Federal Office
for Information Security

BSI

National response plans: IT-Crisis Response in Germany

André Vorbach, CERT-Bund

Federal Office for Information Security

Bundesamt für Sicherheit in der Informationstechnik

4th ENISA Workshop, Athens

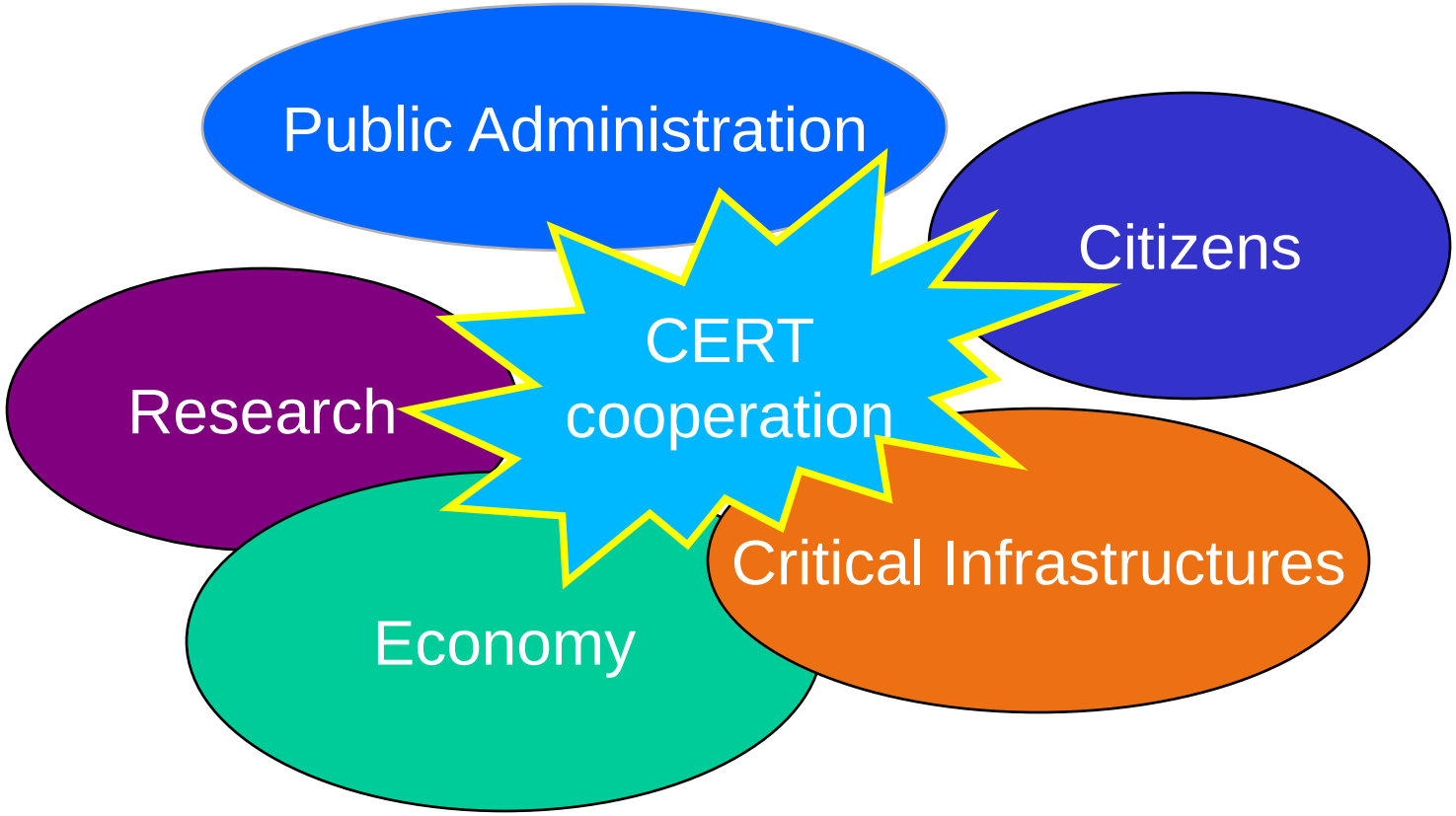
29.05.2008

Agenda

- CERT cooperation on a national level
- National Plan for Information Infrastructure Protection (NPSI)
  - Implementation Plans
    for the Federal Administration and Critical Infrastructures
- CERT-Bund / National Situation Centre / Crisis Response Centre
- Cooperation for critical infrastructures
- CERT-Alliance - „CERT-Verbund“
- Citizen‘s CERT - „Bürger-CERT“

National CERT Cooperation Levels

- *Who is involved in the national CERT cooperation?*



National Plan for Information Infrastructure Protection (NPSI)

- Comprehensive political “umbrella strategy” for IT security in Germany
- Coordinated across departments,
  adopted by federal government on 13.07.2005
- Target group: the public administration, critical infrastructures, private businesses, the general public
- Three "areas":
  - Prevention
  - **Preparedness**
  - Sustainability
- 15 objectives

National Plan – Three Strategic Aims

Protecting information infrastructures **adequately**

Responding effectively to IT security incidents

Enhancing German competence in IT security –
setting international standards

NPSI - Strategic Aim: Preparedness

Effective action in the event of IT security incidents

Time is essential when responding to disruptions of information infrastructures. Primary tasks include:

- **collecting** and **analyzing** information by **identifying, registering** and **evaluating incidents**,
- **informing**, **warning** and **alerting** of those potentially affected, and
- taking **measures** to contain the damage while **responding to IT security incidents**.

