

A decorative graphic element on the left side of the slide, consisting of a black vertical bar, a red square, and a yellow square.

IT-Sicherheit – Herausforderung für Staat und Gesellschaft

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

Bonn, 28. September 2010





Agenda

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



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

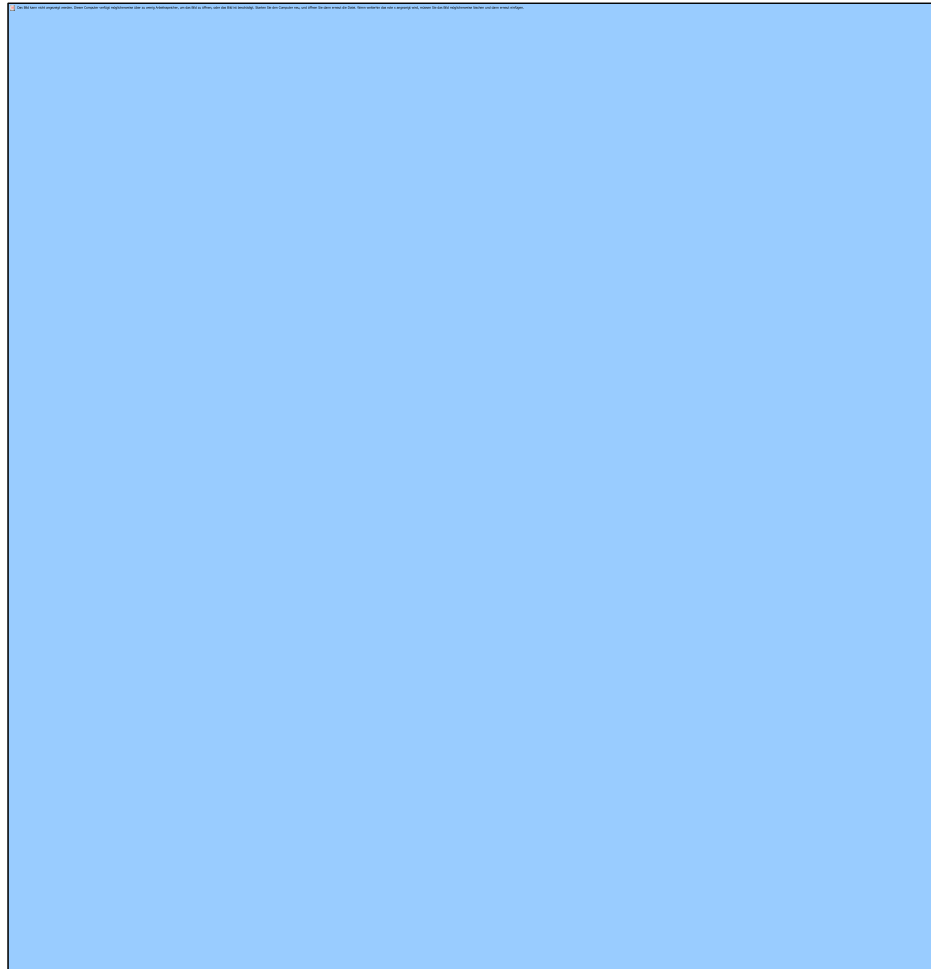


IT-Sicherheitslage

- 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

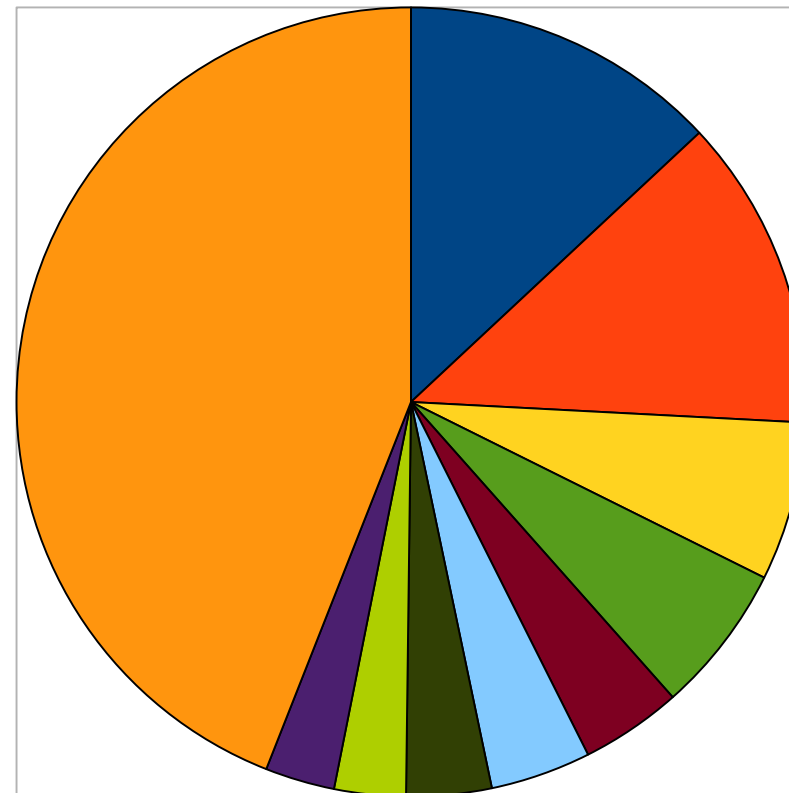


Spam Juli 2010



Quelle:
BSI

Quelle: Trend Micro



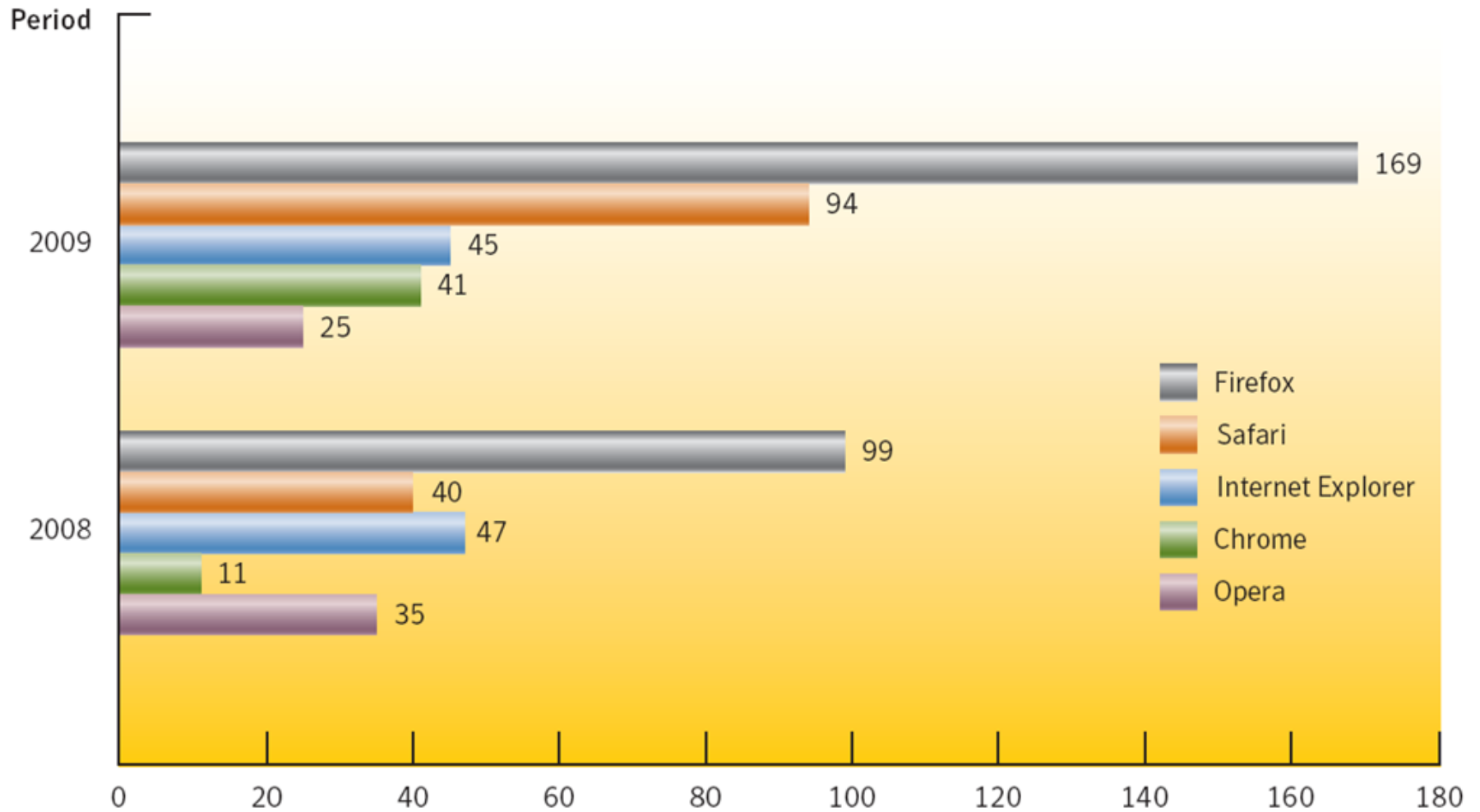
- Brasilien
- Indien
- Vietnam
- Deutschland
- UK
- USA
- Russland
- Italien
- Saudi Arabien
- Andere

