

Kritische Infrastrukturen im Spannungsfeld zwischen lokaler und internationaler Aufgabe

Prof. Dr. B. M. Hämmerli, bmhaemmerli@hta.fhz.ch



Inhalt

- ❖ Einführung
- ❖ Situationsanalyse und das Bedürfnis nach CI(I)P
 - Nationale Dienstleistungen / Freier Markt / Sektoren
 - Economy of Scale / Dezentralisierung
 - Neue Bedrohungen
 - Schlussfolgerungen und Strategien
- ❖ Trend in betrieblicher Informationssicherheit
 - Geschäftsorientierte Sicherheit
 - Wirtschaftlichkeit der Sicherheit
 - Grenzen betrieblicher Sicherheit
- ❖ CIIP Ansätze in der Schweiz
- ❖ Trend in CI(I)P EU Forschung
- ❖ Weitere Trends zur Verbesserungen der Sicherheit
- ❖ Schlussfolgerungen und Diskussionen

Einführung

Definition eines kritischen Service (CIIP Handbook 2004, ETHZ)
Services, organizations and institutions,
which are
(absolutely) essential to the public community
such that
failure or disruption of which
will result in
long-lasting supply bottlenecks and/or other dramatic consequences
for substantial elements of the community are considered as critical

Definition Asymmetrische Bedrohung

Report: CIIP Handbuch 2004 zeigt Nationale Vorgehensweisen

Inhalt: Primär werden neue Herausforderungen und neue Applikationen
gezeigt: Trend in betrieblicher Sicherheit, Nationaler Sicherheit, EU Forschung in
Sicherheit

Situationsanalyse und Bedürfnisse in CI(I)P Übersicht

Jedes länger betriebene System tendiert optimiert zu werden. .
Wegen dem Gesetz "Economy of Scale" tendieren Systeme dazu,
grösser und zentraler zu werden:

- ❖ Vom Monopol zum freien Markt
- ❖ Economy of Scale
- ❖ Dezentralisierung und Zentralisierung
- ❖ Schlussfolgerungen

10th Symposium on Privacy and Security

Situationsanalyse und Bedürfnisse I Nationale Dienstleistungen: Vom Monopol zum freien Markt

Vom Monopol zum freien Markt

Für jede Nation

Security ?

Task Task Task
Task Task Task
Task Task Task

Freier Markt führte zu:

- Konkurrenz (Ziel: günstigste Dienstleistung)
- Vielen Dienstleistern mit betriebseigener Sicherheit
- Delegieren des Versorgungsauftrages
- Gesamtverantwortung über die Versorgungssicherheit hatte keine Verantwortung
- Zentralisierten Strukturen, (teilweise mit gemeinsamen Knoten und / oder Infrastrukturen)

CIP ist die Antwort zur Sicherung des alten „service public“ im (inter) & nationalen Bereich

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 5

10th Symposium on Privacy and Security

Situationsanalyse und Bedürfnisse II Economy of Scale / Decentralization I

Economy of Scale

Management Center

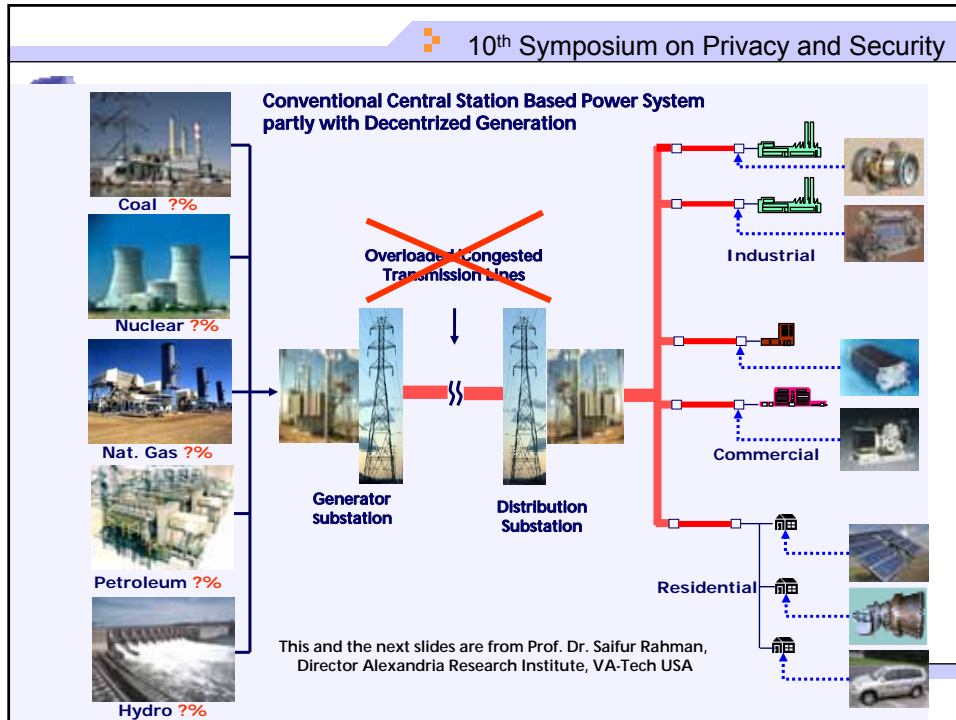
— Logische Kanäle für Management Informationen