Implementation Plans

National Plan
for Information Infrastructure Protection (NPSI)

2005

National Plan
Implementation Plan
Federal Administration

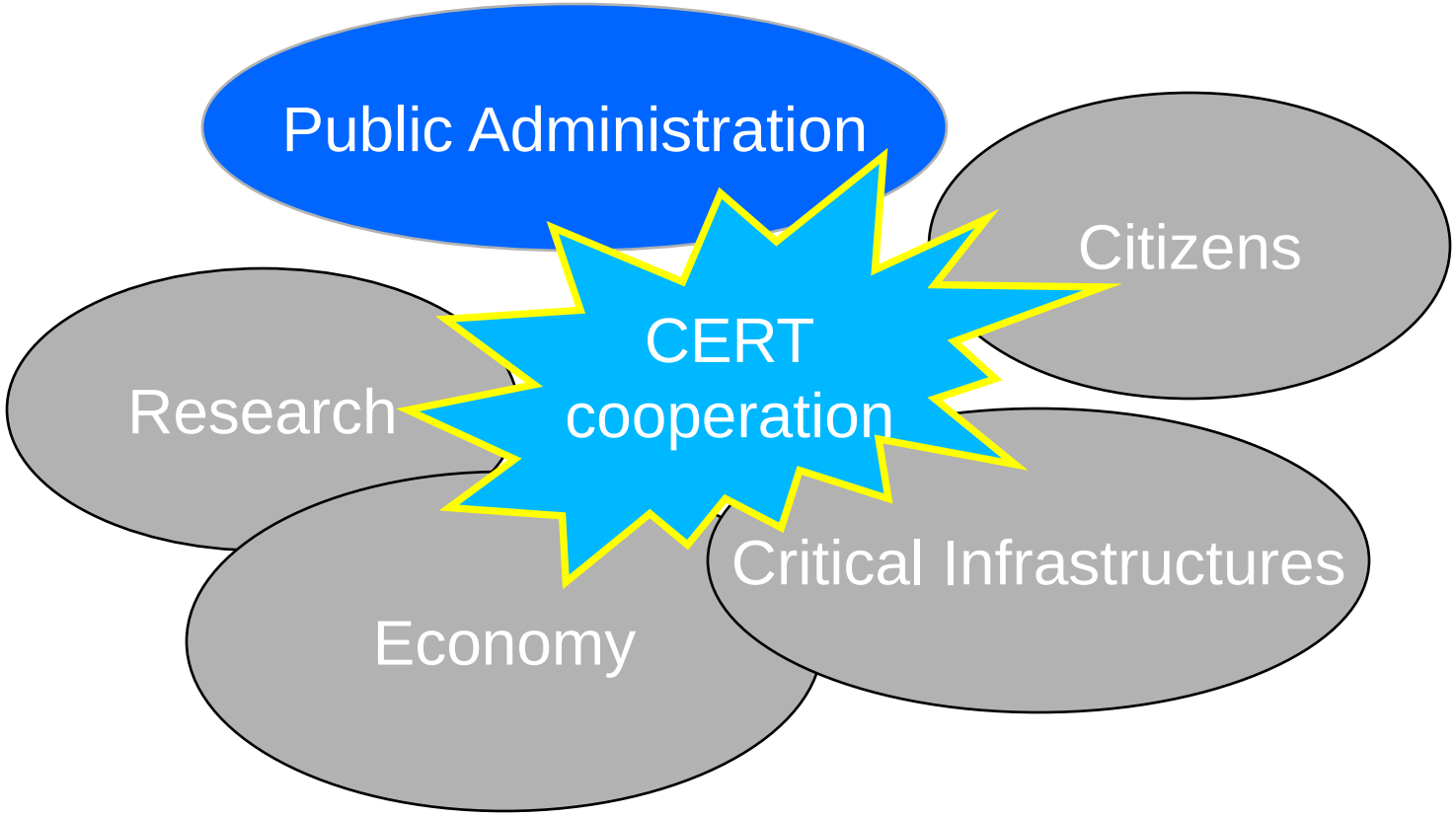
- Developed by the Ministry of the Interior for all departments
- **Obligatory** for the federal administration
- Elaboration of measures and amicable IT-security standards for the administration
  - Crisis response
- ***Classified***

National Plan
Implementation Plan
Critical Infrastructures (CIP)

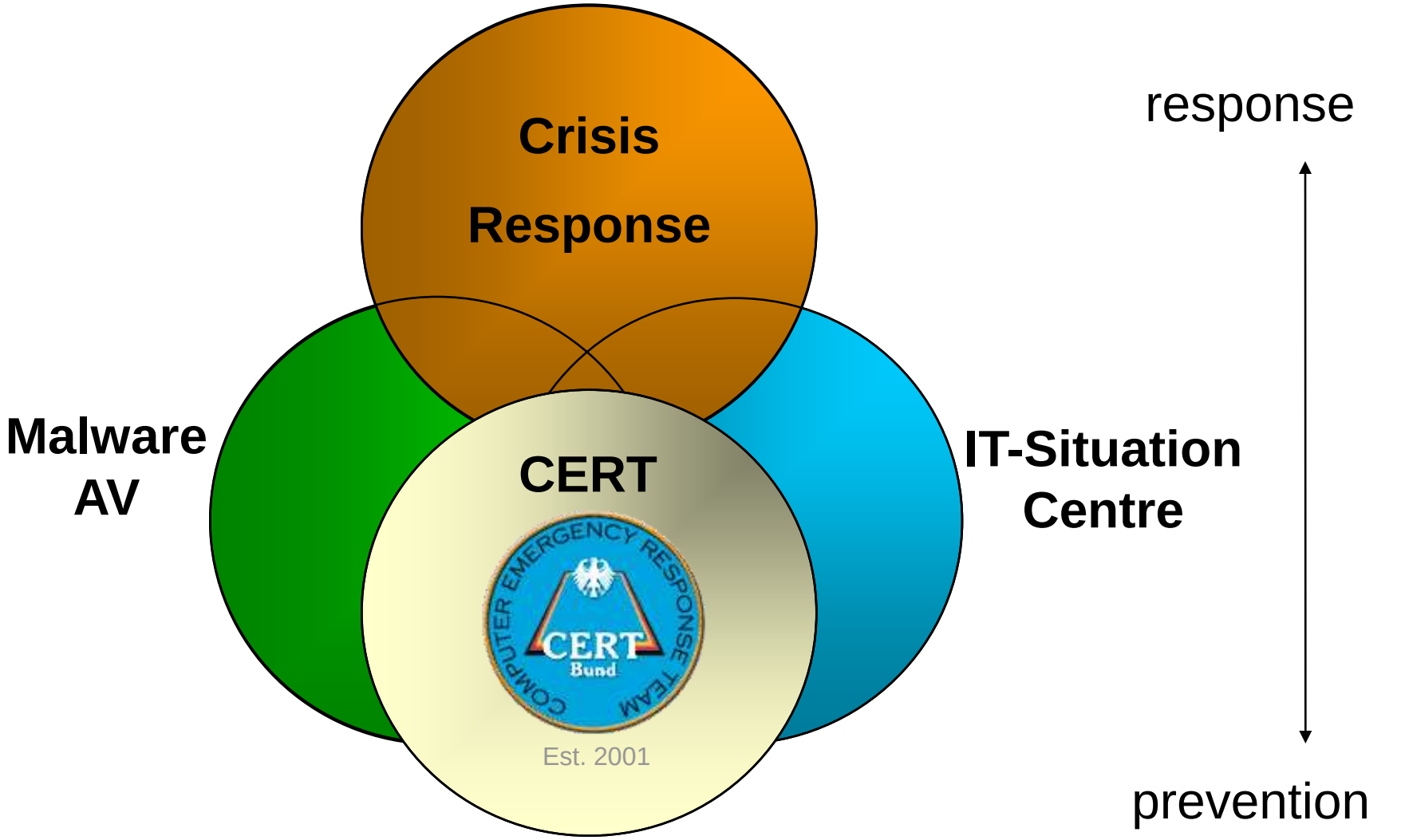
2007

- Developed by the operators of critical infrastructures
- **Voluntary** commitment
- Agreement on equally high IT-security basic level in critical infrastructures
- ***Publicly available***

