Das Prinzip: Keiner weiß alles

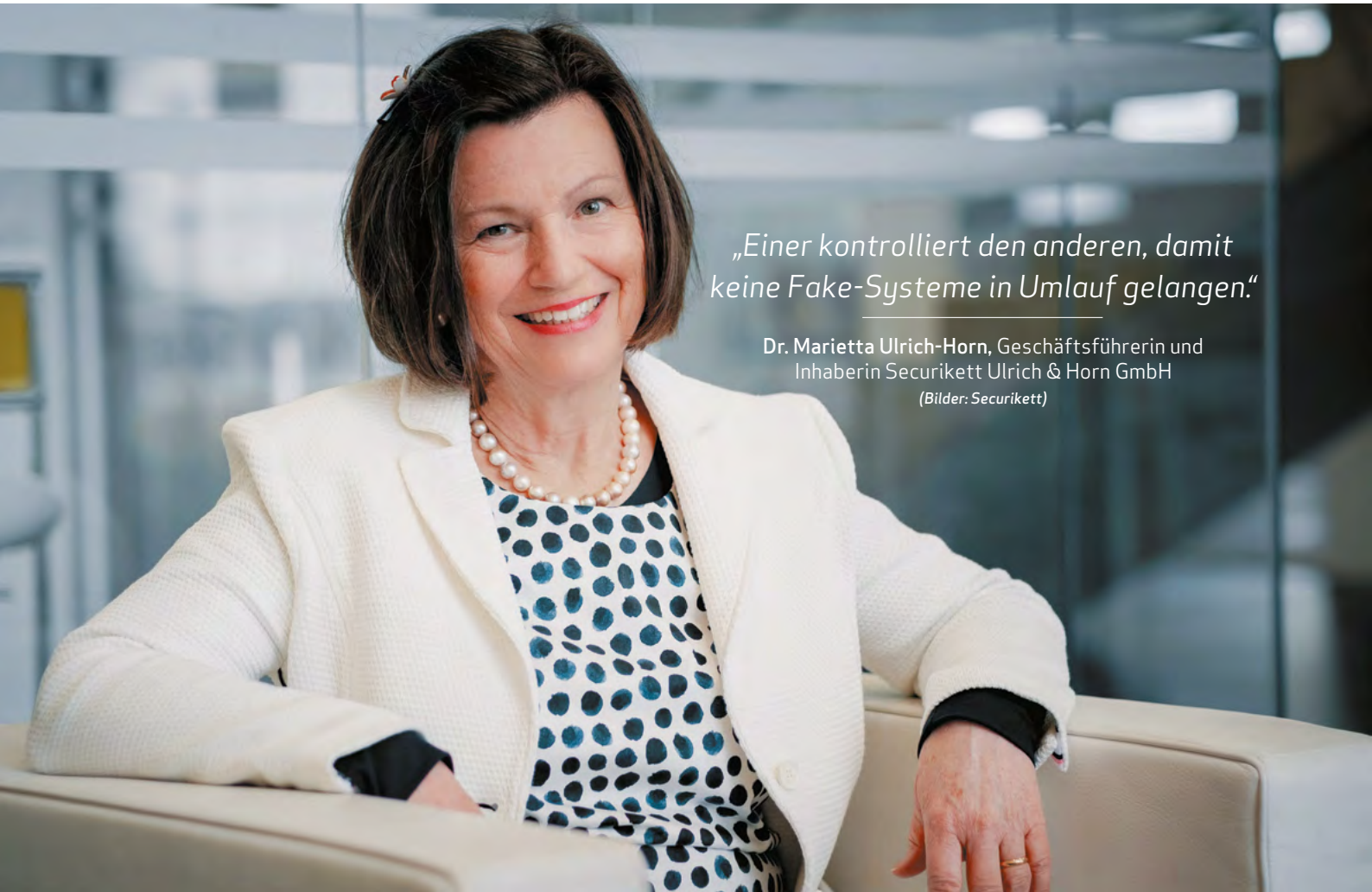
Wie transparent wird man beim Wareneinkauf, wenn man Warencodes scannt? Wie sicher ist der ganze Zinnober? Man scannt ein Produkt und kommt dann wieder auf eine Landingpage? Konsumenten können echte Digitalisierungen von falschen Digitalisierungen auf den ersten Blick schwer unterscheiden. Doch was kann man dagegen tun? Auskunft über diese Entwicklungen gibt Dr. Marietta Ulrich-Horn.

