Bundesministerium
des Innern

National IT-Security Strategy -

National Plan for Information Infrastructure Protection

Dr. Stefan Grosse
Project Group "Communication and Security"
IT Security
Federal Ministry of the Interior

Nationaler Plan
zum Schutz der
Informationsinfrastrukturen

Overview

- Threat Situation
- New Orientation in IT-Security - General aspects
- National Plan
  - Prevention
  - Preparedness
  - Sustainability
- Implementation
- Selected Measures

The threat situation of information infrastructures

Threat quantity

- **Annual multiplication of the number of vulnerabilities of IT products**
- **Annual multiplication of malicious software (7,300 new variants in the second half of 2004)**
- **Approx. 160.000 known viruses, worms, etc.**

Threat quality

- **Impact of modern malware without user interaction:**
  - „fast“, highly evolved, target oriented and difficult to detect
- **trend towards unobtrusive spyware (Trojans) that**
  - is specifically programmed for espionage or
  - is rented out in the form of “botnets” for criminal purposes

Change of perpetrator skills

- **Organised crime instead of script kiddies**
- **Attackers become more professionell and international**

National Plan - Strategic Objectives

On 13 July 2005 the Federal Government adopted a comprehensive IT security strategy, i.e. the

“National Plan for Information Infrastructure Protection”

This plan has **3 strategic objectives:**

- **Prevention**: Protecting information infrastructures adequately
- **Preparedness**: Responding effectively to IT security incidents
- **Sustainability**: Enhancing German competence in IT security/ Setting international standards

Addressees: **the Public Administration, critical infrastructures, private businesses, the general public**

New orientation

This strategy is the key element of a **new orientation** towards IT security and can be seen as a **response** to the **threat situation** and the action the latter requires.

Key tasks :

- Introduce the National Plan as a political **“umbrella strategy”**
- **Implementation** of the strategy in **implementation plans**
- Expansion and **re-definition** of the role of the **Federal Office for Information Security** (BSI) (2005/2006) and
- Establishment of the **Project Group “Communication and Security”** (PG KS) at the Federal Ministry of the Interior

Strategic objective: Prevention

Reduce security risks associated with the use of information technology by

- disseminating **knowledge** about threats and **protection** possibilities
- clearly defining **responsibilities** for security, setting up a **security management**, and implementing **security measures**, and
- using **trustworthy** products and processes.

Prävention

Strategic objective: Prevention

#1 Raise **awareness** of risks related to IT use

#2 Use of **safe** IT products and **secure** IT systems

#3 Respect **confidentiality**

#4 Putting **safeguards** in place

#5 Creating **framework** conditions and **guidelines**

#6 Coordinated security **strategies**

#7 Shaping **policy** on national and international level

Prävention

Strategic objective: Preparedness

Time is of the essence when responding to disruptions of information infrastructures.

Primary tasks include

- **collecting** and **analyzing** information,
- **warning** and **alerting** of those potentially affected, and
- taking measures to **contain the damage**.

Reaktion

Strategic objective: Preparedness

#8 Identifying, registering and evaluating **incidents**

#9 **Informing**, **alerting** and **warning**

#10 **Responding** to IT security **incidents**

Strategic objective: Sustainability

In addition to the political will and the commitment of all competent parties, to ensure long-term protection of national information infrastructures and to strengthen IT security, Germany needs

- technical expertise**,**
- **national** know-how**,**
- **trustworthy** IT services and IT security products**.**

Nachhaltigkeit

Strategic objective: Sustainability

#11 Promoting **trusted** and **reliable** information technologies

#12 Enhancing **national** competence in IT security

#13 IT security **competence** in **school** education and professional training

#14 Promoting **research** and **development**

#15 Expanding **international cooperation** and setting **standards**

Nachhaltigkeit

National Plan – Implementation

- Develop measures jointly with other federal ministries
- Agree on standards for IT security in the federal administration

- Develop measures jointly with operators of critical infrastructures
- Ensure an equally high basic level of IT security
- Agree on an implementation approach for critical infrastructures