Public Administration



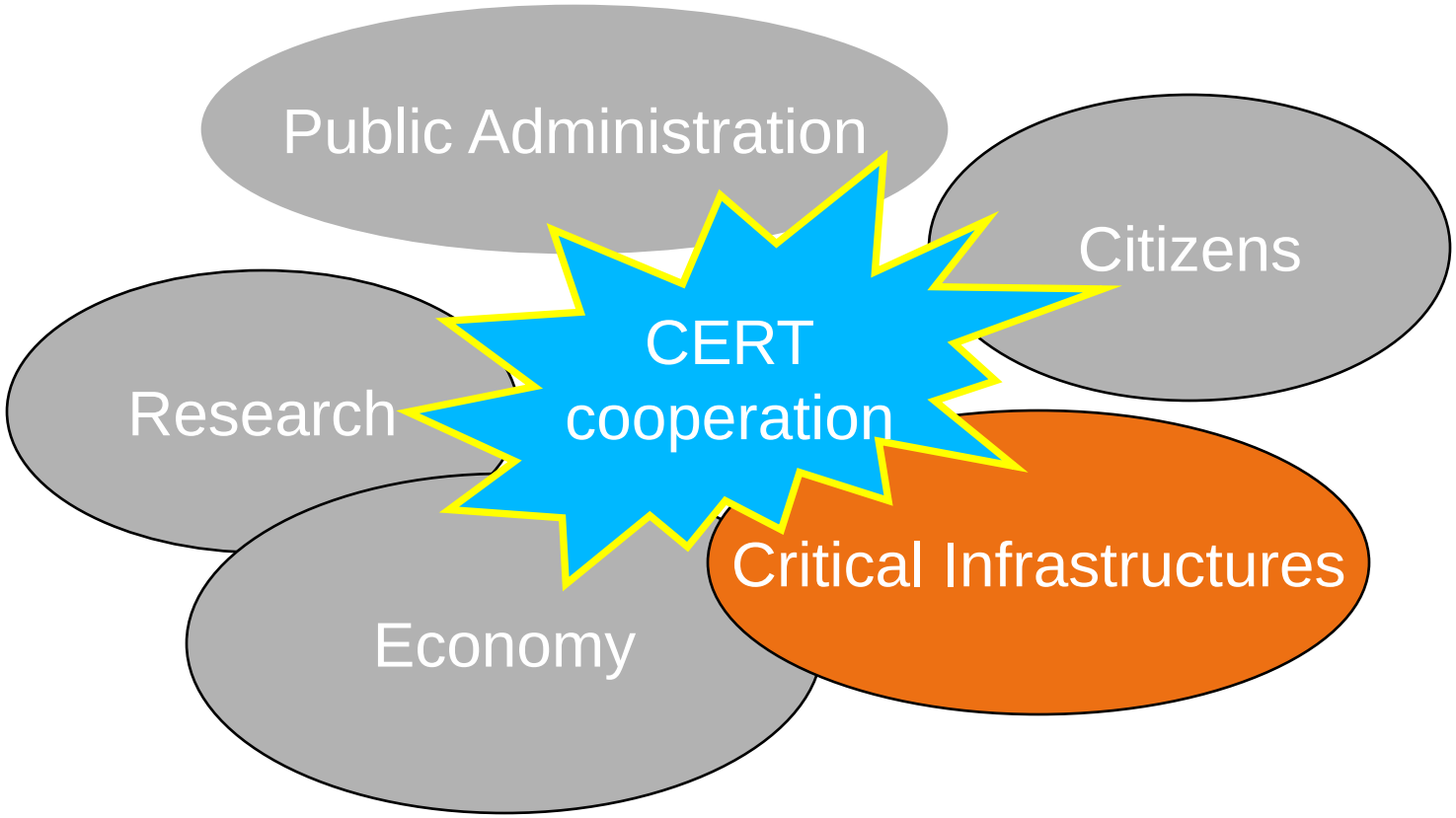
BSI Unit 121
CERT-Bund, IT-Situation Centre



