Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheit – Herausforderung für Staat und Gesellschaft

Michael Hange
Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

Bonn, 28. September 2010

Bundesamt
für Sicherheit in der
Informationstechnik

Agenda

- Das BSI
- Bedrohungslage IT- und Datensicherheit
- Lösungen: Botfrei-Initiative, Neuer Personalausweis
- Cloud Computing
- BSI-Services für Unternehmen

Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI: Aufgaben und Kompetenzen

Zentraler IT-Sicherheitsdienstleister des Bundes

Nationale Behörde für Cyber-Sicherheit

Neues BSI-Gesetz seit Mitte 2009:

- Zentrale Meldestelle
- Warnung vor Sicherheitsrisiken
- Prüfung und Zertifizierung von Produkten
- Technische Richtlinien / Mindeststandards

Eigene Projekte und Initiativen mit Partnern

- Fachkompetenz
- Unabhängigkeit / Neutralität

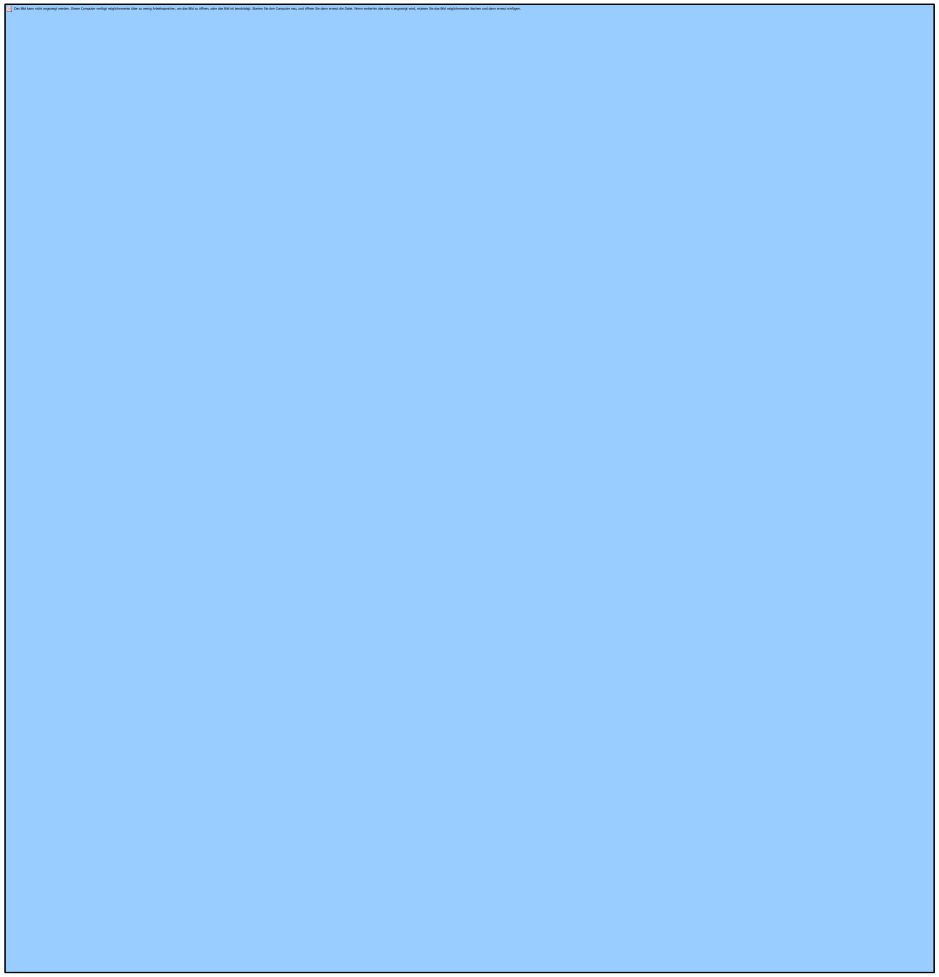
Bundesamt
für Sicherheit in der
Informationstechnik

