

Was gibt's Neues vom Hydranten?

Der „Heimatschutz“ als neues Geschäftsfeld der Sicherheitsindustrie

Von Andrea Stercken

Der wachsende Sicherheitsbedarf lässt einen neuen Markt entstehen. Das amerikanische Magazin „Wired“ sprach kürzlich sogar von der „größten Marktchance seit dem Dotcom-Boom“. Die Euphorie in diesen Worten ist durchaus geschmacklos – wird dabei doch geflissentlich unter den Tisch gekehrt, dass immerhin der Dotcom-Boom nicht Tausenden von Toten, Krieg, Zerstörung und Terrorismus geschuldet war.

Denn verglichen mit dem Budget des „Departments of Homeland Security“ in den USA, das allein in diesem Jahr rund 40 Milliarden US-Dollar beträgt, sind die Investitionen

hier zu Lande noch gering. Fest steht aber, dass die öffentliche Hand schon heute ein wichtiger Auftraggeber für die IT-Industrie ist, die sich mit Lösungen für den „Heimatschutz“ befasst. Zu verstehen sind darunter neue Sicherheitstechnologien, die die Bevölkerung vor Terrorismus, Naturkatastrophen und Pandemien schützen sollen. Dazu gehören etwa biometrische Grenzkontrollsysteme oder Leitzentralen, die Rettungshelfer im Notfall schneller zum Einsatzort bringen. Nach Schätzungen der Analysten von Pierre Audoin Consultants sollen 2008 mehr als 2,5 Milliarden Euro in entsprechende IT-Projekte investiert werden. Das ist rund eine halbe Milliarde mehr als noch im Jahr 2004.

Auch beim Branchenverband Bitkom stehen die Zeichen auf Homeland Security: Dort kümmert sich seit Beginn vergangenen Jahres eine ei-

gene Projektgruppe, bestehend aus 60 Unternehmen, um die Verzahnung nationaler und europäischer Sicherheitsforschung. Nach den Vorstellungen des Verbands solle ein leistungsfähiges ITK-System die Basis für ein virtuelles Informations- und Leitsystem bilden, das die Gesellschaft im Krisenfall bis in das letzte Ende informiert. Aufgabe der IT-Firmen sei es, so Bitkom-Projektleiter Michael Bartsch, kritische Infrastrukturen abzusichern und Informationsverbünde zu planen, die bei Bedrohung schnell aktiviert werden können. Die Schwerpunkte der Projektgruppe liegen bei der Grenzkontrolle, dem Katastrophenmanagement sowie Dienstleistungen und Prozessen bei den kritischen Infrastrukturen.

„E-Pass“ erleichtert Grenzkontrolle

Der Bedarf ist groß an neuen Lösungen zum Schutz der inneren und äußeren Sicherheit. Aufwind erhält der Markt etwa durch neue gesetzliche Regelungen der Europäischen Union. Diese hatte im Juni vergangenen Jahres beschlossen, das digitale Bild oder den Fingerabdruck künftig als verpflichtendes biometrisches Element in Reisepässe aufzunehmen. Spätestens ab 2009 soll der Fingerabdruck als zweites, zusätzliches Merkmal hinzukommen.

Mirko Panev, Leiter Homeland Security bei Siemens IT Solutions and Services (www.siemens.com/it-solutions), sieht für die weitere Entwicklung elektronischer Passlösungen

drei Trends: Im ersten Schritt müssten die Behörden in den EU-Ländern mit biometrischen Systemen ausgerüstet werden, um die Ausweisdokumente ausgeben zu können. Deutschland hat



Welche sicherheitsrelevanten Informationen sich hier unterbringen lassen, wissen vermutlich nur Experten.

dabei die Nase vorn: Seit November 2005 werden hier zu Lande so genannte E-Pässe verteilt. Jedes neue Reisedokument enthält einen RFID-Chip, auf dem das Gesicht des Passinhabers gespeichert ist. Damit hat die Bundesrepublik schneller als jedes andere Land das EU-Passgesetz in die Praxis umgesetzt.

Um die Daten in den Pässen auch lesen zu können, müssen im zweiten Schritt die Grenzkontrollsysteme angepasst werden. Das erste Land, in dem das schon bald möglich sein wird, ist Kroatien. Dort implementiert der IT-Dienstleister derzeit am Flughafen Zagreb und am Grenzübergang Bajakovo ein Grenzkontrollsystem, das auch die neuen biometrischen EU-Pässe auslesen kann. Die Grenzbeamten gleichen hierzu die Reisedokumente mit einer zentralen Datenbank ab, in der biometrische Merkmale, Passbilder und die Gültigkeit von Visa hinterlegt sind. Die Lösung ist in diesem Februar in Betrieb gegangen. Mit der neuen Grenzkontrolle erfüllt Kroatien das Schengener Abkommen – die Voraussetzung für den geplanten EU-Beitritt 2009.

Ein weiteres Pilotprojekt mit biometrischen Systemen ist Ende 2006 am Frankfurter Flughafen in Betrieb gegangen. Dort beteiligt sich die Lufthansa an einem Versuch der Bundespolizei zur Automatisierung der Grenzkontrollen. Passagiere können sich dort mit ihren Daten aus dem Reisepass und einem Irisscan registrieren lassen.