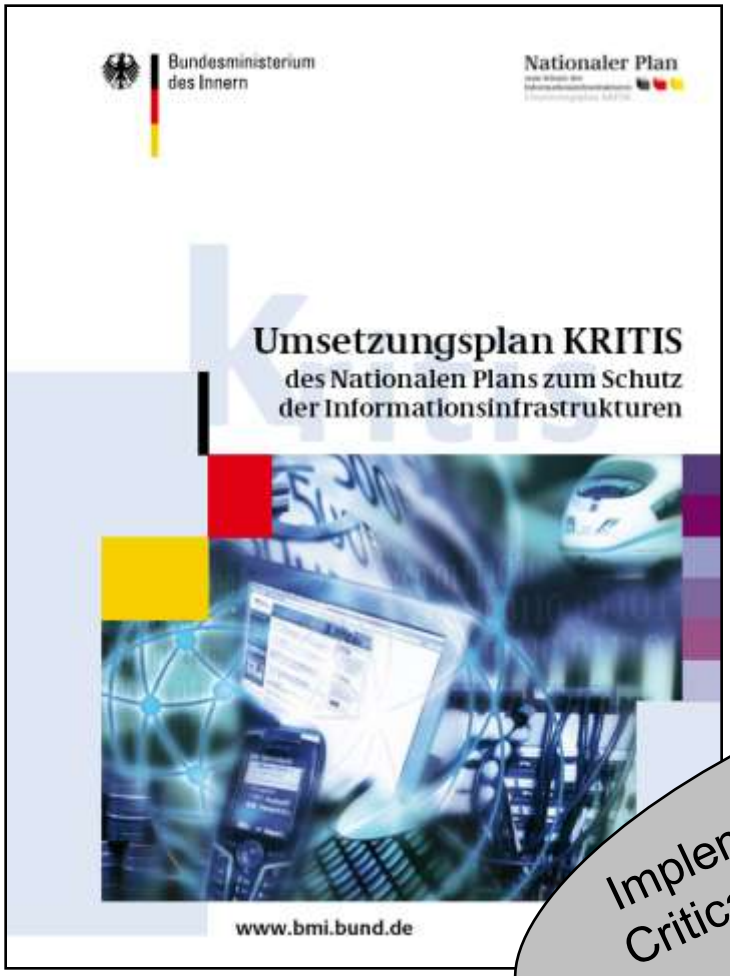
The national CERT: CERT-Bund

- Emerged from the BSI CERT as **governmental CERT** for the federal administration
- Providing central **24/7 PoC**
- Running an ***IT-Situation Centre*** for monitoring public sources and technical sensors
- **Analyzing** incoming incident reports and other information about **vulnerabilities**
- Supporting the **investigation of incidents** and the **recovery process**
- Coordinating **incident handling** & **malware reports**
- Publish **advisories** or information on **counter measures** and/or **workarounds** by running a ***Warning & Information Service***
- Running a telephone based **alerting service** for the federal administration
- Providing the **PoC** for **national** and **international cooperation**
- Running the ***National IT-Crisis Response Centre***

Critical Infrastructures



Critical Infrastructure Protection (CIP)



Implementation Plan
Critical Infrastructures
2007

Critical Infrastructures

- Definition: *Critical infrastructures are organisations and facilities that are of **vital importance** for public welfare and whose failure or disruption could result in **long-lasting supply bottlenecks** or **substantial disturbances** of the public order and/or could have other **dramatic consequences**.*

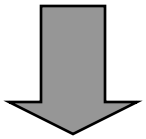
- Transport and traffic
- Energy
- Hazardous materials
- Information technology and telecommunications
- Finance, funds and insurance
- Supply services
- Authorities, administration and justice
- Others

Implementation Plan CIP: Aims

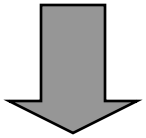
- **Implementation plan for critical infrastructures** as part of the National Plan for Information Infrastructure Protection
- Addressed to critical infrastructure **enterprises** and **organizations**
- Assumption of **joint responsibility for IT security** in critical infrastructures
- Established in **cooperation** with a **large number** of critical infrastructure operators, including the public administration
- Offers **concrete measures** for the operators of critical infrastructures
- Aims on an **equally high IT-security basic level** in the critical infrastructures
- Agreement on **recommendations** of how to reach this IT-security basic level
- Cooperation **before**, **during** and **after** IT-crises of national significance
- Offers **guidelines** and **orientation** for all **other enterprises**

Implementation Plan CIP:
Current situation

Growing interconnection between enterprises and greater dependency



In-house **security measures** are good, but by themselves are **no longer sufficient**



also needed:

sector-wide, inter-sectoral

and cross-border measures

Implementation Plan CIP: Communication

- Aims:
  - **Early warning**, **early detection** of IT crisis situations
  - More **intensive cooperation**, especially between sectors

- How to achieve them:
  - **Voluntary sharing** of information about IT security incidents
  - Establishing **single points of contact** (SPOC) for each sector, to coordinate the flow of information to and from the **IT Situation Centre**
  - **IT Situation Centre** at the BSI as **central clearing house** for gathering, evaluating and channelling information
  - **Joint analysis** of past IT crises: - “Lessons learned”

Implementation Plan CIP:
Working Groups

- **WG 1: Emergency and Crisis Exercises**
  - To draft and implement the necessary **framework conditions** for planning, staging and evaluating emergency and **crisis exercises**
  - To develop **inter-sectoral crisis scenarios** and carry out drills on a regular basis

- **WG 2: Crisis Response and Management**
  - To improve **coordination of crisis response** and the development of **crisis response planning** within and between sectors
  - To establish **crisis response procedures**

Implementation Plan CIP:
Working Groups

- **WG 3: Maintenance of Critical Infrastructure Services**
  - To identify **critical processes**
  - To identify the need for further **protection strategies** and measures

- **WG 4: National and International Cooperation**
  - To **strengthen coordination** between those taking part in the CIP Implementation Plan
  - To **share information** on **international CIP** activities by individual participants
  - To coordinate **strategic goals**

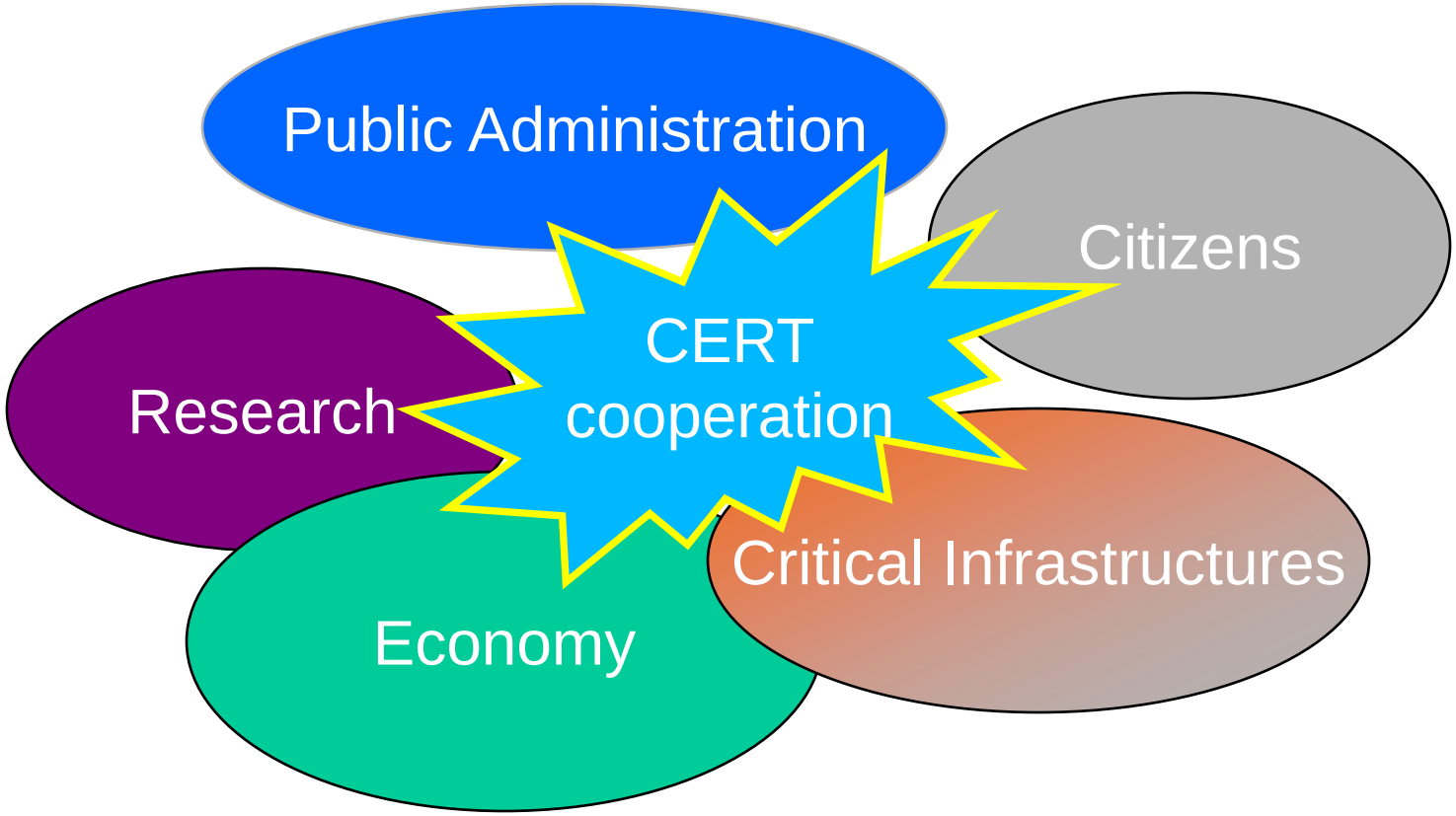
Implementation Plan CIP:
Next Steps & Summary