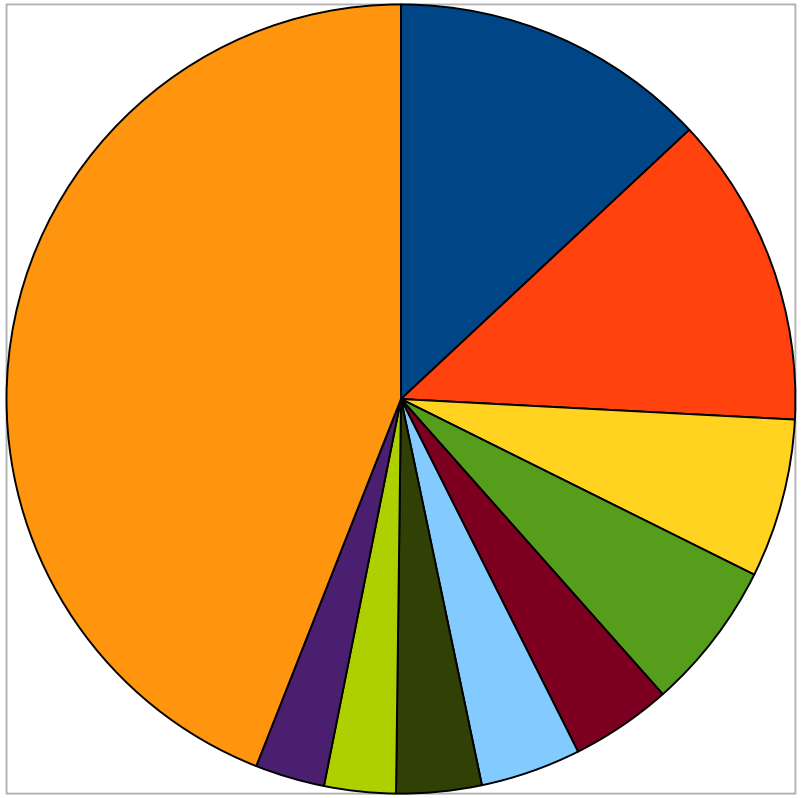
IT-Sicherheitslage

- Professionalisierung der Internetkriminalität schreitet voran
- Schadprogramme ermöglichen erhebliche Gewinne und verursachen Schäden in Milliardenhöhe
- Gefährdungstrends BSI Lagebericht zur IT-Sicherheit 2009
  - SPAM, Identitätsdiebstahl, DDoS-Angriffe, Trojaner, Spyware
- Eine Hauptursache: Botnetze

