



AFCEA 2010

Security@BITKOM

ISBN 978-3-934401-15-0

*Behörden Spiegel-Gruppe
in Zusammenarbeit mit AFCEA Bonn e.V.*

Brauchen wir noch Grenzkontrollen?

Jörg Scholz, sBS Client Executive Customs, Border & Revenue Management, IBM Deutschland GmbH, Leiter der Projektgruppe Bordercontrol im AK Öffentliche Sicherheit



Jörg Scholz

Januar 2010; Sicherheit kennt keine Grenzen – ohne einen legalen und effizienten Datenaustausch kann im Zeitalter der Mobilität keine angemessene Sicherheit erreicht werden. Der Umbau der Grenzverwaltung zählt zu den dringlichsten Aufgaben. Neue Bedrohungen zeigen die Verwundbarkeit der modernen Wirtschaftsregionen. Bisherige Ansätze fokussieren oft-

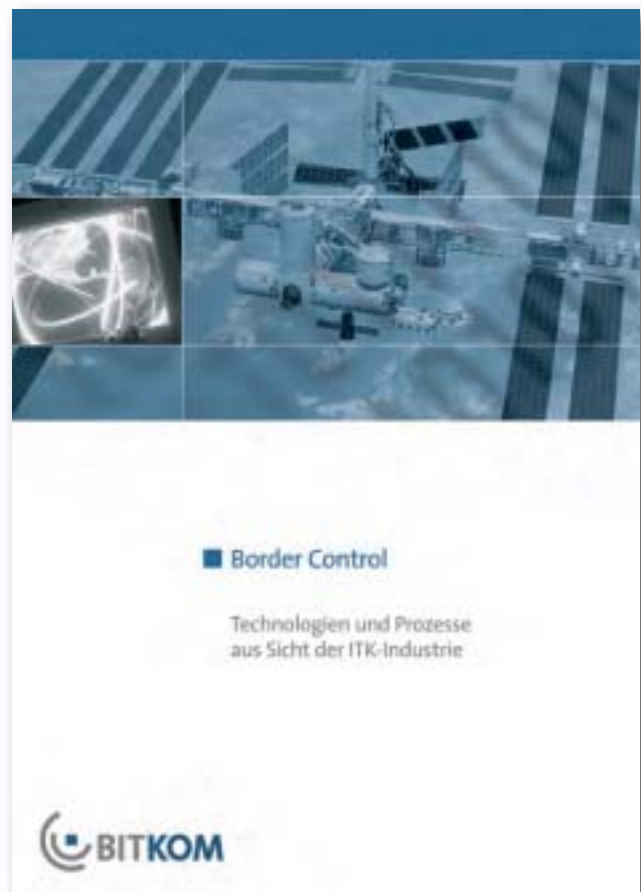
mals auf die Kontrollen im unmittelbaren Zusammenhang mit der Reise. Der Wirksamkeit dieser noch größtenteils manuellen Kontrollen sind enge zeitliche und kapazitive Grenzen gesetzt, die die Geduld der Beteiligten strapazieren. Die Akzeptanz von IT-unterstützten Grenzkontroll-Lösungen zeigt die Bereitschaft der Gesellschaft, die hohen Sicherheitsanforderung durch intelligenteren Kontrollmechanismen umzusetzen, um die Reisebewegungen von Personen und Waren über die Luft-, See- und Landesgrenzen in einem modernen Europa weiter praktikabel zu halten. Die Pläne der Europäischen Union setzen Standards und Akzente und fordern die Entscheidungsträger in den Mitgliedsstaaten des Verbundes zu einem Wettbewerb nach höherer, vernetzter Sicherheit unter Beachtung der Vereinfachung von Reisetätigkeiten auf. Deutschland hat die Chance, eine Leuchtturmposition zu erreichen und technologische Investitionen sowie deren Standardisierung mitzubestimmen.

1. Die Balance von Sicherheit und Komfort

Millionen von Reisenden sind täglich in der gesamten Welt unterwegs, um ihren privaten und geschäftlichen Interessen nachzugehen. Tendenziell rechnet der aktuelle Touristikbericht wieder mit einem Anstieg von Reisebewegungen und baut die entsprechenden Infrastrukturen an den ca. 1.800 Grenzpunkten in Europa proaktiv aus. Auf der anderen Seite verschwinden die physischen Grenzen zwischen den Ländern und die bisherige Deutung einer Grenze verändert sich

unter der Aufwertung der Interessen der Europäischen Union. Wir müssen fortan zwischen materiellen und virtuellen Grenzpunkten unterscheiden, die entlang der gesamten Reisekette liegen. Dabei ist es irrelevant, ob es sich um Reisebewegungen von Personen, Waren oder Geldströmen handelt.