- **Include critical infrastructure enterprises** that have **not yet participated** in the CIP Implementation Plan
- Information and **awareness-raising** effort will extend to areas **beyond the field of critical infrastructure**
- **Cooperation** with academic and the private sector on national and EU projects

- The necessary **strategies** have been **developed**, now they need to be **put into practice**
- In particular, it is necessary to **build trust**!

- Working groups 1,2 and 4 started:
  - conceptual **framework for exercises**
  - conceptual **framework for IT-crisis response**
  - expected in the end of 2008
  - first **tabletop exercises** were performed

CERT-Alliance

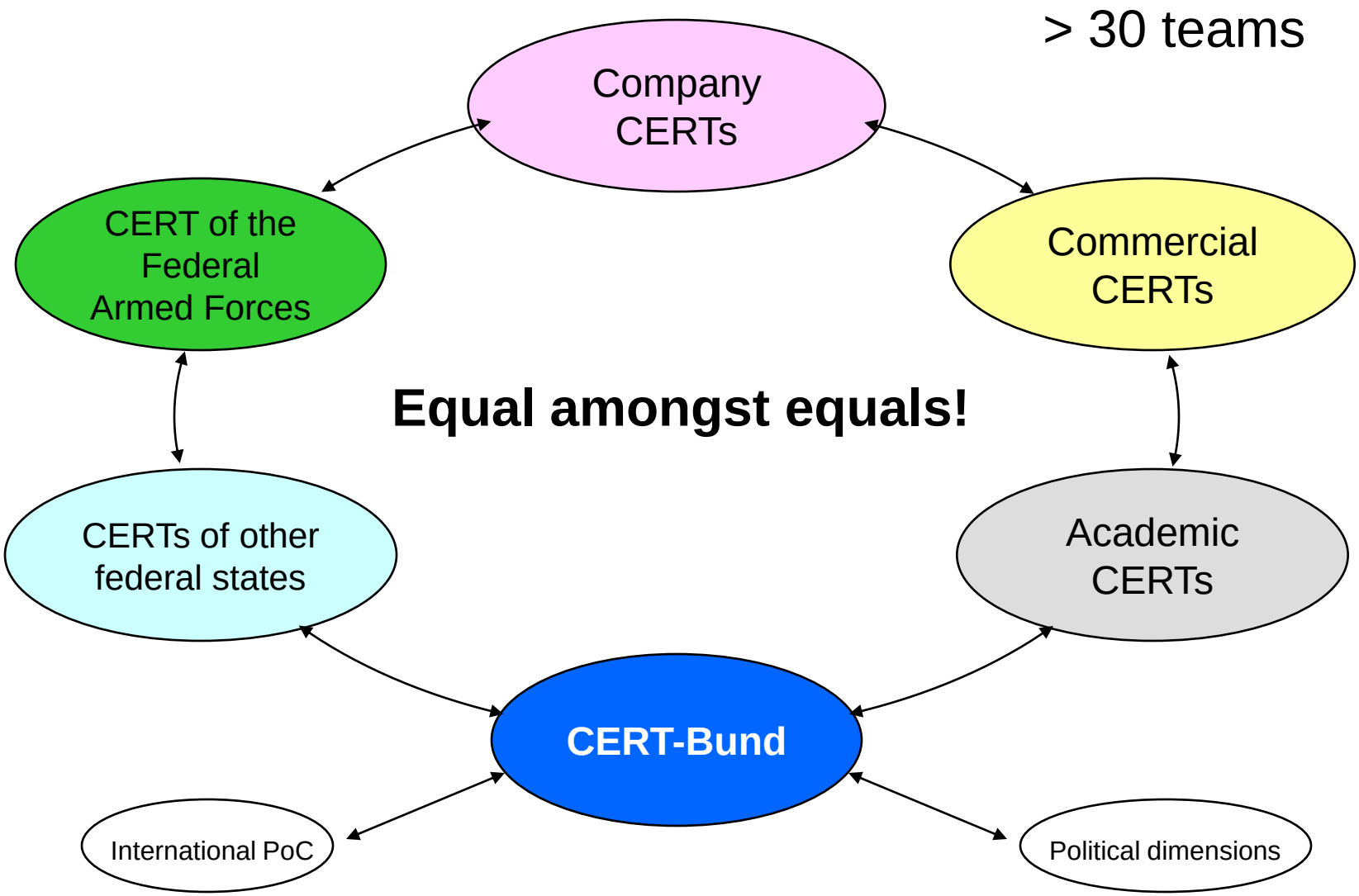


CERTs in Germany

CERT-Alliance „CERT-Verbund“

- CERT Working Group („CERT-Arbeitsgruppe“)
  - About 40 german CERTs organised in an **inofficial working group**
  - regular meetings **2 per year**
- CERT Alliance („CERT-Verbund“)
  - About 30 very **closely cooperating CERTs**, based on signed “Code of Conduct“ & NDA
  - http://www.cert-verbund.de
- **Most** of CERT Working Group **members joined** the CERT Alliance

CERT-Alliance „CERT-Verbund“



CERT-Alliance „CERT-Verbund“

Deutscher CERT-Verbund

(CERT-Verbund - Homepage) (Code of Conduct) (Projekte) (Impressum)

CERT-Verbund - Homepage

Wer wir sind:

Der CERT-Verbund ist eine Allianz deutscher Sicherheits- und Computer-Notfallteams.