Daten vor Manipulation schützen

In einem dritten Schritt könnten biometrische Verfahren auch bei anderen Ausweisdokumenten zum Einsatz kommen. Denn die neue Infrastruktur bildet eine gute Basis, um nationale ID-Systeme für Personalausweise oder Führerscheine aufzubauen. So hat die Bundesregierung Ende 2006 eine Novelle des Personalausweisgesetzes geplant, der zufolge biometrische Daten in die Personalausweise aufgenommen werden. Auch eine Kopplung mit Funktionen der elektronischen Signatur ist denkbar.

Ein entscheidender Aspekt bei den neuen biometrischen Ausweisen ist die Aufnahme der Daten in einem sicheren Prozess: Die biometrischen Daten müssen durch hohe Verschlüsselung vor unbefugtem Zugriff geschützt werden. Multiple Systeme, die zwei bis drei biometrische Merkmale kombinieren, verbessern die Sicherheit entscheidend. Außerdem muss gewährleistet sein, dass die Daten nur von zertifizierten Systemen ausgelesen werden und der gesamte Prozess unter Aufsicht stattfindet. Die Europäische Kommission hat kürzlich ein Verfahren verabschiedet, nach dem nur eigens berechnete Lesegeräte Fingerabdrucke entschlüsseln können.

Eine weitere EU-Vorgabe lautet, einheitliche europäische Notrufnummern zu schaffen. Alle Mitgliedsstaaten sind gehalten, sukzessive die technischen Voraussetzungen zu schaffen, um überall und jederzeit

unter „112“ Hilfe anfordern zu können. Italien hat diese Anforderung bereits umgesetzt. Wer 112 wählt, erreicht die Einsatzleitstellen der Carabinieri. Über ein mobiles Notrufsystem sind dort 8.000 Einsatzfahrzeuge und Streifenpolizisten mit über 100 Provinzkommandanturen vernetzt. „Motorisierte Patrouillen und Fußstreifen können so im gesamten italienischen Staatsgebiet über Funk lokalisiert werden“, erläutert Oberst Luigi Robusto, CIO Telematic Systems, Arma dei Carabinieri.

Das Notfallmanagement umfasst vielerlei Anforderungen: Dazu gehören der transparente Informationsfluss, sparsames Ressourcenmanagement, aussagekräftige Statistiken, eine kosteneffektive Systemverfügbarkeit und die rasche und angemessene Reaktion auf alle Arten von Einsätzen. Denn medizinische Notfälle erfordern Informationen über Spezialkliniken oder diensthabende Ärzte. Feuerwehrleute benötigen Angaben zu Hydranten oder Gebäudezugängen. Die Polizei muss in der Lage sein, bei Verkehrsunfällen oder Straftaten jene Streife zum Einsatz zu rufen, die den kürzesten Weg hat.

Schnelle Datenübermittlung

Die Terroranschläge in Madrid im März 2004 haben klar gemacht, dass die schnelle Datenübermittlung zwischen den Mitarbeitern in der Zentrale und den verschiedenen technischen Bereichen lebensrettend sein kann. „Durch die Bündelung von Po-

Buch-Tipp

Nicolas P. Sokianos (Hrsg.)

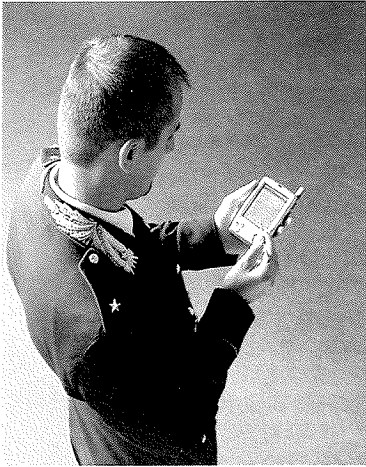
Produkt- und Konzeptpiraterie

Erkennen, vorbeugen, abwehren, nutzen, dulden

2006, 340 Seiten
EUR 49,90

Verlag Dr. Th. Gabler, Wiesbaden

Jährlich entstehen durch Produktpiraten Schäden in Millionenhöhe. Das Buch bietet neben Daten, Fakten und Fallbeispielen auch konkrete Empfehlungen für den Umgang mit Produkt- und Konzeptpiraterie im Unternehmen. Relevant ist das für nahezu alle Unternehmensbereiche, denn es geht nicht nur um den Schutz der eigenen Produkte vor Fälschung, sondern auch um den Schutz vor illoyalen Vertragspartnern, etwa in der Entwicklung, vor plagiierenden Lieferanten und um personalpolitische Aspekte. Das Buch stellt Beispiele vor aus der Automobil-, Software-, Textil- und Pharmaindustrie sowie aus dem Anlagen- und Gerätebau. Auch der Nutzen von Produktpiraterie – den gibt es tatsächlich! – wird behandelt. Der Autor, ehemals Industriemanager, ist Berater der Industrie und der produktionsnahen Dienstleistungen im In- und Ausland sowie Leiter des Studiengangs International Technology Transfer Management an der University of Applied Science, Berlin. Außerdem ist er im Vorstand der Gesellschaft für Produktmanagement e. V.