Hinter den grenzüberschreitenden Bewegungen steckt ein hochkomplexes und effizientes System mit eingespielten logistischen Prozessketten. Eine Vielzahl von Beschäftigten in Firmen, Behörden und Institutionen sind an dem Gesamterfolg beteiligt. Häfen aller Art haben eine hohe wirtschaftspolitische Bedeutung für die betroffenen Regionen und darüber hinaus. Der Flughafen in Frankfurt beispielsweise verzeichnete im Zeitraum von 1980 bis 2009 einen Anstieg der Arbeitsplätze von 30.000 auf 70.000. Bis 2012 wollen die Berliner Flughäfen 40.000 neue Arbeitsplätze schaffen und



zählen damit zu einem der größten Arbeitgeber der Region. Auch Stellen in der sekundären Wertschöpfung, wie zum Beispiel im Hotelgewerbe oder bei den Transportunternehmen, spielen für den Arbeitsmarkt eine wichtige Rolle. Diese Hochleistungsmetropolen sind nicht nur bedeutende Arbeitgeber, sondern zugleich auch identisch mit Grenzpunkten eines Landes und der Europäischen Union. Dies birgt gewisse Risiken, denn unvorhersehbare Ereignisse oder Fehler können zu signifikanten Risiken und Bedrohungen für alle Beteiligten der gesamten Reisekette führen. Sicherheit und Bequemlichkeit stehen sich bei Grenzkontrollen oftmals entgegen. Unzählige Reisende haben diese Erfahrung bereits gemacht, zum Beispiel beim Anstehen in lästigen Warteschlangen oder Detailkontrollen. Daher ist ein hohes Maß an Fingerspitzengefühl der Entscheidungsträger notwendig, um gleichzeitig sicheres und komfortables Reisen zu ermöglichen.

Die hierfür notwendigen und verordneten Kontrollprozesse sind sehr personalintensiv. Jede gesetzliche Änderung greift in die Prozesse ein und zieht teilweise aufwändige Anpassungen



Reguläre Grenzkontrolle am Flughafen

Quelle: Bundespolizei

beim Personal, der Ausbildung, der Organisation oder den Technologien nach sich. Bei der partiellen Auslagerung von Kontrollaufgaben an private Anbieter lassen sich kaum noch signifikante Einsparungspotenziale realisieren



„be brilliant together“ : Immer mehr Organisationen verstehen, dass beste Ergebnisse nur durch brillante Zusammenarbeit im Team erzielt werden. Für sie ist Logica der Serviceanbieter für Business und Technologie. Wir integrieren Menschen, Business und Technologie in ein dauerhaftes Zusammenspiel, das für Sie als Kunden optimal wertschöpfend ist. Dazu suchen wir die langfristige Kooperation mit ihnen und ihren Partnern, um Sie auf diese Weise nachhaltig bei der Entwicklung Ihres Unternehmens unterstützen zu können. Unsere Mitarbeiter und Teams kombinieren dafür täglich neu tiefes Kundenverständnis und praktisches Expertenwissen über Technologien und Systeme, um innovative Lösungen für Ihre Geschäftsanforderungen zu entwickeln. Wir verstehen Ihr Geschäft und Ihre Kultur, bringen uns auf allen Ebenen offen ein, hören zu und fragen nach.

In brillanter Zusammenarbeit mit Ihnen, Ihren Partnern, Kunden und Dienstleistern liefern wir so genau das, was Sie benötigen. Genau dort, wo sie es benötigen. Das meinen wir mit be brilliant together.

Bei Logica Deutschland sind 2 200 Mitarbeiter beschäftigt. Die Beratungs- und Entwicklungsteams sind regional disloziert und werden deutschlandweit koordiniert. So steht Logica immer in der Nähe des Kunden bereit, kann seine Teams flexibel und aufgabenorientiert einsetzen und damit rasch und flexibel kundenspezifische und herstellerunabhängige Lösungen verwirklichen. Auf diesem Weg trägt Logica entscheidend zur zukunftsfähigen Gestaltung der Geschäftsprozesse der Kunden bei. Und das sichert den Erfolg des Kunden!