Produktionskosten in regulären Situationen sind mit dem zentralen Ansatz oft tiefer .

Sicherheitsmassnahmen reduzieren die Verletzlichkeiten, aber der zentrale Wunde Punkt bleibt.

Dezentralisierung macht die Infrastruktur robuster.

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 6



10th Symposium on Privacy and Security

Situationsanalyse und Bedürfnisse IV
Economy of Scale / Decentralization III
Distributed Generation Technologies

Solar Cells

Wind Turbines

Gas Turbines

Reciprocating Engines

Zurich, 31. August 2005

Prof. Dr. Bernhard M. Hämmerli

Page 8

10th Symposium on Privacy and Security

Situationsanalyse und Bedürfnisse V Neue Bedrohung: Abhängigkeiten sind strukturiert!

Es sind nicht alle Abhängigkeiten zwischen den Systemen gleich wichtig. Grundsätzlich hat die Energie erste Priorität, gefolgt von der Kommunikation.

Transport / Post
 Rettungs- und Gesundheitswesen
 Entsorgungsdienste
 Regierung und Administration
 Gas / Öl Versorgung
 Wasser
 a. s. o.

InfoSurance
Stiftung
Schweiz

Applikationen

Finanzanwendungen

Operating System / Middleware

Kommunikation

Elektrizität

Physische Bedrohungen

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 9

10th Symposium on Privacy and Security

Situationsanalyse und Bedürfnisse VI Neue Bedrohungen: Analyse I

Neue
Bedrohungen
und
Verletzlichkeiten

März 11, 2004
Black out N. Y.
usw.

Die Gesellschaft muss damit leben !!!!!!!

- ❖ Das Leben mit dauernden Bedrohungen und Verletzlichkeiten ist ein Faktum
- ❖ Abhängigkeiten wachsen, weil der Komfort profitiert (GPS und Cell Phone Anwendungen in verschiedenen Geräten.)
- ❖ Ökonomische Aspekte und das Geschäft fördern vernetzte Lösungen und Anwendungen. Sicherheit in neuen Systemen wird oft vernachlässigt.
- ❖ Durch die Abhängigkeiten werden die Verletzlichkeiten noch grösser.

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 10

10th Symposium on Privacy and Security

Situationsanalyse und Bedürfnisse VII: Vernetzte CIP

View from EU Project ACIP

Analysis

- Knowledge Management
- Co-operation & Decision Support
- Vulnerability Analysis
- Risk Analysis / Safety Management

CIS Hierarchy

Methods

- Socio-economic Models
- Gaming
- Scenario Techniques
- System Dynamics
- Empirical Modeling etc.
- System Simulation
- Optim. Algorithms
- Human Behavior Mod.
- Technical Simulation
- Technical Experimentation etc.

