Digital Data Security: Wahrung von Identität, Vertrauen und Privatsphäre in einer digitalen Welt

IBM Software Group

Herzlich willkommen zum Podcast über digitale Datensicherheit. Christian Achermann im Gespräch mit Jan Camenisch, Wissenschaftler am IBM Research Lab in Rüschlikon.

Christian Achermann: „Kannst du uns etwas über dich und deine Funktion bei IBM erzählen?“

Jan Camenisch: „Ich bin Mitglied des Forschungsteams hier und Kryptograf. Parallel leite ich das europäische Projekt Primelife. Dieses Projekt widmet sich dem Schutz von persönlichen Informationen im Internet, der Wahrung von Identität, Vertrauen und Privatsphäre in einer digitalen Welt.“

Christian Achermann: „Wer heute Online-Dienstleistungen in Anspruch nimmt, muss oft eine Vielzahl persönlicher Informationen preisgeben. Welche Risiken birgt dies?“

Jan Camenisch: „Auf der einen Seite besteht die Gefahr, dass die vertraulichen Daten in falsche Hände geraten, entweder weil sie, wie immer wieder in der Presse zu lesen ist, schlichtweg verloren gehen oder weil sie von Mitarbeitern der Firma, der die Daten zur Verfügung gestellt wurden, missbraucht werden. Auf der anderen Seite besteht auch die Gefahr, dass mithilfe der Daten, die jemand preisgibt, Profile erstellt werden. So können zum Beispiel Informationen, die wir über uns in einem sozialen Netzwerk veröffentlichen, einem potenziellen Arbeitgeber als Entscheidungsgrundlage dafür dienen, ob er uns einstellt oder nicht.“

Christian Achermann: „In der letzten Ausgabe von THINK!, dem Kundenmagazin von IBM, war zu lesen, dass du und dein Team an einer zukunftsorientierten Lösung zum Schutz von sensiblen Daten namens „Identity Mixer“ arbeiten. Könntest du etwas zum derzeitigen Stand dieses Projekts und zur Funktionalität dieser Lösung sagen?“

Jan Camenisch: „Mit dieser Lösung wollen wir das Problem, dass zu viele Informationen preisgegeben werden, auf dreifache Weise bekämpfen: Zunächst einmal versuchen wir die Menge der Daten zu reduzieren, die man preisgeben muss. Zweitens versuchen wir bei den Usern die Entwicklung von Vertrauen in die jeweiligen Online-Kommunikationspartner zu fördern; und drittens möchten wir den Benutzern die Kontrolle über ihre Daten zurückgeben. Hier ein Beispiel für Datenreduzierung: Bestellt jemand in einem Lokal ein Bier, muss er oftmals nachweisen, dass er dafür alt genug ist. Besitzt diese Person einen elektronischen Personalausweis, könnte das dazu führen, dass sämtliche auf dieser digitalen Identity Card enthaltenen Informationen, einschliesslich aller persönlichen Daten, preisgegeben werden. Mit unserer Technologie dagegen könnten Sie dem Wirt beweisen, dass volljährig sind, ohne mehr über sich zu verraten. Das ist Datenreduzierung.

Des Weiteren müssen Sie, wenn Sie ein Lokal besuchen, sicher sein können, dass es sich auch wirklich um ein Lokal handelt und Sie tatsächlich mit einem Wirt sprechen. Bei dem Beispiel mit dem Lokal ist das natürlich kein Problem. Im Internet aber können Sie nie sicher sein, auf welcher Seite Sie sich befinden und ob Sie ihr vertrauen können oder nicht. Wir arbeiten auf eine Lösung hin, die es Ihnen erlaubt, eine Vertrauensbasis aufzubauen. Und was die in einigen Fällen unvermeidliche Weitergabe von persönlichen Informationen betrifft, so informieren wir den Benutzer zunächst, was mit seinen Daten geschieht, ob sie für zehn Jahre gespeichert werden, ob sie unmittelbar nach der Transaktion wieder gelöscht werden und wer im Umgang mit Ihren Daten wozu befugt ist.
Einige der Lösungen sind bereits als Download verfügbar; ein Basis-Code ist bis zu einem gewissen Grad erhältlich. Andererseits sind wir immer noch im Auf- und Ausbau begriffen und suchen nach Möglichkeiten der Standardisierung und nach möglichen User-Schnittstellen, um die Technologie für möglichst viele Menschen zugänglich zu machen und zugleich der Industrie einen Weg zu bahnen, sie als Standardlösung in ihre Technologien zu integrieren."