30 Jahre Partnerschaft mit der Bundeswehr/NATO

Logica ist in Deutschland in fast jeder bedeutenden Branche aktiv. Die Kunden rekrutieren sich vor allem aus dem gehobenen Mittelstand und den Großunternehmen sowie aus dem Bereich der öffentlichen Dienste. Im öffentlichen Sektor ist besonders die seit über 30 Jahren erfolgreiche Partnerschaft mit der Bundeswehr hervorzuheben. Aktuell sind insbesondere folgende Projekte zu nennen:

- Führungsinformationssystem der Streitkräfte (FüInfoSys SK)
- Beratung der NATO C3 Agentur bei der Einführung des NATO Graphical Information System
- Implementierung und Support des NATO Document Handling System (NATO-DHS) – an über 20 Standorten und auch in Einsatzgebieten der NATO
- Entwicklung eines Demonstrators für ein Vorhaben Informations- und Planungssystem Bundeswehr auf Basis der aktuellen Sharepointtechnologie

In diesem Jahr treten wir gemeinsam mit der Firma **Kontron** auf:

Robuste Embedded Computing Lösungen für das Militär

Kontron ist führend in Embedded Computer Technologie für militärische Anwendungen. Wir liefern an die weltweit bedeutendsten Militärdienstleister anspruchsvolle und technologisch führende robuste Military COTS Boards und Systeme, technischen Support sowie umfassende Services für das Programm- und Life-Cycle-Management. Kontron's Erfahrungen mit robuster Military COTS Technologie ist in unzähligen Anwendungen unter rauen Umgebungsbedingungen über viele Jahre hinweg gewachsen und praxiserprobt. Unser stetiges Engagement im Bereich der Embedded Computer Technologie für Wehrtechnik-Applikationen hat schon viele innovative Antworten auf die besonderen Herausforderungen im militärischen Markt zu Tage gefördert. Unsere COTS-Produkte werden selbst in besonders sensiblen militärischen Anwendungen eingesetzt.





Die Einzelkontrolle bindet viel Personal

Quelle: Bundespolizei

ren. Vor dem Hintergrund des zunehmenden Kostendrucks bei den Behörden sind neue Ideen zur effizienteren Nutzung der Ressourcen notwendig.

2. Empfindlichkeit der Reisekette

Die jüngsten Vorfälle an Bord des Delta North-West-Airline Flugs 253 von Amsterdam nach Detroit im Dezember 2009 sind ein Beweis dafür, wie anfällig das heutige Reisesystem ist. Ein Reisender versuchte, während des Fluges eine explosive Mischung zu zünden, konnte aber von Mitreisenden gestoppt werden. Dieser Fall zeigt, dass Sicherheitsbehörden trotz hoher Sicherheitsvorkehrungen nicht jede mögliche Situation abdecken. Bleiben bei den Kontrollen im Land des Reisebeginns Risiken unentdeckt, kann sich schnell eine Gefahr für das Zielland der Reise entwickeln.

Der Vorfall wirft die Frage auf, wie das explosive Material durch die Flugkontrollen in das Flugzeug gelangen konnte. Noch interessanter ist jedoch die Tatsache, dass die Sicherheitsbehörden bereits über das Gefahrenpotenzial des mutmaßlichen Täters informiert waren. Daher muss die Kernfrage lauten, warum konnte der Reisende überhaupt am Flughafen einchecken? Die Beantwortung verlangt eine nahezu unüberschaubare Sisyphusarbeit, denn mehrere tausend Meldungen über mögliche Gefahrenpotenziale gelangen täglich in die Zentralen der Sicherheitsbehörden. Nachrichtendienste, Visa-Behörden, Ausländische Botschaften, Hilfsorganisationen, Grenzschutzbeamte, Medien, Bürger und viele andere Beteiligte informieren aus In- und Ausland. Die zeitnahe Aufarbeitung dieses Puzzles gleicht der Suche nach der Nadel im Heuhaufen. Ohne Unterstützung von Informationstechnologie kann die Analyse einer solchen Datenflut kaum noch bewältigt werden. Dabei sind Art der

Speicherung, Bewertung, Vernetzung und Wiederfindung der Erkenntnis die Haupterfolgskriterien für eine intelligente Auswertung.