Das Internet of Things (IoT) bedeutet in der Welt der Verpackungen, dass jedes Produkt mit einem einmaligen Code serialisiert wird, der ihm eine eindeutige Identität gibt: ein einmaliger QR-Code anstatt eines einmaligen Chips sozusagen. Das ist ein Megatrend für den Echtheitsnachweis und die Produktrückverfolgbarkeit, der aber leicht zu Fehlentwicklungen führen kann. Fälschungssysteme, doppelte Codes und Datenschutz sollten strategisch weitergedacht werden. Seit vielen Jahren beschäftigt sich Dr. Marietta Ulrich-Horn, Geschäftsführerin der Securikett Ulrich & Horn GmbH in Österreich, mit interoperablen Systemen in Zusammenhang mit IoT und gewährt unserem Fachmagazin Einblicke in unterschiedliche Lösungsansätze.

Warum liegt diese Problematik Ihnen und Ihrem Unternehmen so besonders am Herzen?

Dr. Marietta Ulrich-Horn: Wir setzen auf Qualität und Nachhaltigkeit, auch bei der Softwareentwicklung. Produzenten, Handelsbetriebe und Onlineshop-Betreiber überlegen sich aus unserer Sicht noch zu wenig, wie weit die Produktdigitalisierung und die damit verbundenen Systeme zu Ende gedacht sind. Wenn man nicht von vornherein Maßstäbe setzt, um die Sicherheit von Systemen und deren Benutzern zu gewährleisten, kann dies leicht zu Missbrauch und Rückschlägen führen.

Wir sind der Meinung, IoT macht nicht alles komplizierter, wir sind absolute Befürworter und bieten das als Unternehmen auch selbstverständlich an: mit einer Cloudsolution für Track-&-Trace und Produktverifika-



„Einer kontrolliert den anderen, damit keine Fake-Systeme in Umlauf gelangen."

Dr. Marietta Ulrich-Horn, Geschäftsführerin und Inhaberin Securikett Ulrich & Horn GmbH

(Bilder: Securikett)

Jede einzelne Tax-Stamp enthält einen eigenen QR-Code. Papierbasierte Tax-Stamps werden in Europa zum Versiegeln von Zigarettenpackungen verwendet.

tion und mit einer Plattform für „UID-Issuance", also die sichere Herausgabe einmaliger Codes. Wir plädieren jedoch dort, wo es sinnvoll ist, auf eine Dezentralisierung der Macht über die Daten und setzen uns für interoperable Lösungsvorschläge ein.

Wie dürfen wir das verstehen?
Dr. Marietta Ulrich-Horn: Es ist vorhersehbar, dass Fälscher nicht nur ein Hologramm nachstellen können, sondern ein ganzes digitales System samt Landingpage nachbauen. Auch ein Zollbeamter kann nicht immer erkennen, auf welche Landingpage er geleitet wird und ob sie echt ist. Eine kleine Änderung oder ein Buchstabe mehr in der URL, und man strandet auf einer nachgebauten Landingpage, auf einer von Fälschern betriebenen Plattform. Der Konsument kann ebenfalls oft nicht wissen, wo er hingeführt wird, wenn er die Echtheit eines Produkts überprüfen oder Informationen zu einem Produkt abrufen will.

Wir wollen nur Dinge anbieten, die wirklich verlässlich und zukunftssicher sind, und haben uns als Ziel gesetzt, bei unseren Produkten den Fälschern immer zwei Schritte voraus zu sein. Wir sind der Auffassung, dass es sehr schädlich wäre, wenn digitale Parallelwelten in größerem Umfang entstehen würden. Das würde das Vertrauen der Konsumenten in die Produktdigitalisierung, die viele Vorteile mit sich bringt, untergraben. Wenn mehrere Systeme interoperabel verbunden sind, kann ein Fälschersystem nicht so einfach in die Landschaft eintreten.