Bundesamt
für Sicherheit in der
Informationstechnik

Spam Juli 2010





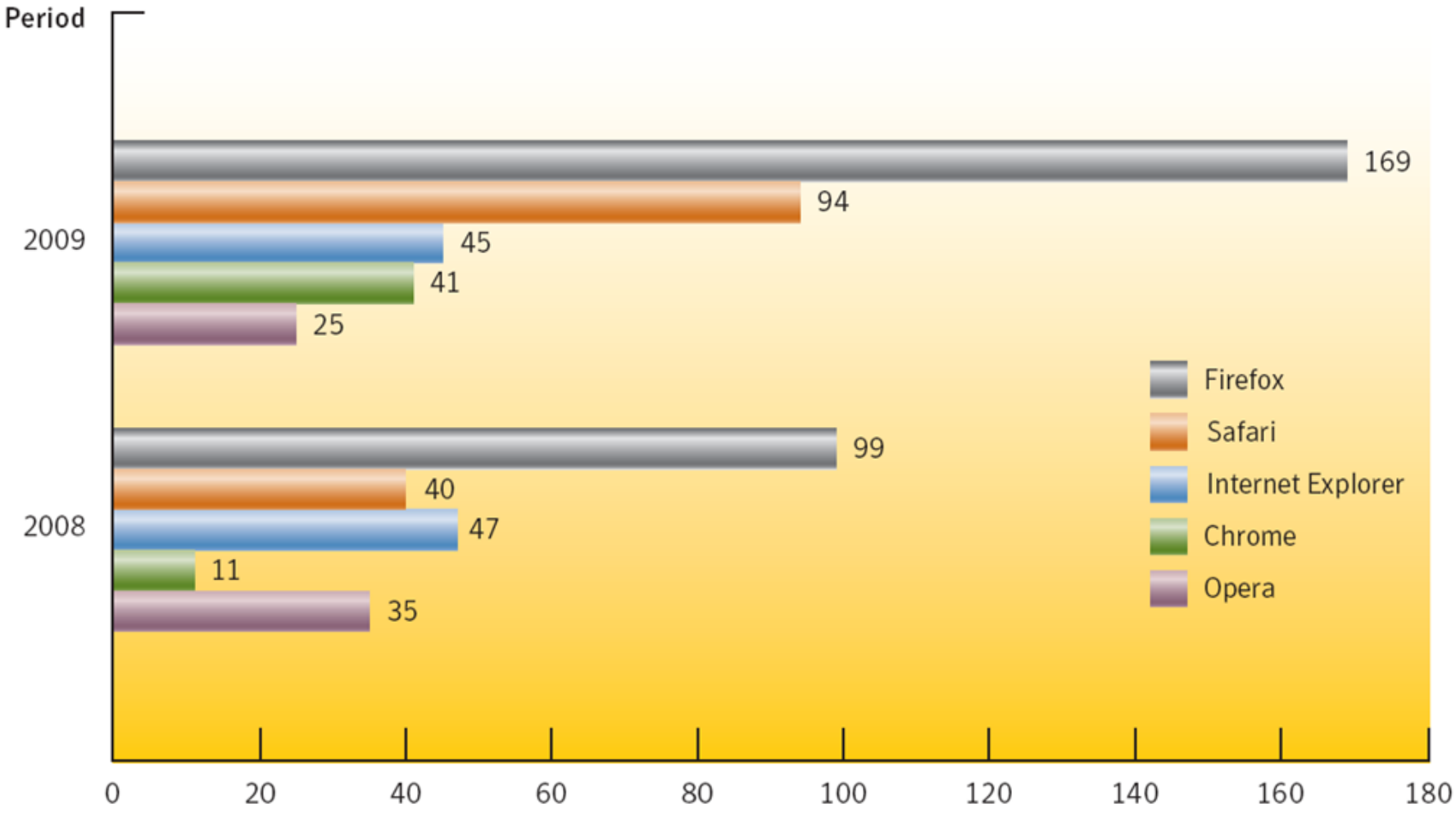
Quelle:
BSI

Quelle: Trend Micro

80% der infizierten Rechner sind mehr als **30 Tage** infiziert!

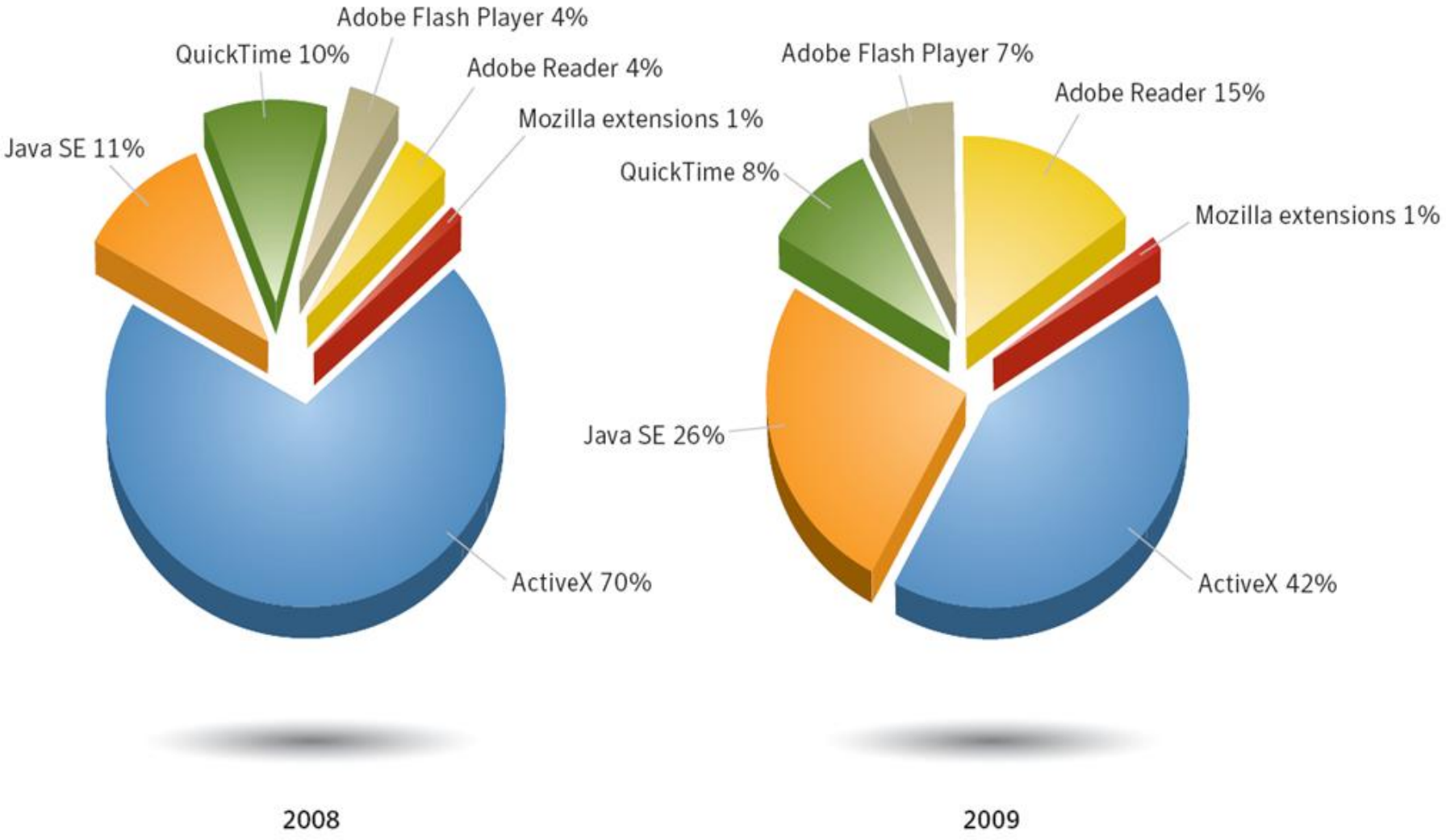
50% der infizierten Rechner sind mehr als **300 Tage** infiziert!