Es gleicht einem Desaster, wenn wie im beschriebenen Fall die Sicherheitsbehörden rückwirkend feststellen, dass eine Katastrophe bereits im Vorfeld hätte verhindert werden können, weil schon Informationen zur Gefährlichkeit des Täters vorhanden waren. Die Verantwortung aller Beteiligten in der Reisekette wird bei dem Ereignis schnell klar. Nur durch den Mut und die Zivilcourage des holländischen Bürgers Jasper Schuringa konnte der Anschlag vereitelt, Schlimmeres verhindert und die Leben von rund 300 Menschen gerettet werden. Der gute Ausgang eines solchen Zwischenfalls darf jedoch nicht vom ohne Zweifel lobenswerten Mut von Einzelpersonen abhängen. Hier stehen Staaten und Bürger in der Verantwortung. Die Aufarbeitung der Vorfälle um den Flug 253 wird zeigen, ob die zur Bewertung notwendigen Daten bekannt und richtig waren und an welcher Stelle möglicherweise Potenziale zur Verbesserung und Standardisierung des Informationsaustauschs unter den Sicherheitspartnern im In- und Ausland liegen. Erste Analysen der Geschehnisse zeigen, dass bei der Betrachtung der Gesamtreisekette neue und intelligente Ansätze zur Erhöhung der Sicherheit über die materiellen und virtuellen Kontrollpunkte hinweg erarbeitet werden können.

3. Die Idee der Integrierten Grenzverwaltung

Zurzeit erleben wir eine neue Welle der politischen Auseinandersetzung zu möglichen Maßnahmen über die Erhöhung der Sicherheit der Reisenden in Deutschland und im Europäischen Staatenverbund. Der internationale Trend der virtuellen Vorverlagerung der Grenzen sorgt dafür, dass eine Reise nicht erst bei der Landung auf dem Flughafen in Deutschland beginnt, sondern bereits bei der Reiseplanung oder Buchung. Die Reise endet entweder im Hotel des Zielortes oder mit der Rückkehr an die Startadresse.

Folgender Sachverhalt verdeutlicht die Gesamtproblematik: Momentan ist es unmöglich festzustellen, wie viele Personen sich ohne Aufenthaltserlaubnis in Deutschland befinden. Sicherheitsexperten schätzen die Zahl illegal eingereister Personen in Europa auf rund acht Millionen, wobei die Mehrzahl legal einreiste, aber die Aufenthaltsdauer überschritt. In welchem der Schengen-Mitgliedsländer diese Personen momentan verweilen, kann nicht beantwortet werden, da sich Reisende im Schengenraum ohne weitere Sicherheitskontrollen bewegen dürfen.

Aufbauend auf dem Tampere- und dem Haager Programm wurden durch die Europäische Union die Kontrollen an den



Moderne Kontrollstellen sichern Datenintegrität

Quelle: Bundespolizei

Die Evolution der Sicherheitssysteme beginnt beim anonymen Reisen, wie es beispielsweise bei der Bahn heute noch praktiziert wird. Niemand weiß genau, wer wann und wo in den Zug steigt und welche Reise-Risiken diese Person möglicherweise mit sich bringt. Im Rahmen des evolutionären Ausbaus werden als Ziel intelligente Echtzeit-Lagesysteme über alle Reiseketten (Reisende, Immigranten, Waren etc.) hinweg etabliert, wie sie in den Ideen des Stockholmer Programms in Zukunft vorstellbar sind.

Beim anonymen Reisen erfolgt der Datenaustausch durch das Prüfen der Fahrkarte. Der Vorgang dient jedoch mehr der Kontrolle der entrichteten Fahrtkosten und wird erst in Kombination mit einem Ausweis oder einem Aufenthaltstitel zu einem Sicherheits- und Transparenzgewinn. Die nächste Qualitätsstufe im Evolutionsprozess wird durch die Abfrage in einer Fahndungsdatenbank erreicht. Hier wird bereits ein erster Schritt in Richtung der Identifikation geleistet. Der Abgleich mit dem Fahndungssystem INPOL ergibt nur eine Antwort auf die Frage, ob die überprüfte Person im Fahndungssystem eingetragen ist. Nur im Trefferfall stehen weitere Informationen über den Reisenden zur Verfügung. Ein negatives Ergebnis erlaubt i.d. Regel die Weiterreise. Hier prallen internationale Personendaten aus Ländern, in denen das Geburtsjahr nur geschätzt wird, auf historisch gewachsene Ermittlungssysteme mit beeindruckender Datenqualität und funktionalen Hilfestellungen aufeinander. Dies zeigt: Das Innovationspotenzial zur Modernisierung der vorhandenen Systeme ist gewaltig.