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 11

10th Symposium on Privacy and Security

Situationsanalyse und Bedürfnisse VIII

Schlussfolgerungen und Strategien I

- **Architektur: künftiges Infrastrukturdesign** (Neue Bedrohungen, freier Markt)
 - Migration auf neue Architekturen (Dezentralisierung, Redundanzen, Separation der Information und Steuer- & Kontrollebene)
 - Härten der bestehenden Infrastruktur (z.B. gegen mehrfache simultane Attacken) mit Methoden wie Dezentralisierung und der Separation und Information und Steuer- & Kontrollebene
 - Granularität des CIP Modells (braucht noch lange Expertendiskussionen)
 - Dezentralisierung der Infrastrukturen (die Sektoren und innerhalb der Sektoren die Anbieter) und Erzeugen einer gegenseitigen Unabhängigkeit.
 - Vermeiden eines "Single Point of Failure" (verlangt intensive Untersuchungen (z.B. gemeinsamer Telekommunikationsleitungen))
 - Zentralisierung der Managementplattformen von dezentralisierten Systemen, um Wissen über den aktuellen Zustand für die bestmöglichen Entscheidungsgrundlagen zu erreichen. Mehrere Managementcenter sollen die Robustheit erhöhen.
 - Fehlende Modelle und fehlende Verträge mit internationalen Unternehmungen (Diese Unternehmungen sind profitorientiert, haben keine spezielle Loyalität zu einer Nation, Sicherheit ist ein begrenztes Thema)
→ Die Staaten sollten verhandeln und die Situationen klären - auch mit Risikobewertung.

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 12

Situationsanalyse und Bedürfnisse IX Schlussfolgerungen und Strategien II


- ❖ **“CIP Middleware“** fehlt (Vom Monopol zum freien Markt)
 - Top down: Der „Policy“ Ansatz hat Staaten zum nationalen Denken gebracht. (Netze sind weltweit)
 - Bottom up: Die Betriebe investieren sehr viel in in BCP, DRP und IT Sicherheit
 - Dazwischen ist die „CIP Middleware“, Information Sharing Centers (ISAC): Themen die spezifiziert werden müssen (Automatische gegenseitige Unterstützung, bilden von C(I)IP Gemeinschaften)


Der Aufwand für betriebliche und teilweise auch sektorielle Sicherheit ist heute beträchtlich.
Die Integration dieser komplexen Infrastruktur und ihrer Schnittstellen in einen nationalen oder übernationalen Plan ist eine der grössten C(I)IP Herausforderungen.

Situationsanalyse und Bedürfnisse X Schlussfolgerungen und Strategien III

- ❖ **Breitere Sicht (Von betrieblicher IT-Sicherheit zu CIP)**
 - CIP sollte alle Verlässlichkeitsaspekte umfassen **Verfügbarkeit, Vertraulichkeit, Integrität, Nachvollziehbarkeit**, (Verbindlichkeit, Authentizität) basiert auf einer Risikobewertung
- ❖ **Corporate Risk Manager (CRM) sind Personen, die in den CIP Prozess einbezogen sein sollen**
 - In den Unternehmungen sollte ein einziger Punkt für das Risikomanagement geben (Basel II): Corporate Risk Manager CRM.
 - CRM verwaltet alle Risiken (Länder, Finanzielle, Markt, ... und Infrastruktur). Die Infrastruktur umfasst: Heizung / Kühlung, Gebäudezutritt, unterbrechungsfreie Stromversorgung, Wasser (Reserven), IT-Sec (Firewall, IDS, Virenschutz, Logs), Kommunikationsdoppelzugriff, Managed Security Services a. s. o.
- ❖ **Das Teilen von Sicherheitsressourcen hat Tradition** (Polizei, Feuerwehr, Medizinische Versorgung, ...)! **Vertrauen (Trust and Confidence)** sind unverzichtbare Schlüsseleigenschaften und müssen deshalb kultiviert werden.
- ❖ **Neue Sicherheitskultur: „Das Leben mit permanenten Bedrohungen“ und „Betrieb mit Attacken“**
 - Monitoring und Reporting
 - Vertrauen und Bedrohung balancieren
 - Verstehen und reduzieren der Motivation von Terroristen

Neue Technologien bieten Werkzeuge für starke Widerstandskraft (Policy Enforcement, KPI Überwachung). Die grosse Herausforderung wird risikobezogene Integration und Anwendung dieser Werkzeuge sein.