Unsere Mitglieder sind u. a.:

- Bayern-CERT, Landesamt für Statistik und Datenverarbeitung
- BFK Consulting GmbH
- CERT Baden-Württemberg, Innenministerium Baden-Württemberg
- CERT-Bund, BSI
- CERT-NRW, Landesamt für Datenverarbeitung und Statistik NRW
- CERT-VW, Volkswagen AG
- CERTBw, Bundeswehr
- CERTCOM AG
- ComCERT, Commerzbank AG
- DFN-CERT Services GmbH
- GNSec
- IBM BCRS
- Mcert Deutsche Gesellschaft für IT-Sicherheit mbH
- PRESECURE Consulting GmbH
- RUS-CERT, Universität Stuttgart
- S-CERT, SIZ Informatikzentrum der Sparkassenorganisation GmbH
- secunet Security Networks AG
- Siemens-CERT, SIEMENS AG
- Telekom-CERT, DTAG

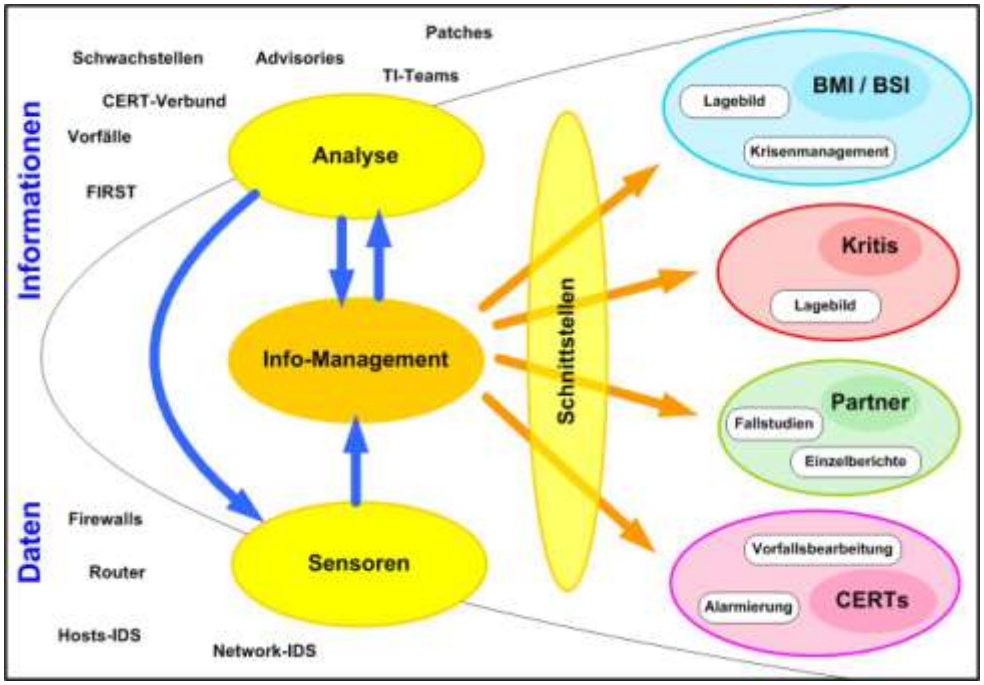
founder members in 2002

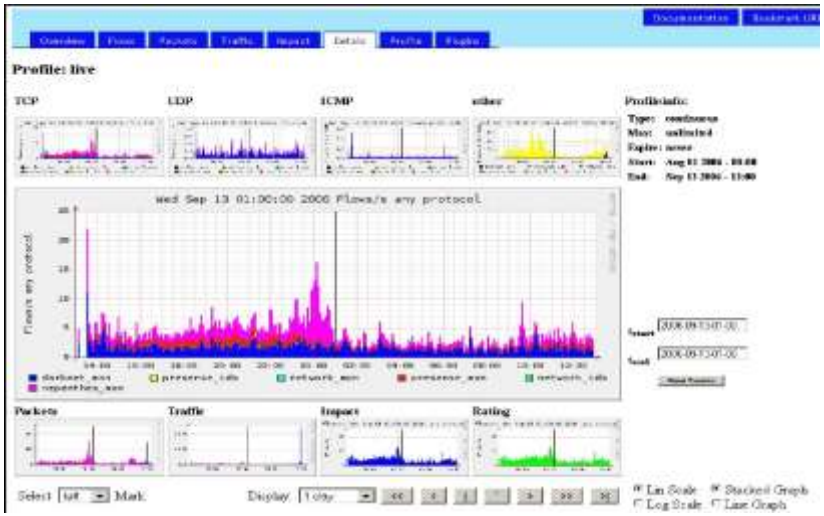
CERT-Alliance „CERT-Verbund“

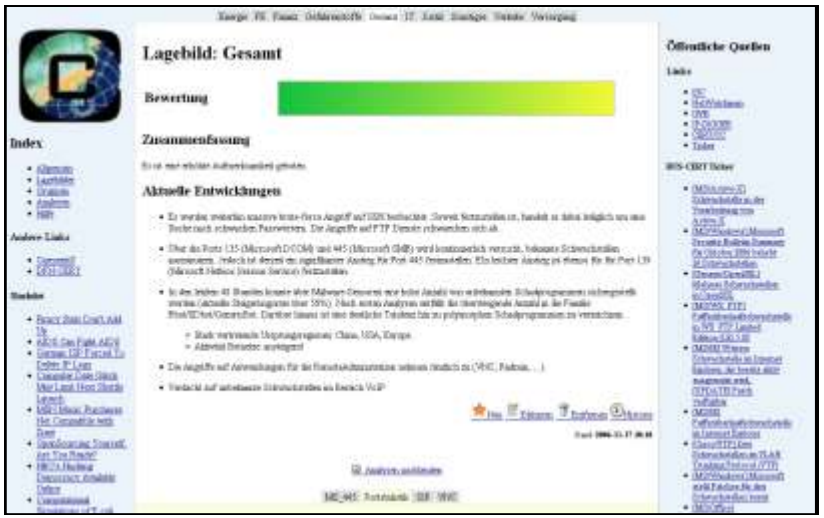
- Strategic cooperation among CERTs
- Cooperation in the case of a national IT-crisis
- Technical exchange and support
- Common projects
  - Incident Handling System (SIRIOS)
  - National Early Warning Capability (CarmentiS)
  - German Advisory Format (DAF)