Im nächsten Schritt können dann bereits die Passagierlisten oder Warenmanifeste vor Ankunft der Person oder Ware an den Zielort gesandt werden (Identifiziert vor Ankunft). Hier sprechen wir von einer Überprüfung der Personen, die in Verbindung mit dem Abgleich anderer Sicherheitssysteme

einen bedeutenden Schritt zur Identifikation des Reisenden ermöglicht (Zu welchen anderen Personen, Objekten und Ereignissen im Netzwerk gibt es belastbare Beziehungen?). Auch wenn zumeist nur mit einem einzigen Fahndungssystem geprüft wird, so ist der zeitliche Vorlauf ein entscheidender Qualitätsgewinn. Die Prüfung nur weniger Datenbanken ist relativ trivial und kann mit den einfachen Mitteln eines Massendatenabgleichs vorgenommen werden. Mit jeder weiteren Kontrolle in anderen Datenpools steigt die Komplexität exponentiell. Hier ist die Etablierung einer belastbaren und serviceorientierten Datenaustauscharchitektur dringend anzuraten. Nicht selten müssen über 30 IT-Systemstandards durch die Sicherheitsbehörden zur Annahme der Passagier-Listen (PAX) von den Beförderungsunternehmen unterstützt werden, obwohl die Felder und die Reihenfolge der Austauschinformationen gesetzlich vorgeschrieben wurden.

Zur Erhöhung der Transparenz bei der Reise sind die Informationen unter den Beteiligten Partnern standardisiert auszutauschen. Je konstruktiver und aktueller der Austausch ist, umso wirksamer können Sicherheitsvorkehrungen greifen.

Eine große Problemstellung wird durch die sogenannten "Non-Arrival-Maßnahmen" sichtbar. Sollte ein Passagier ohne gültige Reisedokumente in ein anderes Land reisen, so wird die Einreise verweigert. Die Beförderungsträger sind verpflichtet, die Passagiere auf deren eigene Kosten zurückzubringen. Die Behörden erkennen, dass eine verantwortungsvolle Echtzeit-Entscheidung über die Ein- und Ausreise von Reisenden, die sogenannte "Authority to Carry" nur mit genauen Hintergrundprüfungen von erweiterten Passagierdaten möglich ist. Ein großes Problem stellt hier der Datenschutz dar. Jedoch zeigt die Erfahrung, dass durch das Prinzip der Freiwilligkeit mögliche Ansätze umsetzbar sind. Tests bestätigen, dass die Bereitschaft der Reisenden im Sinne einer erhöhten Reisesicherheit und besserem Reisekomfort durchaus für die freiwillige Erhebung vorhanden ist.

Dazu ist ein Risikomanagement über den Gesamtreiseprozess notwendig, das mit bisherigen Sicherheitsinstrumenten schwer abbildbar ist. Allein die ausländische Schreibweise von Eigennamen überfordert ältere IT Systeme, die auf Fragestellungen nur mit "Ja" oder "Nein" antworten können. System-Vorschläge, die zur optimierten Steuerung der Kontrollkräfte notwendig wären, automatische Alarmgenerierungen und Weiterleitung über den Datenfunk an den zuständigen Diensthabenden und die Kontrolltiefe für die Sicherheitskräfte, sind aktuell noch Zukunftsmusik.

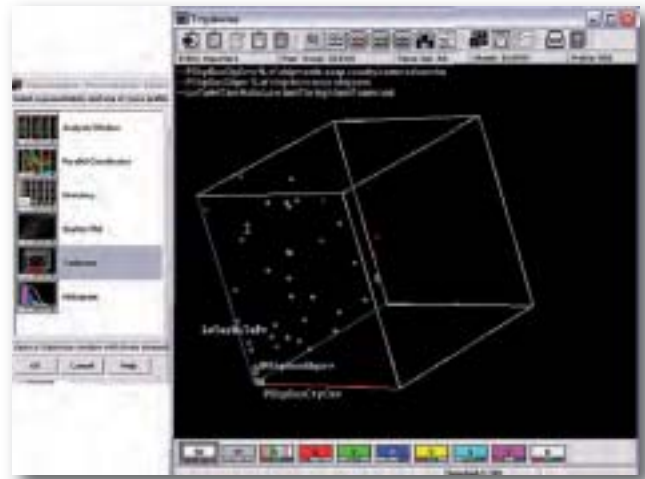
Wahrscheinlichkeiten, Schlüsselfiguren und Hintergrundnetzwerke sind schwierig oder sehr zeitaufwändig abzubilden. Letztendlich können diesbezügliche Fragen, wie beispielsweise welche Personen sich unerlaubt in Deutschland aufhalten, nicht beantwortet werden. Bisherige Mechanismen sind zumeist statischer Natur. Wenn sie greifen, dann hat sich die Form der Kriminalität bereits gewandelt. Die Kosten der ständigen Aktualisierungen lähmen die Verwaltungen und die Zeitspanne bis zur Wirksamkeit der Mechanismen ist beachtlich. Mit Dynamischem Risiko-Profilung können Risikogruppen identifiziert werden und spezifischen Bewertungen unterzogen werden.