Measures (Selection) i.e.:
Strategic objective: Preparedness # 8,9,10

Multi-Level Approach

- Internal Measures
  - Implementation Plan Bund
  - “IT Crisis Response Centre”
  - Early warning system
- National Measures
  - Implementation Plan Critical Infrastructures
  - Public private partnerships
  - CERT-Alliance
- International Measures
  - EGC - European Government CERT Group
  - International Watch and Warning activities
  - Bilateral co-operation

Strategic objective: Preparedness
Internal Measures

- **“IT Crisis Response Centre”**
  - **24/7 (8/7)** availability
  - **Pool** of approx. 100 **specialists** throughout BSI
  - compiling **daily reports**

Strategic objective: Preparedness
Internal Measures

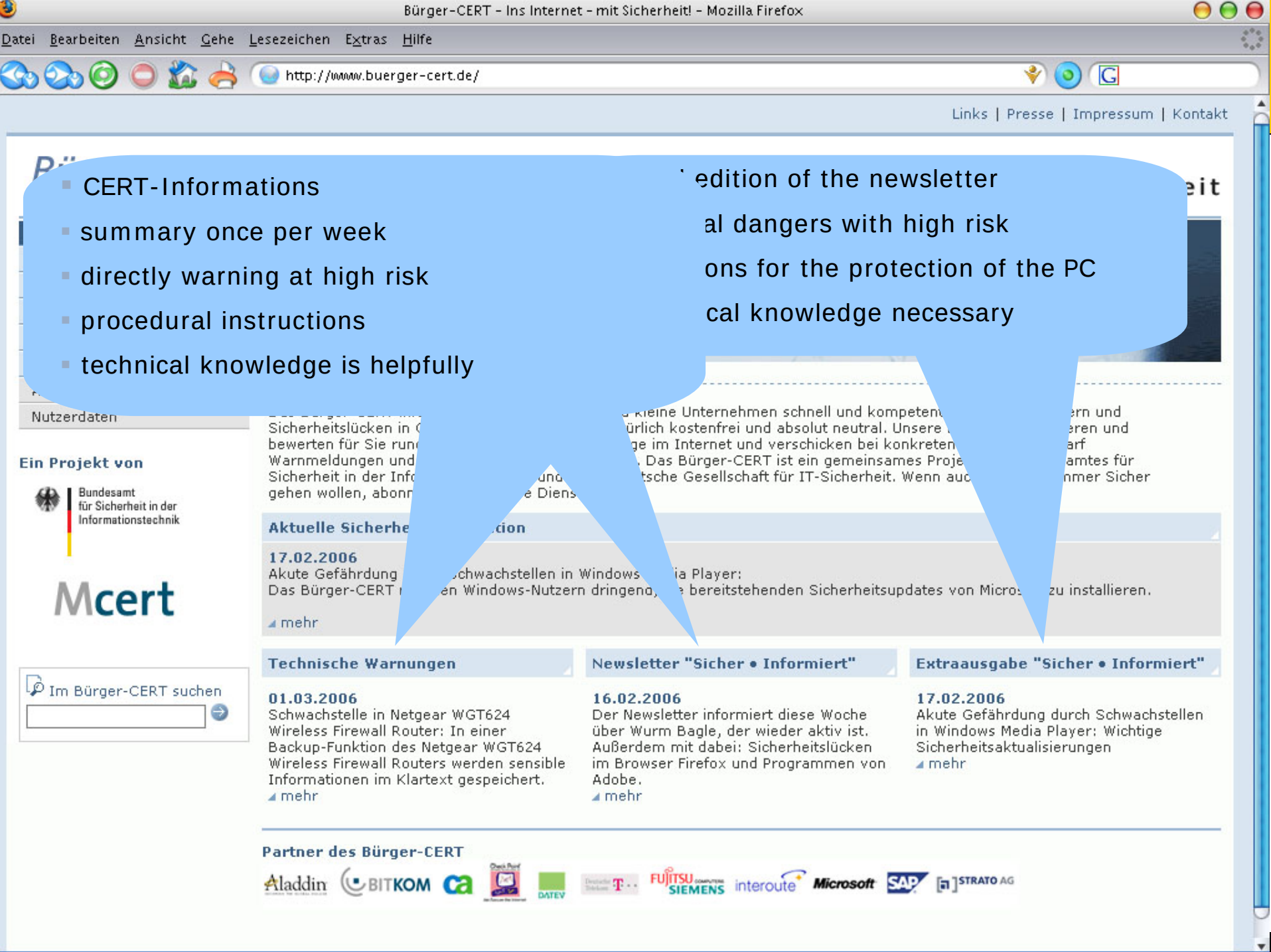
National Early Warning System

- **Public Information** (Online Publications, News, Defacement Archives, Open Security Community, …)
- **Non-public Information** (Governmental Institutions, IVBB, Bilateral / Multilateral Coop., Closed Security Community,…)
- **Technical Projects**
  - Internet Analysis System (IAS)
  - Early Warning in the German Internet (CarmentiS)
  - Botnets & Trojans
  - Honeynets, Honeypots & Malware Collector Systems
- **Non-Technical Considerations**
  - Public-Private-Partnerships *(especially Critical Infrastructures)*
  - Information Sharing & Co-operation *(IWWN; EGC; CERT-Alliance)*

Strategic objective: Preparedness
National Measures

Bürger-CERT

For ?	**Citizens and Small Business Companies**
From ?	**Federal Office for Information Security (BSI) and Mcert German Association für IT-Security sponsored by leading business-partners such as:**
Why ?	**Preventing clearing-up over the dangers and risks of the Internet use**
How ?	**Understandable safety information**
How much ?	**free**
Where ?	**www.buerger-cert.de**


Bürger-CERT - Ins Internet - mit Sicherheit! - Mozilla Firefox
Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe
http://www.buerger-cert.de/
Links | Presse | Impressum | Kontakt
CERT-Informations
summary once per week
directly warning at high risk
procedural instructions