Sicherheitslücken in Webbrowsern



Quelle: Symantec Threat Report XV, April 2010

Sicherheitslücken in Browser-Plugins



Quelle: Symantec Threat Report XV, April 2010

Bundesamt
für Sicherheit in der
Informationstechnik

Stuxnet-Angriff – Unternehmenssysteme im Fokus

- Gezielter Angriff auf SCADA-Prozessleitsysteme von Siemens
- Professionelle Industriespionage/-sabotage vermutet
- Angriffsqualität bisher einzigartig
- Auch deutsche Unternehmen betroffen

heise Security

News-Meldung vom 23.07.2010 11:34

LNK-Lücke in Windows: Angriffswelle rollt an

Die kritische **LNK-Lücke[1]** in Windows ist nach wie vor ungepatcht und ruft zunehm
auf den Plan: Inzwischen haben mindestens zwei weitere Schädlinge die Schwachs

News-Meldung vom 20.07.2010 17:02

Windows-LNK-Lücke: Lage spitzt sich zu

Während Microsoft noch an einem Patch arbeitet, spitzt sich die Lage weiter zu: Aufgrun
kritischen **LNK-Sicherheitslücke[1]** in den meisten Windows-Versionen hat das Interne
Center (ISC) nun die Gefahrenwarnstufe von Grün auf Gelb **erhöht[2]**. Hiermit will das I

Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI | Themen | Aktue

esse

rzmitteilungen
essearchiv

› Startseite › Presse › Neue Sicherheitslücke im Windows-Betriebssystem von Microsoft