In der mittelfristigen Erreichbarkeit steht ein Cockpit für ein Integriertes e-Border Lagezentrum, das die aktuelle Situation über die Reiseströme von Personen- und Warenströmen transparent darstellt, kritische Situationen frühzeitig erkennt und entsprechend entschärft. Für die Entscheidungsträger im Sicherheitsbereich wird ein Instrument der Vorhersage und Planung etabliert, das legale Daten austauscht und mehr Services sowie Sicherheit für die Reisenden bietet. Identifizierte Gefahrensituationen werden über regelbasierte Lösungen direkt an die verantwortlichen Diensthabenden per Datenfunk übermittelt.

Einzelne Länder in Europa haben derartige Systeme bereits erfolgreich erprobt und können auf beachtliche Erfolge verweisen. Zu dem bekanntesten Projekt zählt "Semaphore" in Großbritannien, bei dem in der Zeit von 2005 bis 2008 Daten zwischen 103 Fluggesellschaften und Beförderungsinstitutionen und mehreren Sicherheitsdiensten ausgetauscht wurden. Dabei wurde auf 182 Linien mit über 30 Millionen Reisebewegungen eine risikorelevante Steuerung der Sicherheitsbehörden getestet. Ergebnis des Tests waren 20.000 Hinweise und 1.700 Festnahmen. In den nächsten Jahren ist der Ausbau des Systems auf alle Kontrollstellen des Landes beabsichtigt. Die Einbindung von Unternehmen der Industrie konnte bei der Etablierung einer neuen e-Border Architektur mit den zugehörigen Standards und Service-Definitionen helfen.

5. Risikomanagement im Reiseverkehr

In den letzten Jahren hat sich die Entwicklung von Risikomanagement-Systemen sehr erweitert. Im Bereich der Netzwerkforschung versuchen Wissenschaftler soziale Phänomene mit naturwissenschaftlichen Methoden zu beschreiben. Hierbei spielen auch Verbreitungen von Gerüchten zur Bewertungen von Informationen oder massenhaftes soziales Verhalten bei Migrationen eine Rolle. Die Bedeutung von Multiplikatoren, sogenannten "Superspreaders", erklärt Pro-



Risikomanagement-System RMS der IBM

Quelle: IBM

fessor Nicholas Christakis in seinem Buch "Connected". Er beschreibt darin Regeln, wie sich Einflüsse in Netzwerken entwickeln und gegenseitig beeinflussen.

Gerade hier wird die Wissenschaft beim Design von angemessenen intelligenten Überprüfungen in den neuen Sicherheitsarchitekturen helfen. Zukünftige Netzwerk-Analysen in Echtzeit werden die Evolution der Reise- und Migrationssystem beeinflussen.

Moderne Risikomanagement-Systeme bewerten alle verfügbaren Faktoren einer Reisebewegung und filtern Auffälligkeiten heraus. Erst durch eine Darstellung im mehrdimensionalen Raum können Reisetransaktionen, die sich eigentlich in einer Wolke von Massenreise-Transaktionen verstecken, hervorgehoben werden. Die Abweichungen bei einzelnen Faktoren, wie Alter oder Reiseroute liefern noch keine Indizien für eine Auffälligkeit. Erst im Vergleich innerhalb sogenannter Peergroups (Gruppen mit vergleichbaren Eigenschaften, wie etwa bestimmte Vielreisende) lassen sich Besonderheiten extrahieren. Hierzu ist in erster Linie mathematisches und analytisches Knowhow notwendig, um geeignete Regeln für die Risiken zu extrahieren. Ob diese Regeln dann sofort scharf geschaltet werden, entscheiden Rechts- und Fachexperten anhand der Parameter für die Auffälligkeit.