 10th Symposium on Privacy and Security




Trend in betrieblicher Informationssicherheit I Übersicht

- ❖ Trend in betrieblicher Informationssicherheit
 - Geschäftsorientierte Sicherheit
 - Wirtschaftlichkeit der Sicherheit
 - Grenzen betrieblicher Sicherheit (inklusive Abhängigkeiten)

Zurich, 31. August 2005
Prof. Dr. Bernhard M. Hämmerli
Page 15

 10th Symposium on Privacy and Security



Trend in betrieblicher Informationssicherheit II Geschäftsorientierte Sicherheit

Schritte in IT-Security

- Glücklich, dass ein System läuft
- Optimierung der Verfügbarkeit
- IT-Security = Encryption (Technisches Problem)
- IT Security ist delegiert and den Security Officer
- IT Security ist Chef Sache
- IT Security soll prozessorientiert betrachtet werden
- IT Security hat seinen Preis. Deshalb soll die Sicherheit vom Sicherheitsbeauftragten vorgeschlagen und vom Business Line Manager abgesegnet werden: "Commander in Charge Model": Gewinn orientiert unter Beachtung der Risiken.

Betriebe sparen immer mehr an Sicherheitsaufwendungen. Die Bedürfnisse der Gesellschaft als Ganzes werden nur betrachtet, wenn **spezifische Gesetze da sind. (Governance Issue).**

Zurich, 31. August 2005
Prof. Dr. Bernhard M. Hämmerli
Page 16

Trend in betrieblicher Informationssicherheit III Security und Wirtschaftlichkeit

Zur Wirtschaftlichkeit:

- ❖ 20 % des IT Budgets wird für Sicherheit verwendet. Das entspricht dem wirtschaftlichen Optimum (Ross Anderson, Cambridge)
- ❖ „Incentive Model“: Fördern guter Sicherheitspraxis in grossen Firmen mit Belohnungen. Führt zu einer Zunahme des Sicherheitswesens, deshalb haben grosse Firmen mehr Sicherheit als der Durchschnitt. Abhilfe: geschäftsorientierte Sicherheit. In KMU ist Sicherheit ein Kostenfaktor => weniger Security als der Durchschnitt
- ❖ Erforschen von Verletzlichkeiten: Von *“discover for fun”* durch *“discover for recognition”* bis hin zu *“discover to use and get advantage”*.
- ❖ PC Geschichte: Der Markteintritt gelingt nur mit einer einfachen Bedienbarkeit. Es gibt keine Option direkt mit sehr komplexen und sicheren Systemen den Markt zu erobern. Security muss nachgestellt werden.

Trend in betrieblicher Informationssicherheit IV Grenzen der betrieblichen Sicherheit (Abhängigkeit)

Betriebliche Sicherheit umfasst:

- Business Continuity Planning
- Grundschutz der IT Infrastrukturen
- Schutz vor finanziellen Verlusten (nicht für jedes Szenario)
- Schutz des Kundenvertrauens
- Verhindern von Haftungsfällen

Betriebliche Sicherheit umfasst nicht:

- Information Sharing (Austausch von Angriffen und Verletzlichkeiten)
- Gegenseitige Unterstützung im Sektor (CIP Vorgehen)
- Widerstandsfähige Dienste für die (CIP Vorgehen)
- Klare Bewertungen der Abhängigkeiten und der Gegenmassnahmen

10th Symposium on Privacy and Security

CIIP Ansätze in der Schweiz I Übersicht

Geschichte aus Sicht der angewandten Forschung

Zuständigkeit Strategisch: Dr. Ruedi Rytz, ISB:
Operativ siehe Website

- ❖ 1997 Strategische Führungsübung SFU
- ❖ 1999 Gründung der Stiftung InfoSurance (bis 2005)
- ❖ 2001 Informo
- ❖ 2002 Informorena
- ❖ 2003 Kreditbeschluss (BR) für MELANI

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 19

10th Symposium on Privacy and Security

CIIP Ansätze in der Schweiz II

Alte Folie (2000):
Erster Vorschlag für MELANI
Diskussionsgruppe, erstellt von B. Hämmerli

Infosurance
(Überwachung, Koordination, Rechtliche Abklärungen)

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 20

CIIP Ansätze in der Schweiz III

Aus: <http://www.melani.admin.ch/>

- ❖ **Computer- und Internetsicherheit**
- ❖ Schützen Sie Ihre wertvollen Daten! MELANI bietet Ihnen dazu folgende Unterstützung:
- ❖ **Informationen** zum Schutz Ihres Computers und der Daten
- ❖ **Meldungen** zu aktuellen Gefahren und Risiken
- ❖ **Meldemöglichkeit** von vorgefallenen Attacken
- ❖ **MELANI-Net** richtet sich an die Betreiber von nationalen, kritischen Infrastrukturen und ist nur mit Passwort zugänglich.



