

Dokumentation

zum

**Agenda-Workshop
zur Fortschreibung des Programms
„Forschung für die zivile Sicherheit“**

**„Herausforderungen
für
Unternehmen und Wirtschaft“**

2. November 2010

Gustav-Stresemann-Institut Bonn

Langer Grabenweg 68

53175 Bonn

Inhaltsverzeichnis

Tagesordnung 3

Ergebnisse 5



Workshop „Herausforderungen für Unternehmen und Wirtschaft“

im Rahmen des Agenda-Prozesses zur Fortschreibung
des Programms „Forschung für die zivile Sicherheit“

Tagesordnung

Termin: 2. November 2010

Ort: Gustav-Stresemann-Institut in Bonn

Zeit	Thema
ab 10:00	Anmeldung, Begrüßungskaffee
10:30	Einleitung und Ziel des Workshops <i>Dr. Stefan Mengel, BMBF</i>
10:40	Zum Stand der Forschung <i>Dr. Joachim Schaper, SAP AG</i> Forschungsprojekte des laufenden Programms <i>Dr. Stefan Mengel, BMBF</i>
11:10	Impulsstatements: Sicherheit im Kontext globaler Trends Bedrohungen durch Extremismus, Terrorismus und organisierte Kriminalität <i>Prof. Dr. Dr. Hans-Joachim Giessmann, Berghof Conflict Research</i> Risiken durch natürliche oder anthropogene Katastrophen <i>Norbert Pieper, Deutsche Post DHL</i> Risiken durch eine technisierte und global vernetzte Welt <i>Herbert Kurek, Bundesamt für Verfassungsschutz</i> Diskussion
12:20	Einführung in die Arbeitsgruppen <i>Dr. Andreas Hoffknecht, VDI Technologiezentrum GmbH</i>

12:30	Mittagsimbiss
13:30	Identifizierung von Forschungsansätzen (in parallelen Arbeitsgruppen): AG1: „Extremismus, Terrorismus und organisierte Kriminalität“ <i>Jürgen Ebner, Bundeskriminalamt</i> AG2: „Natürliche oder anthropogene Katastrophen“ <i>Dr. Dennis Göge, DLR</i> AG3: „Technisierte und global vernetzte Welt“ <i>Michael Bartsch, T-Systems Enterprise Services GmbH</i>
15:15	Kaffeepause
16:00	Vorstellung und Diskussion der Ergebnisse aus den Arbeitsgruppen
17:15	Ende der Veranstaltung

Ergebnisse

Ziel des Agenda-Workshops „**Herausforderungen für Unternehmen und Wirtschaft**“, an dem 63 Teilnehmer aus Industrie, Forschung und dem Endnutzerbereich teilnahmen, war es, in diesem Kontext die Risiken und Forschungsfragen der zivilen Sicherheit zu diskutieren, die vorrangig die Sicherheitsbelange **von Unternehmen** sowie den Schutz des **Wirtschaftssystems** betreffen. Dabei wurde im Workshop vor allem der Einfluss mittel- und langfristiger Trends für den Bedarf an ziviler Sicherheit betrachtet, wie beispielsweise Internationalisierung, Privatisierung, technische Vernetzung etc. sowie die Auswirkungen globaler Entwicklungen oder Bedrohungen, wie etwa dem Klimawandel oder den Erscheinungsformen des transnationalen Terrorismus und der organisierten Kriminalität.

Im Rahmen des Workshops wurden deshalb drei Arbeitsgruppen zu den Themenschwerpunkten „**Extremismus, Terrorismus und organisierte Kriminalität**“, „**Natürliche oder anthropogene Katastrophen**“ und „**Technisierte und global vernetzte Welt**“ gebildet, die die Aufgabe hatten, auf der Basis der in den Themenschwerpunkten adressierten Herausforderungen, **Bedarfs- und Forschungsthemen** mit geeigneten Umsetzungs- und Anwendungsperspektiven zu identifizieren.

Das Ergebnis lässt sich in fünf thematische Bedarfsschwerpunkte gliedern:

1. **Schutz vor Wirtschaftskriminalität und Industriespionage**

- Bereitstellung einer quantitativen und systematischen Datenbasis bzw. von Methoden zur Schaffung verbesserter Erkenntnisgrundlagen in der „Dunkelfeld“-Forschung
- Lösungen und Konzepte zur Durchführung dynamischer Bedrohungsanalysen, z.B. zu zukünftigen Bedrohungsentwicklungen und Täterprofilen insbesondere im Bereich der organisierten Kriminalität
- Verbesserte Mustererkennung zur Analyse von Verkehrsdaten und Kommunikationsverbindungen im Internet, z.B. für die frühzeitige Aufklärung und Abwehr von Industriespionage
- Verbesserte Verfahren und Technologien zur Sicherstellung von Produktauthentizitäten und für die Aufdeckung von Produktfälschungen bzw. -täuschungen, z.B. durch die Entwicklung intrinsischer Marker, personeller Authentifizierungsmethoden oder optimierter Analyseverfahren

2. **Sicherheits-Governance, Organisationsstrukturen und -kulturen**

- Entwicklung von verbesserten Lösungen und Konzepten für Public-Private-Partnership-Modelle in der Sicherheitsvorsorge
- Ganzheitliche und institutionell übergreifende Kooperationsmodelle (Staat - Unternehmen - Gesellschaft) unter Einbeziehung der jeweiligen Organisationskulturen