Derartige Ansätze werden bereits bei Zoll- und Steuerverwaltungen oder zur Entdeckung von Sozialmissbrauch erfolgreich eingesetzt. Eine manuelle Erkennung aller Regeln, hinter denen sich Risiken verbergen, ist bei der Komplexität und der hohen Dynamik des Umfeldes kaum noch möglich. Ein interessanter Nebeneffekt des Risikomanagements ist die Qualitätssicherung der Fachprozesse. Wenn beispielsweise deshalb Fehler nicht erkannt werden, weil möglicherweise hohe Krankenstände, Abarbeitungsstaus, Kommunikationsproble-



Mehr Komfort für Reisende und bessere Erfassung für die Sicherheitsbehörden *Quelle: Bundespolizei*

me oder sogar Weiterbildungsstatus erkannt werden, so sind hier entsprechende Chancen für die weitere Verbesserung der Geschäftsprozesse realisierbar. Ein Risikomanagementsystem kann bei der Optimierung helfen und Empfehlungen für die Verbesserung der Dienstplanungen generieren.

6. Aktivitäten in Deutschland

Bereits 2005 wurde begonnen, den elektronischen Reisepass in Deutschland einzuführen, um die Identitätsprüfung der Reisenden entsprechend der internationalen Standards umzusetzen. Nach Aussagen des BITKOM wurden allein in den ersten zweieinhalb Jahren rund sechs Millionen Reisepässe ausgestellt. Damit hat die Bundesregierung den Weg in Richtung elektronischer Grenzkontrollen geebnet und mit ersten Projekten begonnen.

Ende 2007 wurde eine Novelle des Bundespolizeigesetzes (BPolG) verabschiedet. In den Paragraphen 31a und 32 sind die Übermittlungen von Fluggastdaten und personenbezogenen Daten neu geregelt worden. Auf Anfrage müssen die Flugunternehmen bei Boarding-Ende ausgewählte Daten nach einem vorgegebenen Format an die Bundespolizei zur Prüfung übertragen. Diese können dann für Hintergrundanfragen oder Weiterleitungen an Drittstellen (§32) genutzt werden und unterliegen strengen Speicherregelungen.

Mit EasyPass¹² läuft auf dem Frankfurter Flughafen seit Ende 2009 ein Projekt zur IT-gestützten Grenzkontrolle, das die Abfertigung von Fluggästen vereinfachen soll. Rund 240 Personen aus der EU sollen pro Kontrollspur und Stunde mit dem elektronischen Reisepass abgefertigt werden. Ein Kontrollsystem vergleicht drei aktuelle Kamerabilder mit dem digitalen Bild in einem Speicherchip des Passes. Bei Abweichungen erfolgt eine Ausleitung zu einer gesonderten

Kontrolle. Die Testphase soll bis März 2010 andauern und möglicherweise erweitert werden.

Die etablierten Mittel und Methoden zeigen, dass der Staat an unterschiedlichen Stellen an der Erhöhung der Grenzsicherheit arbeitet. Mit der Einführung von elektronischen Reisepässen werden erste internationale Standards für eine einfachere Identifikation eingeführt. Im Vergleich zu Partnerländern in Europa oder den Ideen der EU im Stockholmer Programm wirken die Maßnahmen allerdings zu kurz gegriffen. Die Lösungen und Potenziale der ITK Industrie werden bisher nur wenig genutzt.

In der politischen Debatte muss eine Balance zwischen den Persönlichkeits- und Freiheitsrechten des Reisenden und der Sicherheit der Gemeinschaft gefunden werden. Dabei bietet sich eine Breite von Handlungsoptionen an, die sich oftmals auf den althergebrachten Grenzübertrittspunkt konzentrieren.

Die Kontrolle der Fluggäste mit Ganzkörper- oder "Nacktschannern" zählt zu den aktuellsten Lösungsvorschlägen, wobei hierbei nur in "Hardware" und nicht in intelligente Lösungen investiert wird. Die Risiken entlang der Reisekette, die durch das vorhandene Personal in den Flughäfen entstehen, werden kaum beachtet. Unabhängig von der Verträglichkeit und den ethischen Fragestellungen zu modernen Scan-Systemen wird in den kommenden Monaten über den Nutzen und die Einsatzmöglichkeiten entschieden.