technical knowledge is helpfully
edition of the newsletter
al dangers with high risk
ons for the protection of the PC
cal knowledge necessary
Nutzerdaten
Ein Projekt von
Bundesamt für Sicherheit in der Informationstechnik
Mcert
Im Bürger-CERT suchen
Technische Warnungen
01.03.2006
Schwachstelle in Netgear WGT624 Wireless Firewall Router: In einer Backup-Funktion des Netgear WGT624 Wireless Firewall Routers werden sensible Informationen im Klartext gespeichert.
mehr
Newsletter "Sicher • Informiert"
16.02.2006
Der Newsletter informiert diese Woche über Wurm Bagle, der wieder aktiv ist. Außerdem mit dabei: Sicherheitslücken im Browser Firefox und Programmen von Adobe.
mehr
Extraausgabe "Sicher • Informiert"
17.02.2006
Akute Gefährdung durch Schwachstellen in Windows Media Player: Wichtige Sicherheitsaktualisierungen
mehr
17.02.2006
Akute Gefährdung
Das Bürger-CERT
Windows-Nutzern dringend
bereitstehenden Sicherheitsupdates von Micros
zu installieren.
mehr
Partner des Bürger-CERT
Aladdin BITKOM ca DATEV FUJITSU SIEMENS interoute Microsoft SAP STRATO AG

CERT-Alliance

- First mention: december 2001 - Signing: 29. august 2002
- Private-Public-Partnership – approx. 40 members
- Signing members: CERT-Bund, DFN-CERT, IBM BCRS, S-CERT, Siemens-CERT und Telekom CERT
- “Tight cooperation”:
  - based on a signed Code of Coduct“
  - responsibilites, commitments
- „Loose cooperation“
  - based on an NDA
  - regular meetings: CERT-Workshop,
  - exchange opinions and experiences and contact informations,
  - develop common views and strategies

Measures (Selection) i.e.:
#14 Promoting research and development

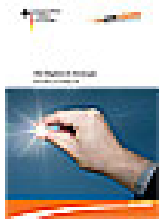
In 2006 the Federal Government adopted a national strategy

the **“Hightech strategy”**

With 17 priorities for the future.

IT-Security **is part of the priorities:**

- **Safety and security technologies**
- **Information and communication technologies**



Thank you for your attention!

Dr. Stefan Grosse
Project Group “Communication and Security”
IT Security
Federal Ministry of the Interior

pgksbund@bmi.bund.de