Wie könnte das verhindert werden?
Dr. Marietta Ulrich-Horn: Wir setzen auf das Prinzip der Gewaltenteilung, wie es ansatzweise bereits in der europäischen Tabakregulierung verankert ist. Dort werden die einmaligen Codes für Steuermarken von einer nichtstaatlichen und unabhängigen Institution ausgegeben, um sicherzustellen, dass keinerlei Missbrauch bei der Codevergabe erfolgen kann und auch nicht irrtümlich mehr Codes als gewünscht in Umlauf kommen oder doppelt vergeben werden. Mit unserer im Haus entwickelten UID-Issuance-Plattform beispielsweise können wir, wo dies gewünscht wird, diese Unabhängigkeit von der Verwendung der Codes gewährleisten.

Wie funktioniert das bei der praktischen Umsetzung?
Dr. Marietta Ulrich-Horn: Lassen Sie mich kurz ein Beispiel für den Einsatz der UID-Issuance-Plattform, losgelöst von der Tabakregulierung, erläutern: Ein Konzern, der mehrere Marken vertreibt, beauftragt uns mit der Codevergabe. Diese Codes werden an die jeweiligen lokalen Produzenten zur Applizierung in Form von Barcodes, QR-Codes etc. auf das Produkt und zur weiteren Verwendung etwa für Produktrückverfolgung ausgegeben. Es wird damit vermieden, dass für jede Marke eine eigene Codegenerierung mit unterschiedlichen Anbietern erfolgt. Für Markeninhaber ist es ein klarer Vorteil, wenn es eine unabhängige, vom Unternehmen losgelöste Ausgabeinstanz für diese Codes gibt, und lokale Anbieter profitieren von der After-Sales-Kundenkommunikation, die durch IoT erst ermöglicht wird.

Ein weiteres Beispiel zur Gewaltenteilung ist der Einsatz eines Trusted Entry Points (vertrauenswür- ››

Elektronische Verifizierung durch Drittanbieter: Wichtig ist die Kombination der digitalen Identifikation mit der physischen Authentifizierung. Beide Tax-Stamps verweisen auf die App Otentik zur Codeverifizierung. (Bild links: Advanced Track-&-Trace)

digen Zugangspunkts), einer verlässlichen Verifikations-App, die auf einer „Chain of Trust" beruht, einem öffentlich registrierten Trustanbieter sozusagen.

Man muss sich das so vorstellen, wie es bereits bei digitalen Signaturen bekannt ist. Erst über den Trusted Entry Point erhält man einen Zugriff bzw. die digitale Signatur, die um den Code herumgelegt wird. Es war unsere Pionierleistung, gemeinsam mit ATT, einem befreundeten Unternehmen, ein Projekt zu realisieren, diesen Trusted Entry Point anhand eines Steuerbanderolen-Pilots zu demonstrieren. Erst wenn ein Code von einer dritten Instanz als echt verifiziert wird, kann davon ausgegangen werden, dass der UID am Produkt echt ist und das Produkt das hält, was es verspricht.

In dem Pilotprojekt konnten wir auch zeigen, wie wichtig die Kombination der digitalen Identifikation mit physischer Authentifizierung ist: Auf der „trusted" Landingpage wird genau erklärt, worauf man achten muss, damit nicht etwa der QR-Code allein nachgedruckt werden kann. Für die physische Authentifizierung eignen sich nichtkopierbare Sicherheitselemente, detaillierte Erläuterungen dazu würden aber den Rahmen hier übersteigen.

Können Sie uns noch ein weiteres Beispiel für funktionierende Interoperabilität geben?

Dr. Marietta Ulrich-Horn: Im Bereich der sich rasch entwickelnden Rückverfolgbarkeitssysteme wird leider allzu oft nicht weit genug gedacht. Anbieter denken in „Silos". Dadurch ist es nicht möglich, dass ein Dritter als unabhängige Partei eine überwachende Rolle einnimmt. Die Gewaltenteilung spielt für uns, beispielsweise bei Pfandsystemen, eine übergeordnete Rolle. Es sollte immer gewährleistet sein, dass der Markeninhaber keine privaten Daten speichern muss. Das kann man realisieren, indem man einen Dritten ins Boot holt, wie wir beim Feldversuch mit Saubermacher und ARA gut zeigen konnten. Hier ging es darum, dass Konsumenten Flaschen- und Dosenleergebinde nicht in den Shop, sondern direkt beim Recyclinghof oder bereitgestellten Recyclingtonnen entsorgen und das Rückgabepfand direkt auf einer App gutgeschrieben wurde. Die Codes konnten nur einmal ausgelesen werden.