CIIP Ansätze in der Schweiz IV 4-Säulen Modell für Information Assurance

- 1) **Preventive** measures: *InfoSurance*
- 2) **Early recognition**: Reporting and Analysis Centre for Information Assurance **MELANI**
- 3) **Minimisation** of the **effects** of disruptions: Special Task Force on Information Assurance **SONIA**
- 4) **Identification** and **correction** of the **technical cause**: **MELANI** and **Partners**

Definition in CH: Information Assurance ≈ CIIP

10th Symposium on Privacy and Security

CIIP Ansätze in der Schweiz V
InfoSurance Beispiel: Generische Risiken in CI(IP)

„Round Table“
Generische Risiken,
InfoSurance, Frühjahr
Spring 2003

2 Typen von Risiken:
-Kernrisiken
-Applikationsrisiken

Idee: Teile Risiken
mit, identifiziert in
anderen Sektoren,
zum Beschleunigen
der Risikoanalyse

Schnittstellen und
Abhängigkeiten,
Klären der
Risikozuständig-
keiten

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 23

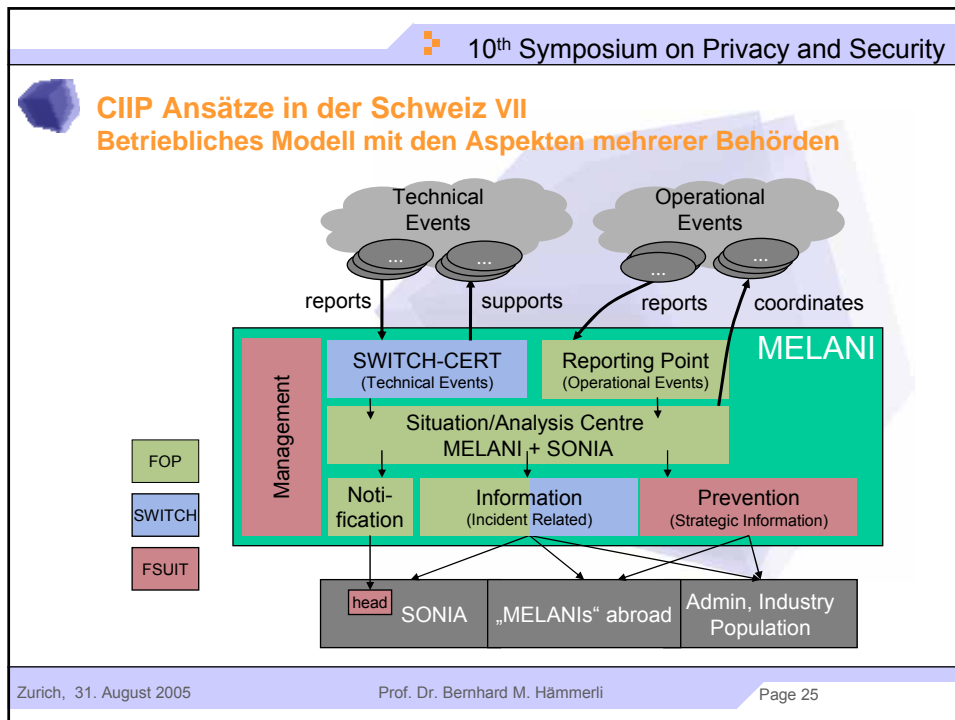
10th Symposium on Privacy and Security

CIIP Ansätze in der Schweiz VI
Ziele und Aufgaben der MELANI

Reporting and Analysis Centre for Information Assurance
(MELANI = **M**elde- und **A**nalysestelle Informationssicherung):

- **Centre of expertise**
- Draw up **strategies**
- **Early recognition** of threats and dangers
- **Incident response coordination**
- **Situation centre** (Federal Authorities, SONIA, ...)
- **Alerts the Special Task Force on Information Assurance SONIA**, if required

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 24



10th Symposium on Privacy and Security

CIIP Ansätze in der Schweiz VIII Constituencies ^{1/2}

Constituency	Closed		Open
	SWITCH-CERT	MELANI	MELANI
Members	Selected Operators of Critical Infrastructures		SME's Citizen
Number (#1 → #2)	30 → 60		Open
Trust	Strong Trust, Close Relationship		Non personal (Weak Trust)
Build-up of Trust	InfoSurance (Round Tables) Federal Office for National Economic Supply (Members of Coordination Centers → SONIA)		Media, WWW SME's: Promoted by Organizations (e.g. InfoSurance)