Christian Achermann: „Mit welchen Problemen warst du beim Entwicklungsprozess konfrontiert? Was hast du unternommen, um diese Schwierigkeiten zu umgehen?"

Jan Camenisch: „Wir entwickeln diese Lösungen seit über zehn Jahren. Als wir damit begannen, waren es vorwiegend mathematische Probleme der Kryptografie, mit denen wir konfrontiert waren. Wenn ich eine Identity Card besitze, die mein Geburtsdatum ausweist, wie kann ich dann einen Wirt mithilfe dieses Ausweises davon überzeugen, dass ich volljährig bin, ohne mein Geburtsdatum preiszugeben? Wie können wir solche kryptografischen Mechanismen konstruieren? Als wir mit Lösungen aufwarteten, war die viel schwierigere Aufgabe, den Menschen zu erklären, wie sie funktionieren würden, so dass diese Kollegen versuchen konnten, User-Schnittstellen zu entwickeln, die eine intuitive Bedienung dieser Technologien ermöglichen. Dies ist meines Erachtens die wichtigste Frage. Ohne gute User-Schnittstellen wird eine solche Technologie niemals implementiert werden, und meiner Meinung nach hat die Forschung hier erst den halben Weg zurückgelegt. Wir verfügen über erste Lösungen, können aber nach meiner Überzeugung weitaus mehr erreichen."

Christian Achermann: „Wenn du ein wenig vorausblickst, in welche Richtung wird deine Lösung nach deiner Meinung in den nächsten Monaten oder Jahren weiterentwickelt werden?"

Jan Camenisch: „Ich würde sagen, dass wir die Basistechnologie mit den Kryptografiealgorithmen ziemlich gut im Griff haben. Wir wissen, wie wir elektronische Identity Cards und Zertifikate ausstellen können. Was das nächst höhere Niveau, nämlich die Frage des Datentransfers, betrifft, so sind wir dabei, die Dinge zu standardisieren und Kommunikationsstandards und -protokolle zu entwickeln. In diesem Zusammenhang sprechen wir von Standardisierungsinstitutionen. Wenn wir noch etwas weiter gehen und einen Blick auf die User-Schnittstellen werfen, so haben wir zwar erste Lösungen, weitere Forschungsbemühungen sind jedoch vonnöten. Wenn wir uns zudem anschauen, wie das Internet heute genutzt wird, etwa im Falle der sozialen Netzwerke oder Wiki-Systeme, wo Unmengen persönlicher Daten hinterlassen werden, so ist unsere Technologie hier nicht richtig anwendbar.

Es bedarf noch einiger Forschungsarbeit, um herauszufinden, wie die User so geschützt werden können, dass ein künftiger Arbeitgeber nicht unbedingt die letzten Partybilder zu sehen bekommt.“

Christian Achermann: „Um zum Schluss zu kommen: Wie kann man seine persönlichen Daten in Anbetracht dessen, dass zurzeit kein vergleichbares Produkt auf dem Markt erhältlich ist, am besten schützen? Hast du ein paar Vorschläge?“

Jan Camenisch: „Ich denke, das Beste, was wir tun können, ist, genau darauf zu achten, mit wem wir kommunizieren und welche Daten wir dieser Adresse zur Verfügung stellen. Wir könnten versuchen die betreffen Datenschutzregelungen einzusehen, doch sind diese zuweilen schwer zu finden. Ansonsten würde ich vermutlich Einweg-Kreditkarten und -Mail-Adressen verwenden und keine korrekten persönlichen Informationen herausgeben, wenn dies nicht zwingend erforderlich ist. Gut – wenn Sie etwas an Ihre Haustür geliefert haben wollen, müssen Sie natürlich Ihre wirkliche Adresse angeben.“

Christian Achermann: „Vielen Dank für deine Zeit und für deine umfangreichen Einblicke, die du uns vermittelt hast.“