Neue Sicherheitslücke im Windows-Betriebssystem von Microsoft

BSI empfiehlt kurzfristige Umsetzung der von Microsoft beschriebenen Workarounds

Bundesamt
für Sicherheit in der
Informationstechnik

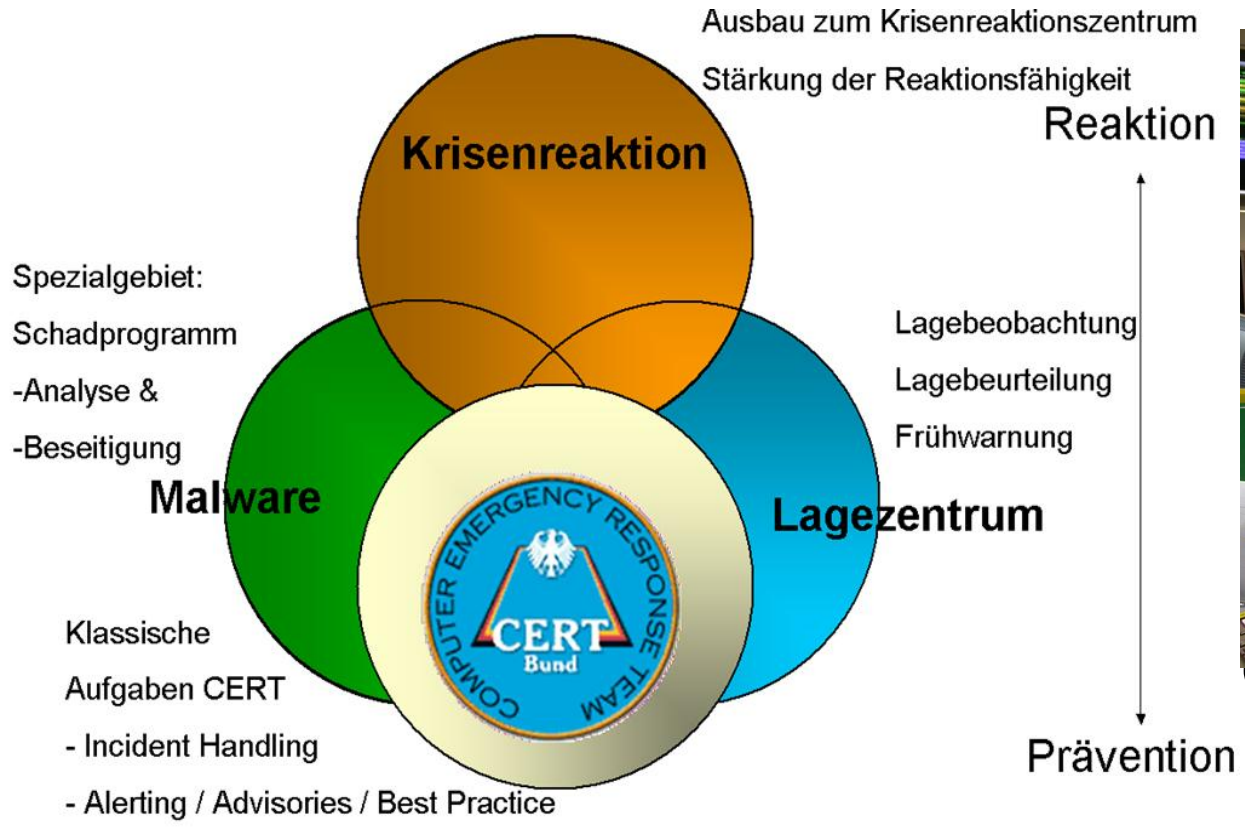
BSI-Lagezentrum

Aktuelle IT-Sicherheitslage in Deutschland

- ➲ Tägliche Lagebeobachtung
- ➲ Monats-/Quartalslageberichte
- ➲ Technische Warnmeldung
  - Advisories, Kurzinformationen
  - Bürger-CERT-Newsletter
- ➲ Zweijahresbericht “Die Lage der IT-Sicherheit in

Bundesamt
für Sicherheit in der
Informationstechnik

BSI IT-Lage- und Analysezentrum



Organisatorische und technische Vorbereitung für den Aufwuchs zum IT-Krisenreaktionszentrum

Bundesamt
für Sicherheit in der
Informationstechnik

1. November 2010:
Neuer Personalausweis

Sichtausweis

Der neue Personalausweis vereint den herkömmlichen Ausweis und die drei neuen elektronischen Funktionen im Scheckkartenformat.

Elektronische Funktionen

1. Elektronischer Identitätsnachweis: eID-Funktion

- für E-Business- und E-Government
- PIN und Berechtigungszertifikat erforderlich

2. Unterschriftsfunktion: Qualifizierte elektronische Signatur

- nachträglich auf den Ausweis nachladbar

3. Hoheitliche Funktion

- digitales Lichtbild und (auf Wunsch) zwei elektronische Fingerabdrücke
- ausschließlich für zur Identitätsfeststellung berechtigte Behörden, z. B. Polizei und Grenzkontrolle

Bundesamt
für Sicherheit in der
Informationstechnik

Vorteile des elektronischen Identitätsnachweises

- Einfaches und sicheres Identifizieren im Internet

- Erhöhte Sicherheit gegenüber der bisherigen Passwortidentifizierung

bisher: Passwort oder PIN = nur Wissen

künftig: Personalausweis + PIN = Besitz + Wissen

- Sichere medienbruchfreie Abwicklung von Online-Diensten unabhängig von Öffnungszeiten, fehlerfreie Datenübermittlung

- Berechtigungszertifikat mit Erforderlichkeitsprüfung Datenübermittlung nur im Rahmen des Berechtigungszertifikats