- Coverage of the target groups:
  - Administration, some critical infrastructures, economy, research
  - Selective coverage, some CERTs with very special target group
  - Broad - but not pervasive - coverage

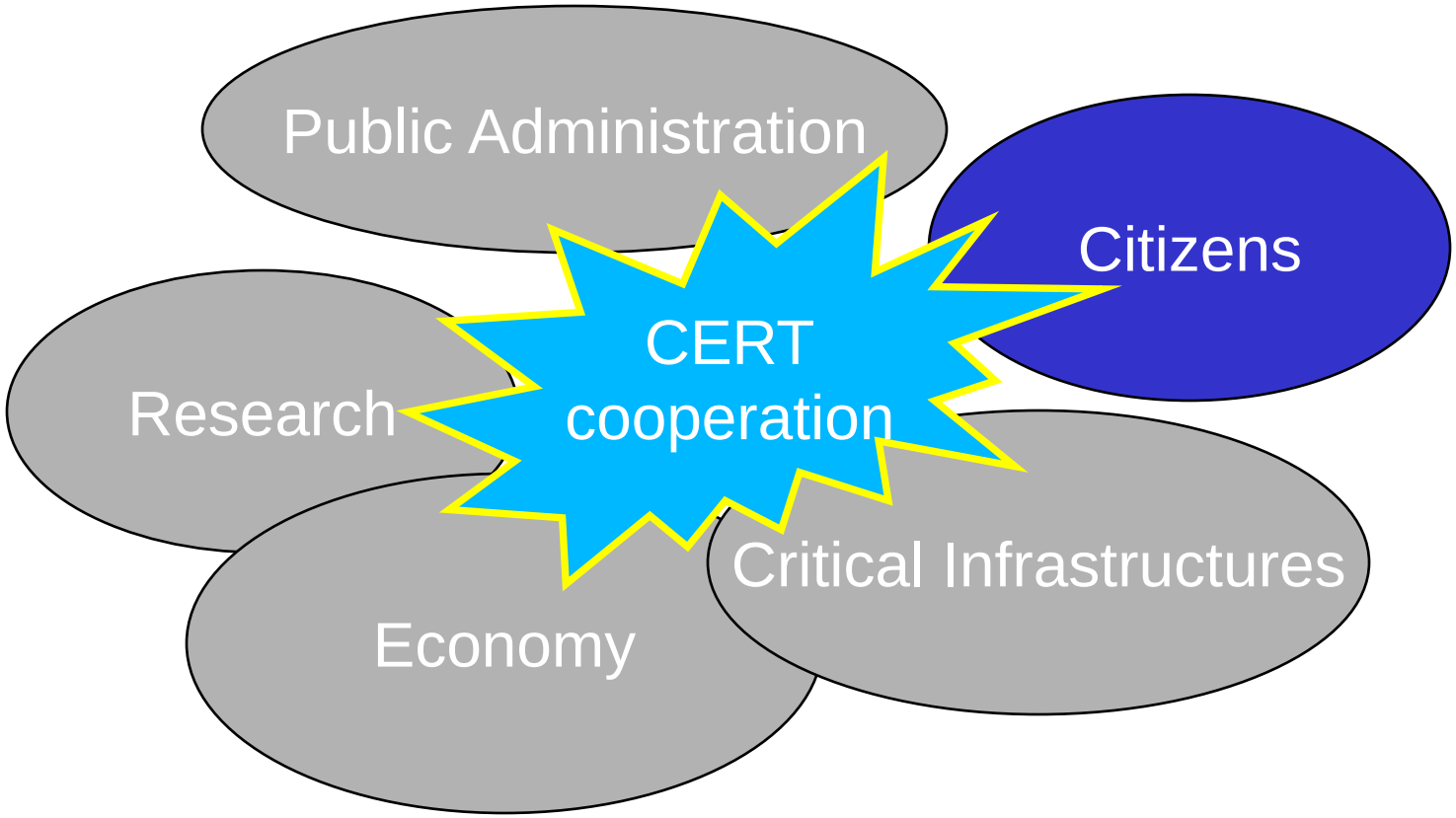
CarmentiS


Patches
Schwachstellen
Advisories
TI-Teams
CERT-Verbund
Vorfälle
FIRST
Informationen
Analyse
Info-Management
Sensoren
Daten
Firewalls
Router
Hosts-IDS
Network-IDS
Schnittstellen
Lagebild
BMI / BSI
Krisenmanagement
Kritis
Lagebild
Partner
Fallstudien
Einzelberichte
Vorfallsbearbeitung
Alarmierung
CERTs


Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Wed Sep 13 01:00:00 2000 Flows/s any protocol
Packets
Traffic
Impact
Rating


Lagebild: Gesamt
Bewertung
Zusammenfassung
Aktuelle Entwicklungen
Index
Öffentliche Quellen

Last but not least: Citizens



Services to warn and alert citizens

When the wildfire spreads,
we need the sirens to sound alarm.

Citizen's CERT - „Bürger-CERT"

BÜRGERCERT

- Launched March 2006
- Spin-off from MCERT (CERT for small and medium enterprises) (discontinued)
- Free service, run by the BSI since 2007
- Target group: (>) average computer users, easy to understand
- Mainly advertised via trade fairs and www.bsi-fuer-buerger.de
- Approx. 80,000 subscribers to push services
- 3 main categories
  - Technical Warning
  - Bi-weekly Newsletter
  - Special Issue (Alert)

BÜRGER CERT

Ins Internet – mit Sicherheit

Startseite
Über uns
Fragen und Antworten
Partner
Hilfstexte
Glossar
Archiv
Abonnieren
Nutzerdaten

Ein Projekt von

Bundesamt für Sicherheit in der Informationstechnik

Sie sind hier: Startseite

Das Bürger-CERT informiert und warnt Bürger und kleine Unternehmen schnell und kompetent vor Viren, Würmern und Sicherheitslücken in Computeranwendungen – kostenfrei und absolut neutral. Unsere Experten analysieren für Sie rund um die Uhr die Sicherheitslage im Internet und verschicken bei Handlungsbedarf Warnmeldungen und Sicherheitshinweise per E-Mail. Das Bürger-CERT ist ein gemeinsames Projekt des Bundesamtes für Sicherheit in der Informationstechnik und Mcert Deutsche Gesellschaft für IT-Sicherheit. Wenn auch Sie auf Nummer Sicher gehen wollen, abonnieren Sie unsere Dienste.