Die Wachstumsdimensionen in Richtung des Seeverkehrs oder sogar der Bahnverbindungen befinden sich im Gegensatz dazu derzeit noch nicht auf dem Themen-Radar. Jedoch sind auch diesbezüglich im Sinne der Integrität der Grenzen wirksame Maßnahmen mittelfristig notwendig. Die Grundlagen dafür müssen durch fundierte Forschungsarbeiten und entsprechende Praxistests geschaffen werden.

Die nächsten Jahre werden zeigen, welche Rolle Deutschland bei der Etablierung neuer e-Border Konzepte einnehmen wird. Die ITK Industrie wünscht sich mehr Kooperation mit den Behörden in diesem Bereich, um gemeinsam den Führungsanspruch bei den Innovationen im Bereich sicherer und bequemer Grenzübertritte im zusammenwachsenden Europa auszubauen.

7. E-Border Roadmap der BITKOM

Bereits 2007 wurde in der Arbeitsgruppe "Border Control" des BITKOM Arbeitskreises "Öffentliche Sicherheit" eine Liste mit Empfehlungen an die Entscheidungsträger im Sicherheitsumfeld aus Sicht der Informations- und Kommunikationsindustrie erarbeitet. Das Dokument beschreibt den Trend

der frühzeitigen Erhebung von Reisedaten zur Aufsetzung eines dynamischen Risikomanagements und die weitere Verbesserung des Austauschs unter den Sicherheitsbehörden. Die Ideen wurden in unterschiedlichen Veranstaltungen mit Entscheidungsträgern diskutiert und lieferten Impulse für weitere Maßnahmen. Die ITK Wirtschaft wünscht mehr Einbindung in die Lösungsumsetzung, um frühzeitig in Ressourcen und Technologien zu investieren. Bisher zählen Investitionen im Bereich der Reisesicherheit durch IT nicht zu den Aktionsschwerpunkten. Das spiegelt sich auch in der geringen thematischen Schwerpunktlegung bei den aktuellen Forschungsprogrammen wider. Hierzu sind entsprechende Impulse zwischen der IT Industrie und den Sicherheitsbehörden notwendig, als deren Botschafter BITKOM in vielen Bereichen bereits einen erstklassigen Dialog etabliert hat. Die jüngsten Vorfälle des Sprengstoffanschlags auf dem Flug 253 und das Stockholmer Programm der Europäischen Union bescheinigen die Aktualität des Themas "Border Control". Durch die intensive und kontinuierliche Zusammenar-

beit von Sicherheitsbehörden, Entscheidern und Entwicklern kann es weiter gedacht und vorangetrieben werden – für mehr Sicherheit trotz sich öffnender Grenzen.

Autor: Dipl. Ing. Jörg Scholz (47) arbeitet seit 15 Jahren im Sicherheitsumfeld und ist bei der IBM Deutschland GmbH als Executive für Lösungen der Öffentlichen Sicherheit beschäftigt. In einem internationalen Netzwerk arbeitet er eng mit den IBM Sicherheitsexperten innerhalb der EU zusammen. Als Mitglied im Vorstand des BITKOM-Arbeitskreises "Öffentliche Sicherheit" leitet Herr Scholz die Arbeitsgruppe "Border Control".



Bringing service to life

serco

Serco: Partner der Bundeswehr



Serco ist ein führender Anbieter von Unterstützungsleistungen im Verteidigungsbereich. Seit über vierzig Jahren unterstützt Serco die Bundeswehr. Wir beraten, entwickeln technische Lösungen, integrieren Systeme und setzen komplexe Betreiberaufgaben um.

- **Systemunterstützung:** Serco unterstützt als Dienstleister die Bundeswehr im Bereich des Einsatzführungsdienstes und der Dokumentationserstellung sowie der Radarvermessung.
- **Systemintegration:** Serco mobilisiert Systeme und Komponenten für Out of Area Einsätze
- **Elektromagnetische Verträglichkeit (EMV):** Serco betreibt akkreditierte EMV-Zentren in Bonn und Ottobrunn
- **IT-Lösungen:** Serco konzipiert, realisiert und implementiert qualitätsgesicherte IT-Lösungen, die unter Nutzung modernster Infrastrukturen für den Kunden betrieben werden.
- **Interaktives Training und Emulation:** Serco setzt an der Schnittstelle zwischen Technik und Mensch auf interaktives Training und Emulation.

Mehr Informationen unter: www.serco.de

Serco GmbH
Autla-von-Weibig-Str. 18
53121 Bonn

Telefon: 0228/6681-367
Fax: 0228/6681-747
E-Mail: info@serco.de