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 26

10th Symposium on Privacy and Security

CIIP Ansätze in der Schweiz IX
Constituencies ^{2/2}

Constituency	Closed		Open
	SWITCH-CERT	MELANI	MELANI
Contact	cert@melani. admin.ch www.melani. admin.ch 0844 800 511	incident@melani. admin.ch www.melani. admin.ch 0844 800 512	www.melani. admin.ch

Note: URLs and e-mail addresses are for illustration purposes only and are subject to changes.

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 27

10th Symposium on Privacy and Security

CIIP Ansätze in der Schweiz X
Schlussfolgerungen und Schlüsselthemen

Weshalb hatte MELANI Erfolg?

- ❖ Expertendiskussionen 1997 / 2001
- ❖ Gründung InfoSurance (Public – Private – Partnership)
 - Schritt 1: Visionäre Phase
 - Viele Personen, umfassende Repräsentation
 - Starke Awareness und starkes Marketing
 - Guter Meinungsbildungsprozess
 - Schritt 2: Projektphase
 - Klare Führung / unité de doctrine
 - koordiniertes und zielorientiertes Arbeiten
- ❖ Für „Information Sharing“ ist Vertrauen **d i e** Voraussetzung
- ❖ Für den Anfang ist der Wille zur Zusammenarbeit wichtiger als Modelle und Prozesse

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 28

10th Symposium on Privacy and Security

Trends in CI(I)P der EU Forschung I
 CIIP Konferenz Frankfurt (Deutschland) GE September 2003

Building and maintaining an EU CI(I)P community (National, Industry and Research), based on the requirements of the task helps nation to foster its CIP:

Generate an “European CIP Platform” as follows:

- European CIP Workshop once per Year
(GI, cooperation with SI + ÖCG; CEPIS (partner of ACM and IEEE), National Administration a. s. o.)
- European CIP Newsletter (4-6 times per year)
(see: US CIP Report, from GMU Fairfax)
- Education (Fundamental 1day experts 5day)
- European CIP Network of Excellence
- European CIP Website
- Running at least one common EU Research Project

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 29

10th Symposium on Privacy and Security

Trends in CI(I)P Research EU II
 (Slide form Andrea Servida, deputy head of ICT Trust and Security)

International Co-operation		
• OECD, G8, Council of Europe, UN, ITU, ...		
Economic, business and social aspects of security in Information Society	Cyber-crime, Internal security	External security / defence
<ul style="list-style-type: none"> • Electronic Signature • Data protection in elect. com. • Network & information security • Culture of security • ENISA • digital right management, biometrics, smart card, IPv6, open source software • critical infrastructure protection 	<ul style="list-style-type: none"> • Framework Decision on attacks against information systems • Lawful interception • G8 CIP • e-identification/e-authentication • biometrics in visas and residence permit 	<ul style="list-style-type: none"> • Pilot action with DG RTD • Dual use technology research • Crisis management
Preparatory Action Security Research		
Research and Technology		
Information and Communication Technologies		
• network security, dependability, cryptography, biometrics, identity management, watermarking, ...		

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 30

10th Symposium on Privacy and Security

Trends in CI(I)P Research EU III
(Slide form Andrea Servida, deputy head of ICT Trust and Security)

- Securing the **Individual**
 - observability vs. confidentiality
 - privacy
 - mobility
 - biometrics
- Securing **Communities** - B2E, B2B, B2C, as well as agents, devices,
 - legacy digital
 - mediation of security policies
 - timed security and mobility
- Securing **Critical Infrastructures**
 - dependability
 - interdependencies

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 31

10th Symposium on Privacy and Security

Trends in CI(I)P Research EU IV
(Slide form Andrea Servida, deputy head of ICT Trust and Security)

To prepare a European Security Research Programme (ESRP) for 2007

- For Internal Security
- To support external EU peacekeeping operations
- Multi-purpose, common technology base for civil and defence applications and systems
- Complements civil community programmes and MS programmes

Technical Priorities

- Improve situation awareness
- Security and Protection of networked systems, infrastructures, utilities
- Protect against terrorism (including bio-terrorism)
- Enhance crisis management
- Achieve interoperability/integrated systems for information & communication

