

Innovationstagung „Digitale Identität und Sicherheit“ lockte rund 160 Teilnehmende an die HSR nach Rapperswil-Jona

Das Thema „Digitale Identität und Sicherheit“ bewegt: Mit rund 160 Teilnehmenden brach die 39. Innovationstagung gestern Abend an der HSR den bisherigen Besucherrekord. Die Referenten fühlten dem aktuellen Spannungsfeld zwischen Komfort und Sicherheit in einer zunehmend digital vernetzten Welt nach und informierten über die Zukunft der digitalen Identität von Menschen und Geräten.

Heute gibt sich jeder Internetnutzer seine Identität weitgehend selbst. Durchschnittlich 92 Identitäten pro E-Mail-Account besitzt jede Internetuserin – bei Onlineshops, sozialen Netzwerken oder Dienstleistungsunternehmen. Den Aufwand für eine hieb- und stichfeste Authentifizierung dieser Identitäten würden heute nur wenige Unternehmen betreiben, „die gesetzlich dazu verpflichtet sind“, brachte Referent Marius Federle von der St. Galler Kantonalbank ein aktuelles Problem auf den Punkt.

Vertragsabschlüsse wie anno dazumal

Viele digitale Geschäftsbeziehungen sind unsicher, rechtsgültige Verträge werden trotz Online-Formular noch klassisch per Unterschrift über den Papierweg abgeschlossen. Spätestens bei der Identitätskontrolle machen Internetnutzer heute einen Schritt zurück in die vermeintliche Vergangenheit: Vertragsdokumente kommen Tage nach der Onlineregistrierung per Post. Sie müssen unterschrieben und zurückgeschickt werden. In anderen Fällen müssen Nutzerinnen eine Ausweiskopie hochladen, die der digitale Geschäftspartner dem Account hinterlegt und als vertrauenswürdig akzeptiert. Bereits hier ist es nicht sicher, ob die digitale Kundin wirklich ist, wer sie vorgibt zu sein.

Die digitale Identität soll das ändern und rechtsgültige Handlungen online sicher ermöglichen. Wenn es nach Federle ginge, würden Banken bei digitalen Identitäts-Konzepten wie der swissID eine zentrale Rolle als Identitätsgarant spielen. Er illustrierte die Möglichkeiten einer digitalen Identität mit Beispielen aus dem praktisch vollständig digitalisierten Estland (Wahlen, Behördengänge, Vertragsabschlüsse etc. via digitale obligatorische Identität) sowie skandinavischen Ländern wie Dänemark und Finnland.

Sicherheit versus Komfort

Technisch sei eine digitale Identität bereits heute auf sichere Art möglich, versicherte Valentin Tanner von der IT-Sicherheitsfirma taNET und führte das Publikum durch die technischen und strukturellen Stärken und Schwächen von Konzepten wie dem heute verbreitetsten Name-plus-Passwort-System über Passwort-Manager und 2-Faktor-Authentifizierung bis zur Zukunftsvision swissID. Aktuelle Konzepte gingen jedoch „immer zulasten des Benutzerkomforts und erfordern Vertrauen in unzählige Akteure: Hardware-Hersteller, Serverbetreiber, Betriebssysteme, Unternehmen und viele weitere.“

Jedoch biete auch eine einzigartige digitale Identität nicht nur Vorteile, weil alle mit dieser ID verbundenen Aktionen eine Datenspur hinterlassen. „Vielleicht möchte ich ja bei einer Online-Bestellung eine andere Identität als bei meiner Steuererklärung“, sagte Tanner.

**HSR**HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

Auch Geräte brauchen eine sichere Identität

Eine eindeutige Identität ist auch für vernetzte IoT-Geräte wichtig. Insbesondere IoT-Geräte im Zusammenhang mit kritischen Infrastrukturen wie der Energieversorgung brauchen eine starke Hardware-Identität, damit sie nicht unbemerkt gestört oder übernommen werden können, wie Andreas Steffen vom Institut for Networked Solutions der HSR betonte. Als zentrale Pfeiler für eine sichere vernetzte Welt sieht Steffen technische Standards, die es erlauben, IoT-Geräte wie Smartphones, Sensoren oder Steuerungssysteme mit einer nicht manipulierbaren Identität auszustatten. Steffen betonte dabei, dass solche Standards im Idealfall Opensource-Lösungen sein sollten, „damit man auch Geräte verschiedener Hersteller sicher miteinander verbinden und nutzen kann und sich nicht an einen Anbieter binden muss.“

Hotel-Check-in ohne Rezeption

Diese Ausführungen veranlassten Patrik Eigenmann vom Schliesstechnik-Systemanbieter dormakaba dazu, Steffen spontan zu einem „Kaffee“ einzuladen. Denn die neuen Geschäftsmodelle würden Anforderungen an kombinierte Zutrittskonzepte stellen, die sowohl cloud- und IoT-basiert wie auch mechanisch funktionieren müssten. Als Beispiel nannte er eine Hotelkette, die allen via digitale Identität authentifizierten Kunden automatischen Zutritt zu allen zugehörigen Hotels weltweit gewähren möchte – ohne Anmeldung an der Rezeption.

Solche Lösungen würden es ausserdem ermöglichen, dass traditionelle Produkthersteller wie dormakaba über den Verkauf von vernetzten Dienstleistungen zu strategischen Partnern ihrer Kunden werden und damit basierend auf dem Erfolg ihrer Kunden das eigene Geschäft mitskalieren könnten. „Das Plattformgeschäft ist die Zukunft, also die Vernetzung mit unseren Kunden, Zulieferern, Produktionsstätten, Dienstleistern und weiteren Partnern“, sagte Eigenmann.

Für derlei Geschäftsmodelle sind die derzeit noch in der Entwicklung befindlichen sicheren, digitalen Personen- und Geräte-Identitäten zentral.

Fotos der Innovationstagung finden Sie [hier zum Download](#).

Kontakt für Rückfragen: Willi Meissner, HSR Kommunikation, Telefon 055 222 49 82, willi.meissner@hsr.ch