- Einheitliche standardisierte Schnittstelle ➔ überwiegend Nutzung des neuen Ausweises zur Authentisierung bei Online-Diensten

- Verschlüsselte Übertragung

Bundesamt
für Sicherheit in der
Informationstechnik

Neuer Personalausweis - Anwendungsgebiete

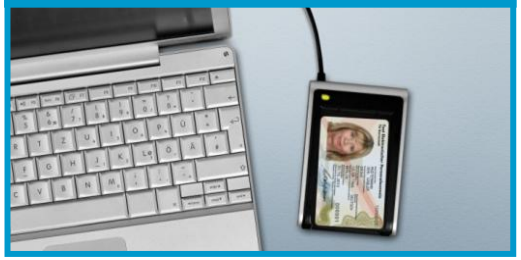
Zugang mit Pseudonym

Altersverifikation

Bürgerdienste

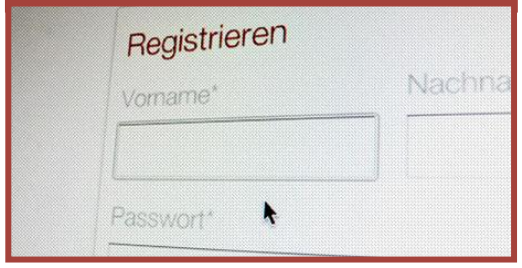
Kiosksysteme / Infoterminals

Automat. Formularbefüllung



Elektronische Signatur

Online-Registrierung

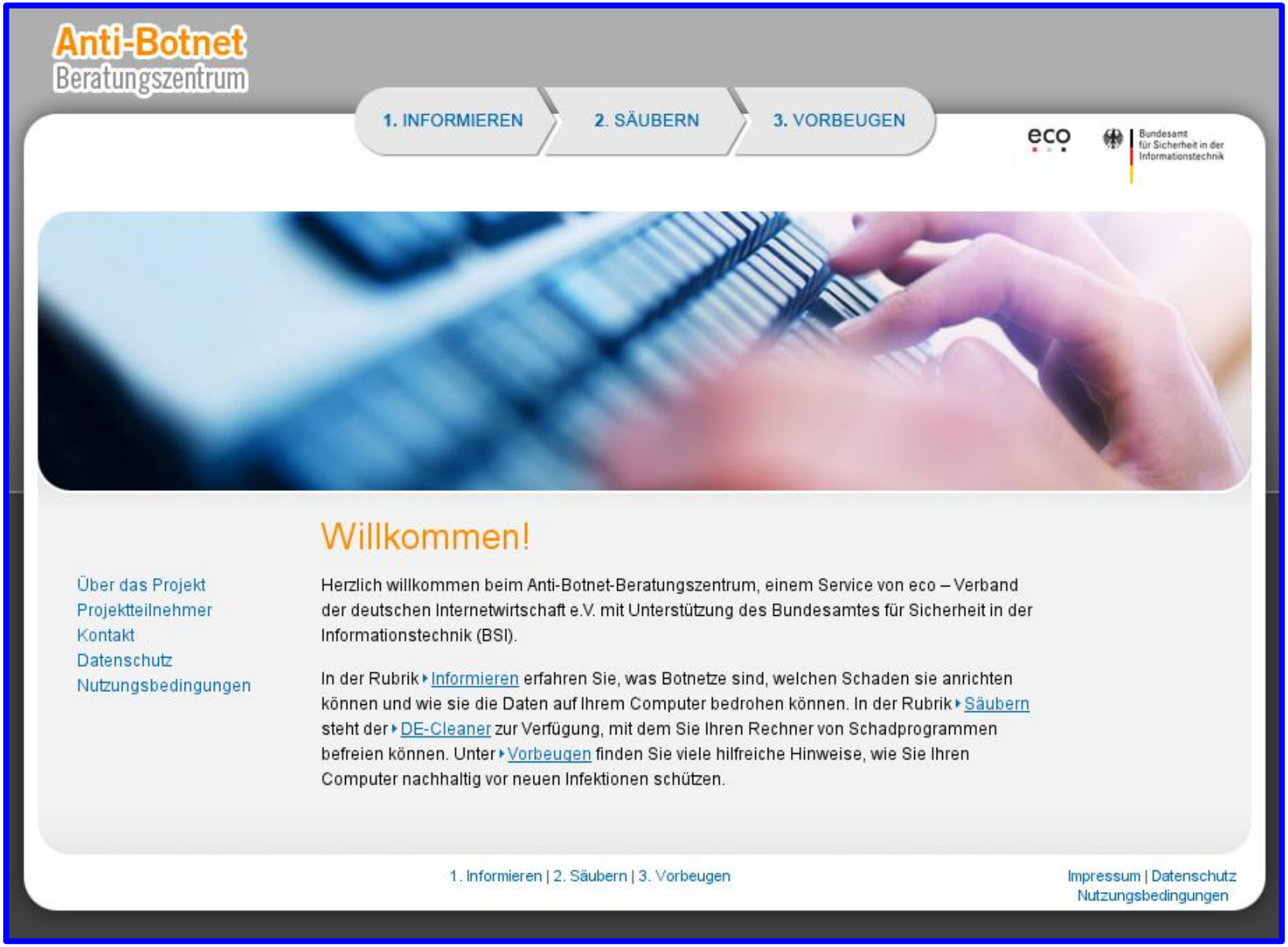


Zutrittskontrollen

Barrierefreie Internetdienste

Bundesamt
für Sicherheit in der
Informationstechnik

Anti-Botnet-Beratungszentrum
www.botfrei.de



Bundesamt
für Sicherheit in der
Informationstechnik

Anti-Botnet-Beratungszentrum
Anwender-Support

Informieren:
Hintergrundinformationen zu Schad-programmen, Botnetzen und dem Projekt

Vorbeugen
Einfache und effiziente Maßnahmen zur Vermeidung von Neuinfektionen wie Updates, AV-Produkte,...

Säubern:
- DE-Cleaner
- DE-Cleaner Rettungssystem-CD
- Weitere Tools wie Online-Scanner

Bundesamt
für Sicherheit in der
Informationstechnik

Cloud Computing

Ziel: Informationssicherheit beim „Cloud Computing“

- BSI hat Eckpunktepapier zum Thema „Cloud Computing“ erstellt (als Diskussionsgrundlage)
- definiert Mindestsicherheitsanforderungen an Cloud-Anbieter
- Das Eckpunktepapier heute auf der BSI-Webseite veröffentlicht

Die fachlich interessierte Öffentlichkeit (Anbieter und Anwender) hat bis Anfang Januar 2011 Gelegenheit die Mindestsicherheitsanforderungen zu kommentieren

