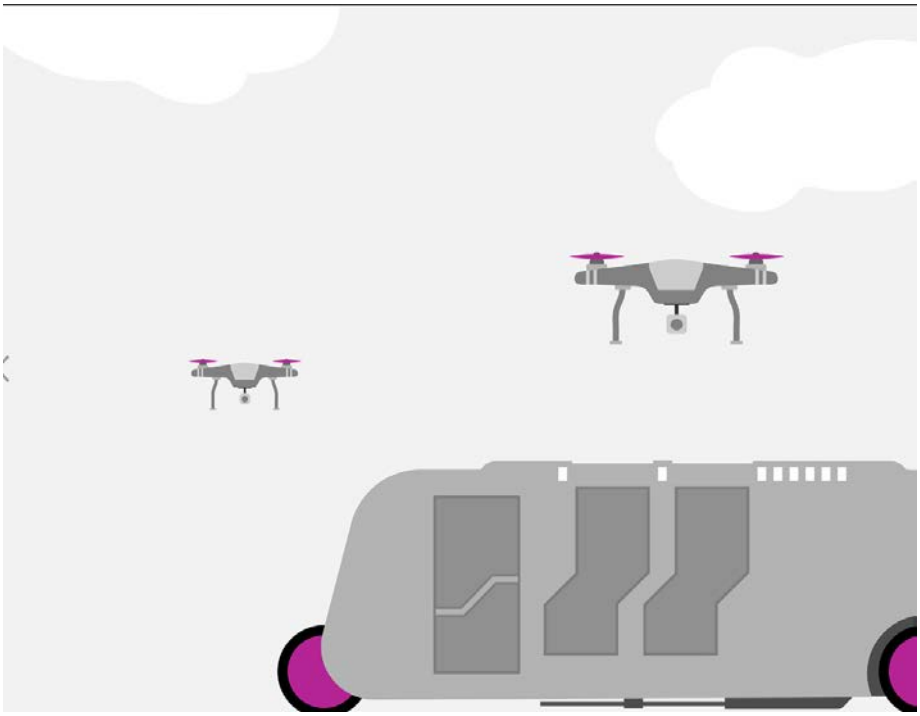
**Verschlüsselung der Zukunft (Uhr)**

Quantencomputer können gegenwärtig genutzte Verschlüsselungsverfahren knacken. Das Startup QuantiCor Security entwickelt daher Sicherheitslösungen der nächsten Generation, die Daten auch vor Quantencomputern schützen.

## Themen Mobility/Autonomous Systems (Bus/Drohnen)

Straßenkreuzung in der Mitte, futuristischer Bus

---



Bus (Räder/Felgen): Mobilität der Zukunft, Verbundprojekt uniCARagil

Drohnen: Autonomous Resilient Systems, Intel Institut / Prof. Sadeghi

**Sicherheit für den Drohnenschwarm (Drohne)**

Die Lieferung vom Onlineshop oder den Wasserkasten vom Getränkemarkt bringen in Zukunft vielleicht mehrere Transportdrohnen, die die Last zusammen tragen. Natürlich werden sie dabei nicht von einem Menschen gesteuert, sondern fliegen selbstständig. Sie sind ein autonomes, kollaboratives System, wie auch selbstfahrende Autos im Straßenverkehr. Neue Technologien bedeuten neue Sicherheitsprobleme − diese versuchen die Forscher am Intel-Lab an der TU Darmstadt zu lösen, z.B. die eigenständige Erkennung und Abwehr von Cyberattacken.

**Mobilität der Zukunft (Bus)**

Das Fahrzeug der Zukunft wird zwar weiterhin vier Räder haben, aber sonst modular aufgebaut sein – zum Beispiel mit einem Motor in jedem Rad. Durch einen Cloud-Dienst wird es automatisiert Personen und Güter transportieren. Das Auto der Zukunft wird dafür komplett mit seiner Umwelt vernetzt sein. Im Projekt UNICARagil entwickeln Sicherheitsforscher der TU Darmstadt ein IT-Sicherheits-Konzept für das autonome Fahren, das die Nutzerdaten schützt und Cyberattacken abwehrt.