Europaweit einheitliche Notrufnummern tragen wesentlich zur Sicherheit der Bevölkerung bei. Wer beispielsweise in Italien die 112 wählt, erreicht die Einsatzleitstellen der Carabinieri. Über ein mobiles Notrufsystem sind dort 8.000 Einsatzfahrzeuge und Streifenpolizisten mit über 100 Provinzkommandanturen vernetzt.

lizei und Feuerwehr bis hin zu ambulanten Notdiensten konnten viele Verletzte in kurzer Zeit versorgt werden“, so Ignacio Mora Rey, als Direktor zuständig für Notfallmanagementlösungen bei Siemens IT Solutions and Services in Spanien. Ein anderes Beispiel sind die Hurrikans im Süden der USA, wo ganze Küstenabschnitte gleichzeitig versorgt werden mussten. Oder erdbebengefährdete Millionenstädte wie Teheran, wo bei

einer Katastrophe gleichzeitig mehrere tausend Menschen versorgt werden müssen. „Ohne intelligente Systeme, welche die vorhandenen Ressourcen optimal nutzen, ist dies nur unzureichend möglich“, ergänzt Panev.

In zahlreichen Städten und Regionen der Iberischen Halbinsel wie Madrid, Barcelona sowie in Aragón, Extremadura, Kastilien, Asturien, Katalonien und auf den Balearen hat die Siemens-Tochter Notfallmanagementsysteme installiert. Der Erfolg solcher Systeme ist beachtlich: In Ma-

drid sank seit der Installierung vor zehn Jahren die Sterberate der Opfer um mehr als 50 Prozent. Dazu trug nicht zuletzt die Ausrüstung der Rettungswagen mit PCs bei, in denen noch während der Fahrt die Patientendaten erfasst und per Funk oder GPRS in die Klinik übertragen werden. Parallel können dort die Vorbereitungen für Aufnahme und Versorgung sofort anlaufen. Selbst nach der Einlieferung wird der Gesundheitszustand der Patienten weiter von den Disponenten verfolgt. So lassen sich mitunter Rückschlüsse auf die Qualität der Versorgung durch die Rettungskräfte ziehen. Die Daten fließen in das Qualitätsmanagement ein und helfen, Notfalleinsätze weiter zu optimieren.

Sichere Zukunft

„Informations- und Kommunikationstechnologien leisten einen großen Beitrag für mehr Sicherheit“, fasst Panev zusammen. Auch Großereignisse wie die vergangene Fußball-Weltmeisterschaft bestätigen das hohe Interesse an ITK-Systemen für Homeland Security. An der Vorbereitung der nächsten Sportgroßveranstaltungen, etwa der Fußball-Europameisterschaft 2008 in Österreich und der Schweiz wird bereits mit Hochdruck gearbeitet. Der Experte blickt in die Zukunft: „Der Markt wird so lange weiter wachsen, bis ein Sicherheitsniveau erreicht ist, das den Bedürfnissen der Bürger entspricht.“

Oder dem der Politiker und Sicherheitsanbieter. □

Das Serienmörder-Prinzip

Die böse Tat in sieben Phasen –
Teil 1: Genese, Identifikation, Antizipation

Von Stephan Harbort

Serienmörder – das Wort schürt Urängste: Hier droht tödliche Gefahr. Grausamkeit und Erbarmungslosigkeit kennzeichnen die Täter als vermeintliche „Unmenschen“, die Unheil über ihre Mitmenschen bringen, Leben auslöschen. Und gerade deshalb rücken sie vielfach und leicht in den Blickpunkt öffentlichen Interesses. Sie inszenieren ein Drama, an dem nur sie selbst freiwillig teilnehmen. Auch wenn es kaum jemand wahrnimmt – sie kommunizieren mit uns. Aufgeführt wird immer dasselbe Stück: die Verstümmelung der Humanität und ihrer Spielregeln.

Die einschlägigen Wissenschaften hinken mit ihren Deutungen, Erklärungen und theoretischen Annäherungsversuchen der Verbrechensentwicklung indes hoffnungslos hinterher. Der vermeintlich tiefe Blick in Kopf und Seele des Killers erweist sich immer wieder als simple Projektion eigener Erwartungen und Vermutungen. Es erscheint sinnvoll, sich bei der Suche nach einem beschreibenden Grundmuster von formalen Kategorien wie Tätertyp, Motive, Lebensläufe, Persönlichkeitsstörungen oder sexuellen Perversionen als Leitbild zunächst zu lösen. Diese in anderer Hinsicht durchaus wichtigen Aspekte sind unter dem Blickwinkel einer Serienmord-Matrix nämlich lediglich Mosaiksteinchen. Dennoch müssen diese Erkenntnisse als empirische Basisinformationen bei der Entwicklung eines Konzepts Berücksichtigung finden.

Serienmörder werden nicht als solche geboren und auch nicht zu solchen gemacht. Menschen entwickeln sich zu Tätern, durchlaufen dabei verschiedene Phasen. Insofern erscheint