Aktuelle Sicherheitsinformation

04.04.2007: Schwachstelle in Windows Betriebssystemen
Microsoft schließt mit dem neuen Sicherheitsupdate MS07-017 eine kritische Schwachstelle in Windows Betriebssystemen, die bereits aktiv zur Verbreitung von Schadsoftware ausgenutzt wird. Das Bürger-CERT rät, dieses Windows-Update möglichst umgehend zu installieren.
Weitere Informationen zu dieser Schwachstelle finden Sie in der Technischen Warnung Bcert-2007-0060.

Technische Warnungen

11.04.2007
Lücke im Windows Kernel ermöglicht Rechteerweiterung: Durch einen Fehler im Windows Betriebssystem können lokal angemeldete Nutzer erweiterte System-Privilegien erlangen.
mehr

Newsletter "Sicher • Informiert"

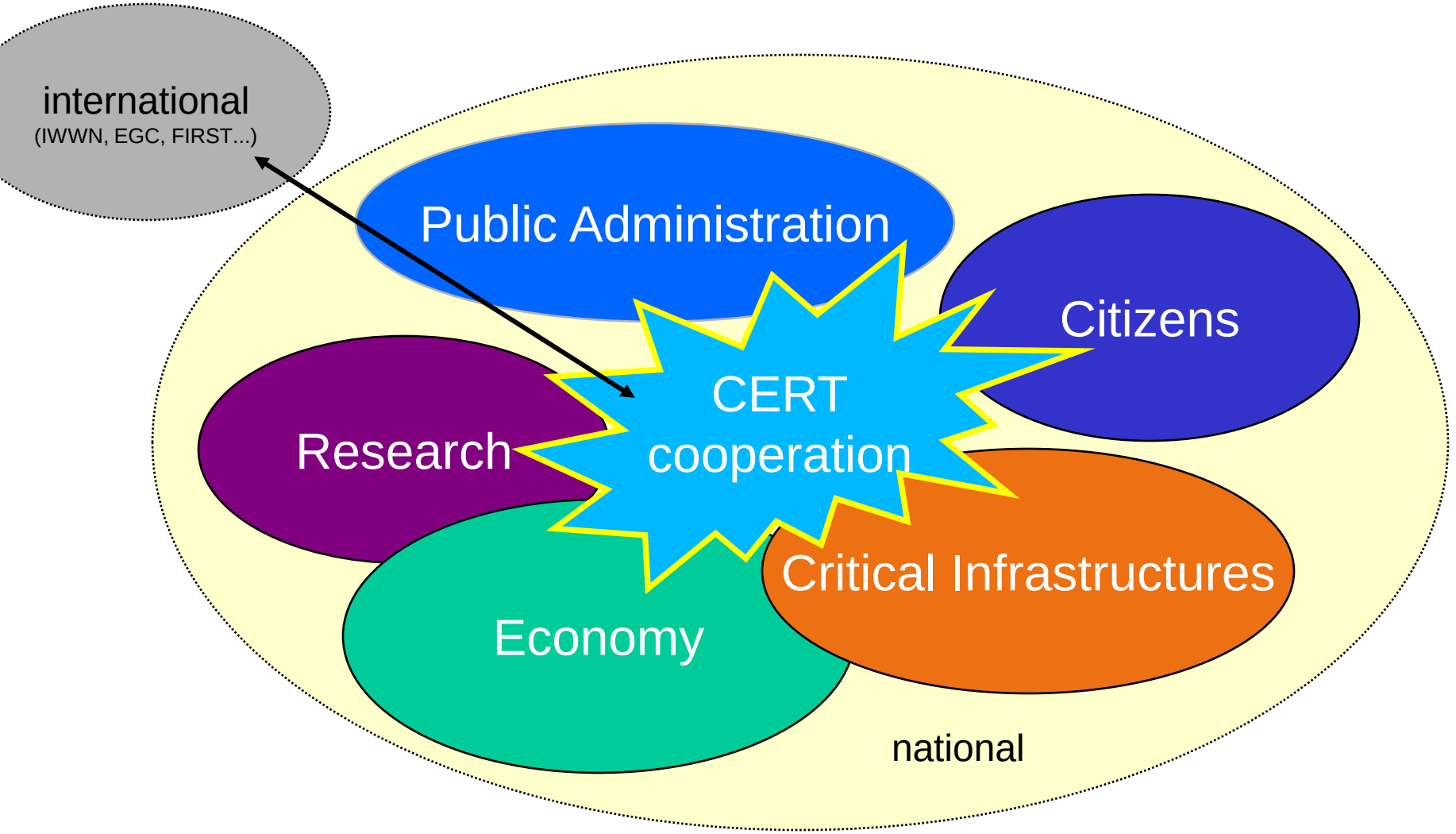
12.04.2007
Diese Woche schließt Microsoft mehrere Sicherheitslücken. Außerdem gibt es Schwachstellen in den Kommunikationstools Instant Messenger und ICQ von AOL sowie im Yahoo Messenger.
mehr

Extraausgabe "Sicher • Informiert"

03.04.2007
Vorsicht bei animierten Mauszeigern: Pfeilangriff auf Windows
mehr

Im Bürger-CERT suchen

Summary: National CERT Cooperation



Summary

- **All levels** (public, private, research, citizen, CIP) are covered by **different facilities**.
- **Cooperation** among CERTs is **inevitable**, because the focus of each CERT is different and others can benefit.
- **CERT-Bund,** the German national CERT, and **the IT-Situation Centre** respectively, is **PoC for national and international incidents** and **neutral information hub** for intersecting matters.
- Sectors of **critical infrastructures establish SPOCs** for information distribution and aggregation and connect to the IT-Situation Centre.
- The cooperation of CERTs supports in **reaching strategic aims** and projects with national focus.
- Consider the **weakest link**. Inform the **citizen**.

Contact Details

Bundesamt für Sicherheit in der Informationstechnik (BSI)

André Vorbach
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228 99-9582-5830
Fax: +49 (0)228 99-10-9582-5830

andre.vorbach@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de
www.buerger-cert.de