Feedback-Möglichkeit an das BSI:

per E-Mail an cloudsecurity@bsi.bund.de oder bei XING:
→ Diskussionsgruppe IT-Grundschutz mit Forum Cloud Security

Bundesamt
für Sicherheit in der
Informationstechnik

IT-und Datensicherheit durch IT-Grundschutz

Sicherheitsbedarf, Anspruch

-

°

+

Leitfaden IT-Sicherheit

Webkurs zum Selbststudium

BSI Standard 100-1: ISMS

Hilfsmittel & Musterrichtlinien

Software: „GSTOOL“

BSI Standard 100-2: IT-Grundschutz-Vorgehensweise

Beispiele: „GS-Profile“

ISO 27001-Zertifikat

BSI Standard 100-3: Risikoanalyse

IT-Grundschutz-Kataloge

Bundesamt
für Sicherheit in der
Informationstechnik

Wichtige IT-Sicherheitsmaßnahmen

Vernetzung

1. Netzdesign
- Netzsegmentierung
- Internetnutzung

2. Schutz der Netzgrenzen
- intern & Außengrenze
- Firewall & Virenschutz

3. Protokollierung
- Internetkommunikation
- Dateizugriffe

Arbeitsplatz-Rechner
- Schutzprogramme: Erweiterte Desktop Firewall, Virenschutz
- Härtung (Berechtigungen, Reduzierung von Schwachstellen)
- Protokollierung der Netzzugriffe
- Auffinden von Systemveränderungen und unbekannten Prozessen

Mitarbeiter
- Schulung: Technik, Social Engineering
- Sensibilisierung, Kontrolle

Daten und Informationen
- Speicherort (lokal, Netz, Stand-alone-System)
- Zugangsschutz, Berechtigungen, Verschlüsselung

Bundesamt
für Sicherheit in der
Informationstechnik

Information und Aufklärung

Bonner Unternehmertage 2010

Vielen Dank!

Michael Hange
Bundesamt für Sicherheit in der
Informationstechnik (BSI), Bonn

Bonn, 28. September 2010