Unsere Aufgabe war es, die Etiketten zu drucken und zu überprüfen, ob der Code echt ist. Ein Dritter hat eine App betrieben, die den Bonus bereitgestellt hat. Hier war es uns wichtig, dass nicht jeder alle Daten für das Pfand sieht. Wir als Unternehmen wussten nicht, wie viele Codes jeder Getränkehersteller, der am Projekt teilgenommen hat, bekommen hat. Die Daten für die Pfandrückgabe, also die Daten über Kontoverbindungen, um das Pfand gutzuschreiben, waren bei dem dritten Teilnehmer, dem App-Betreiber hinterlegt. So wurde durch Interoperabilität gewährleistet, dass Daten keinesfalls missbraucht werden konnten.

Welches Ziel wird mit diesen Lösungen verfolgt?

Dr. Marietta Ulrich-Horn: Wir wollen erreichen, dass private und öffentliche Systeme verlässlich miteinander arbeiten können. Sonst entwickelt sich eine Landschaft von kleinen Codesystemen und niemand weiß, ob diese Systeme echt sind. Staatliche Anwendungen allein decken meist nur das Notwendigste ab. Daher ist für uns Interoperabilität der Systeme, öffentlicher wie privater, eine gute Lösung.

Was ist aus Ihrer Sicht das Besondere an diesen Entwicklungen, was hebt sie von anderen ab?

Dr. Marietta Ulrich-Horn: Wir denken bei allen Lösungen immer einen Schritt weiter und an erster Stelle steht für uns die Sicherheit des Konsumenten. Wir bieten im Unternehmen selbst eine UID-Issuance-Plattform an, arbeiten kontinuierlich seit über zehn Jahren an der Traceability-Plattform Codikett, drucken manipulationssichere Etiketten und verstehen uns auf die Applizierung von IoT auf das Produkt.

Wir erachten eine strikte Trennung der Systeme, je nach Bedarf, als sinnvoll. Und wenn ein Kunde eine Codeausgabe von uns möchte, die Codesystem-Betreiber jedoch Drittanbieter sind, dann ist das Prinzip der Gewaltenteilung angewendet. Für uns steht seit Gründung der Firma Konsumentensicherheit im Vordergrund und wir möchten Fälschern keine Spielwiese geben, um sinnvolle Innovationen auszuhebeln.

Der Einsatz von manipulationssicheren Technologien wie den Void-Etiketten erhöht die Sicherheit. Beim Öffnen entsteht ein nicht entfernbares Muster und es ist praktisch unmöglich, das Etikett wieder anzubringen.

Digitaler Beitrag zum Recyclingprojekt „digi-Cycle“: Rückgabepfand direkt per App – drei „Partner“ teilen sich die „Zugriffsrechte“.

Wie wichtig schätzen Sie diese Entwicklung als Trend für die Verpackungsindustrie insgesamt ein?

Dr. Marietta Ulrich-Horn: Die Zahl der Fake-Produkte ist in den letzten Jahren massiv gestiegen, nicht zuletzt durch den Internethandel und den Paketversand, der sich größtenteils den Zollkontrollen entzieht. Die weltweiten, nicht nur wirtschaftlichen, sondern gesundheitlichen Schäden, hervorgerufen durch gefälschte Produkte, sind nicht zu übersehen. Jede Art von Mehr an Sicherheit für Konsumenten sollte auch der Verpackungsindustrie ein großes Anliegen sein. Schließlich sind wir alle in den Kreislauf eingebunden und selbst Konsumenten.

Wir glauben zudem, dass ein Markeninhaber, der auf IoT setzt, auch wirklich gewährleisten muss, dass wirklich echt ist, was der Kunde kauft. Wenn sein Sicherheitskonzept nicht hieb- und stichfest ist, dann bekommt er ein haftungsrechtliches Problem. Moderne Marken sollten sich sehr überzeugend für die Sicherheit ihrer Marken einsetzen und dies sichtbar transportieren, denn ein enttäuschter Konsument wäre kein gutes Aushängeschild. ■

»» *www.securikett.com*

English version of the article: http://pack.link/securikett