3. **Betriebliches Kontinuitätsmanagement in Katastrophen- und Krisenlagen**

- Entwicklung neuer Trainingsmethoden und verbesserter Informationssysteme zur Kompetenzentwicklung in Bezug auf das Risiko- und Gefahrenpotential in Unternehmen
- Ganzheitliche Informations- und Kommunikationsstrategien zur effizienten und institutionsübergreifenden Krisenreaktion

- Betriebswirtschaftliche Forschung zur Unternehmensresilienz, z.B. zum „Return of Invest“ der Risikovorsorge in Unternehmen

4. Sicherheit von kritischen Infrastrukturen und IT-basierten Systemen und -Produkten

- Untersuchung der (branchenspezifischen) Auswirkungen des Ausfalls kritischer Unternehmensinfrastrukturen und -prozesse für Betreiber und Nutzer
- Methoden und Verfahren zur Modellierung und zum Management von Interdependenzen in und zwischen kritischen Infrastrukturen
- Entwicklungen von Konzepten und Lösungen zur sicheren Gestaltung und Nutzung des Cloud-Computings z.B. im Rahmen unternehmerischer Kommunikations- und Transaktionsprozesse
- Sicherung von Produktions- und Prozesssteuerungssysteme bzw. Verbesserung industriespezifischer Sicherheitsarchitekturen, z.B. durch die Entwicklung sich selbstschützender IT-Systeme
- Entwicklung von ganzheitlichen Sicherheitskonzepten zur Personen- und Frachtkontrolle, z.B. durch die Integration von Sensornetzwerken oder verbesserten Aus- und Weiterbildungsmaßnahmen

5. Übergeordnete Querschnittsthemen

- Entwicklung von Werkzeugen u. Methoden der Risikoanalyse, -bewertung und -priorisierung, z.B. für „proaktive“ Risikoanalysen oder die branchenspezifische Erhebung von Risiken
- Moderne Aus- und Weiterbildungskonzepte, z.B. für verbesserte Aus- und Weiterbildungsmaßnahmen für (privates) Sicherheitspersonal
- Entwicklung ganzheitlicher Standardisierungskonzepte und -strategien, z.B. zur Zusammenführung von technologischen Insellösungen oder zur Festlegung einheitlicher Weiterbildungsstandards in BOS und Unternehmen

Wichtige Aussagen aus den Plenumsdiskussionen und Impulsstatements

- Aufgrund der vielfältigen und zum Teil neuen (asymmetrischen) Bedrohungen ist es notwendig in Zukunft die verschiedenen Handlungsstrategien und Maßnahmen zur Erhöhung der Sicherheit in Unternehmen stärker zu priorisieren.
- Hinsichtlich einer ganzheitlichen, effizienten und auf unternehmensspezifische Risiken ausgerichteten Sicherheitspolitik wird es immer wichtiger, auf der Basis fundierter Risikobeurteilungen bzw. -priorisierungen sowie entsprechender Bedrohungsanalysen, institutionsübergreifende Kon-

zepte und verbesserte institutionalisierte Kooperations- bzw. Public-Private-Partnershipmodelle zu entwickeln.

- Unternehmen sollten innerhalb des Sicherheitsforschungsprogramms und im Kontext der Herausforderungen für Unternehmen und Wirtschaft nicht nur als „Konsumenten“ von Forschung betrachtet werden. Deshalb sollte hier stärker die Frage in den Vordergrund rücken, welche Produkte und Dienstleistungen entwickelt werden können, mit denen zukünftig deutsche Unternehmen erfolgreich auf dem internationalen Markt bestehen können („Security made by Germany“).
- Sicherheit wird zu einem immer bedeutsameren Wirtschaftsfaktor. Insbesondere durch die Tatsache, dass in Unternehmen Kommunikations- und Transaktionsprozesse zunehmend nur noch im Internet stattfinden, ist deshalb die Zertifizierung von sicherheitsrelevanten Systemen und Prozessen ein wichtiges Forschungsfeld mit zugleich hohem wirtschaftlichem Potential.
- Deutsche Unternehmen zeichnen sich bereits heute durch einen hohen technologischen Sicherheitsstandard aus. Jedoch fehlen bisher Schulungskonzepte zur Entwicklung einer „gelebten“ Sicherheit in den Unternehmen sowie zur Erhöhung des Risikobewusstseins bei den Mitarbeitern.
- Im Sinne einer sinnvollen Kosten-Nutzen-Abwägung ist es bei der Entwicklung und Integration innovativer Sicherheitslösungen gerade für KMU die Bezahlbarkeit von Sicherheit im Auge zu behalten und stärker zusätzliche, für die Unternehmen bestehende Mehrwertaspekte einzubeziehen.
- Gerade hinsichtlich der Sicherheit in Unternehmen besteht ein im Rahmen der zivilen Sicherheitsforschung zu beleuchtendes Spannungsfeld bezüglich der Ausrichtung von Sicherheitsmaßnahmen, die präventiv unter Routinebedingungen vorzuhalten sind und Maßnahmen, die in unerwarteten Krisenfällen unmittelbar eingeleitet werden müssen. Die sich daraus unter Umständen ergebenden veränderten Handlungsstrategien müssen deshalb bei der Entwicklung ganzheitlicher Konzepte stärker berücksichtigt werden.

Dr. Olav Teichert (VDI TZ)