Research complementary to existing activities

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 32

10th Symposium on Privacy and Security

Trends in CI(I)P Research EU V
(Slide form Andrea Servida, deputy head of ICT Trust and Security)

- ❖ **Membership Group**
 - Chaired by Commissioners Busquin and Liikanen
 - Political figures, MEPs, Industry leaders, Heads of Research Institutes, Heads of various organisations
- ❖ **Security: a concern for all Member States**
- ❖ **Increase funding for security research in EU**
 - Order of magnitude discussed: **> 1 Bi euro /yr**
- ❖ **Improve coherence of approach**
 - Better coordination EC and all MS's
 - Systematic analysis of capability needs
 - Full exploitation of possible synergies
 - Specific legal conditions and funding instruments
 - Effective institutional arrangements
- ❖ **Targeted International Cooperation**

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 33


10th Symposium on Privacy and Security


Weitere Trends zur Verbesserung der Sicherheit I
Trusted Computing Group (TCG) Initiative

Von unsicherem PC zum komplette sicheren PC (Intel's TCM)

- ❖ Idee: Zum Schutz des PC Markts (Soft- and Hardware)
 - Jede Kommunikation ist automatisch verschlüsselt
 - Jede Kommunikation ist automatisch stark authentifiziert
 - Jedes Gerät hat automatisch ein internes Backup
 - Jedes Gerät hat eine Zugriffskontrolle (nur authentifizierte und signierte Applikationen können gestartet werden)
 - Informationsfreiheit wird stark eingeschränkt dadurch
 - Die Verbindlichkeit und die Nachvollziehbarkeit solcher Systeme sind garantiert.
- ❖ Relevante Fragen:
 - Wer hat die Kontrolle über die Wurzelschlüssel? (Informationsdominanz)
 - Werden die Anwender den Verlust an Informationsfreiheit akzeptieren?


Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 34


 10th Symposium on Privacy and Security

 **Schlussfolgerungen I**

- ❖ Situationsanalyse und Bedürfnisse in C(I)IP
 - Nationen und Betriebe brauchen Politiken und Gesetze zum Schutz der verletzlichen Infrastruktur.
 - C(I)IP ist ein öffentliches Anliegen und muss deshalb vom Staat angegangen werden. Jedoch kann die Aufgabe nur mit der Hilfe der Privatwirtschaft gelöst werden.
 - Zentralisierte Managementplattformen für C(II)P, sollen die Übersicht von kleinen vermaschten und autarken Infrastrukturzellen geben.
 - Finanzierungsmodelle müssen weiterentwickelt werden.
- ❖ Trend in betrieblicher Informationssicherheit
 - Firmen bauen die Sicherheit, welche für das Geschäft gebraucht wird.
 - Nationale Bedürfnisse in Sektoren brauchen Politiken und Weisungen (vergleiche SOX)
 - Firmen sollten sich auf die Einbindung in Sektoren vorbereiten und sich überlegen, welche Sicherheitsinformationen ausgetauscht werden sollen (Erwartung fürs geben und nehmen)

Zurich, 31. August 2005
Prof. Dr. Bernhard M. Hämmerli
Page 35

 10th Symposium on Privacy and Security

 **Schlussfolgerungen II**

- ❖ Eigenheiten von C(I)IP
 - Die Firmen müssen für ihre betriebliche Infrastruktursicherheit sorgen; Versorgungssicherheit ist eine staatliche Aufgabe.
 - "Robustness of critical services" is a transnational security policy issue and can only be researched with unconventional academic research and methodologies" Zitat Jan Metzger, ETHZ
- ❖ Trend in C(I)IP EU Forschung
 - Echte Annahme der Sicherheitsaufgabe (inklusive Budget)
- ❖ Sicherheit muss ein Gegengewicht haben im Privatheitsschutz!
 Es wäre gut, jetzt mit der Implementation der Infrastruktursicherheit als Antwort auf die neuen Herausforderungen zu beginnen. Die Diskussionen und der Aufbau von Sicherheitssystemen werden mehrere Jahre brauchen.

Zurich, 31. August 2005
Prof. Dr. Bernhard M. Hämmerli
Page 36

10th Symposium on Privacy and Security

Fragen

Zurich, 31. August 2005 Prof. Dr. Bernhard M. Hämmerli Page 37