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

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



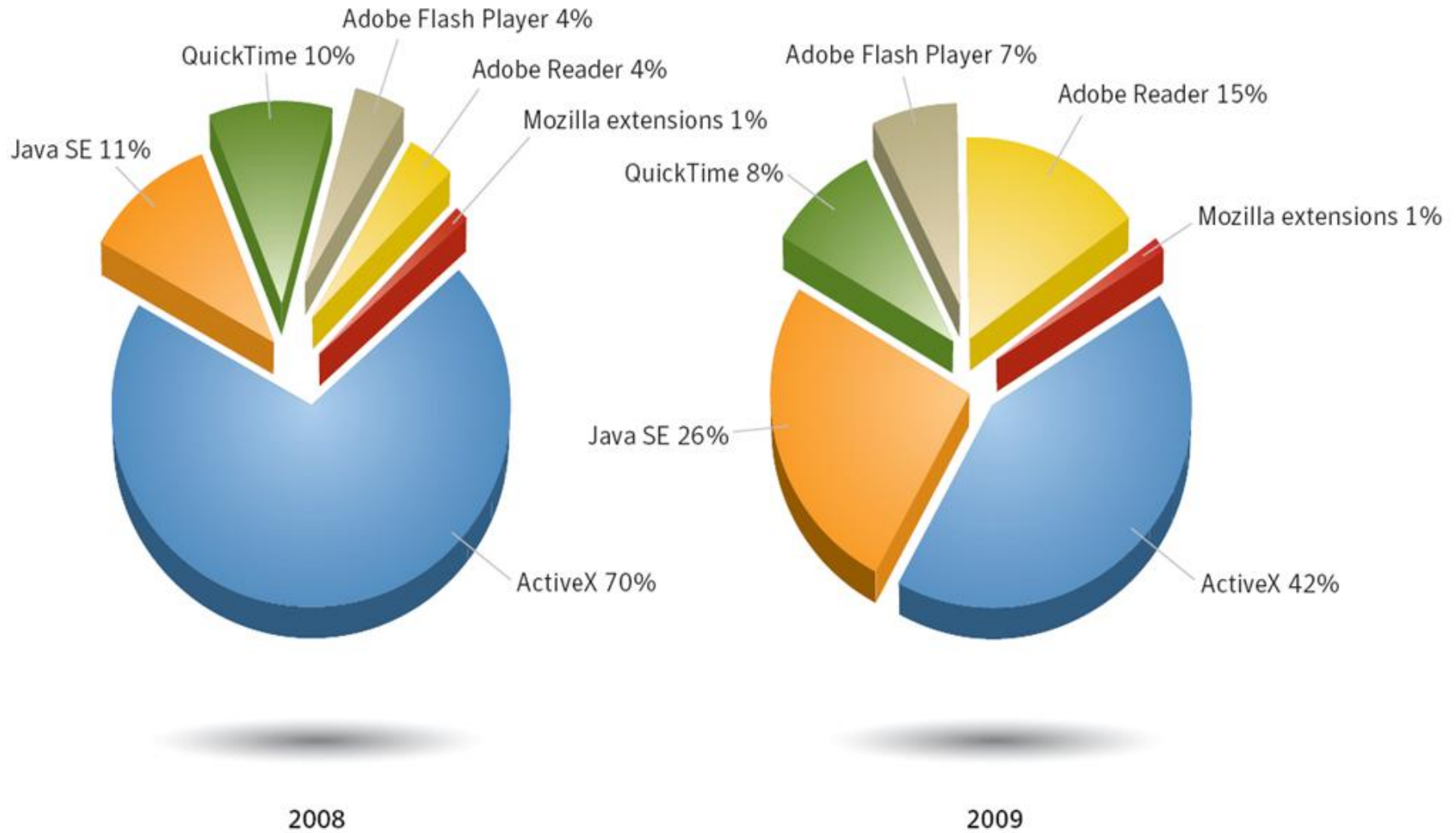
Sicherheitslücken in Webbrowsern



Quelle: Symantec Threat Report XV, April 2010



Sicherheitslücken in Browser-Plugins



Quelle: Symantec Threat Report XV, April 2010



Stuxnet-Angriff – Unternehmenssysteme im Fokus

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



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 zunehmend auf den Plan: Inzwischen haben mindestens zwei weitere Schädlinge die Schwachstelle

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: Aufgrund der kritischen **LNK-Sicherheitslücke**[1] in den meisten Windows-Versionen hat das Internet Security Center (ISC) nun die Gefahrenwarnstufe von Grün auf Gelb **erhöht**[2]. Hiermit will das I

[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





BSI-Lagezentrum

Aktuelle IT-Sicherheitslage in Deutschland

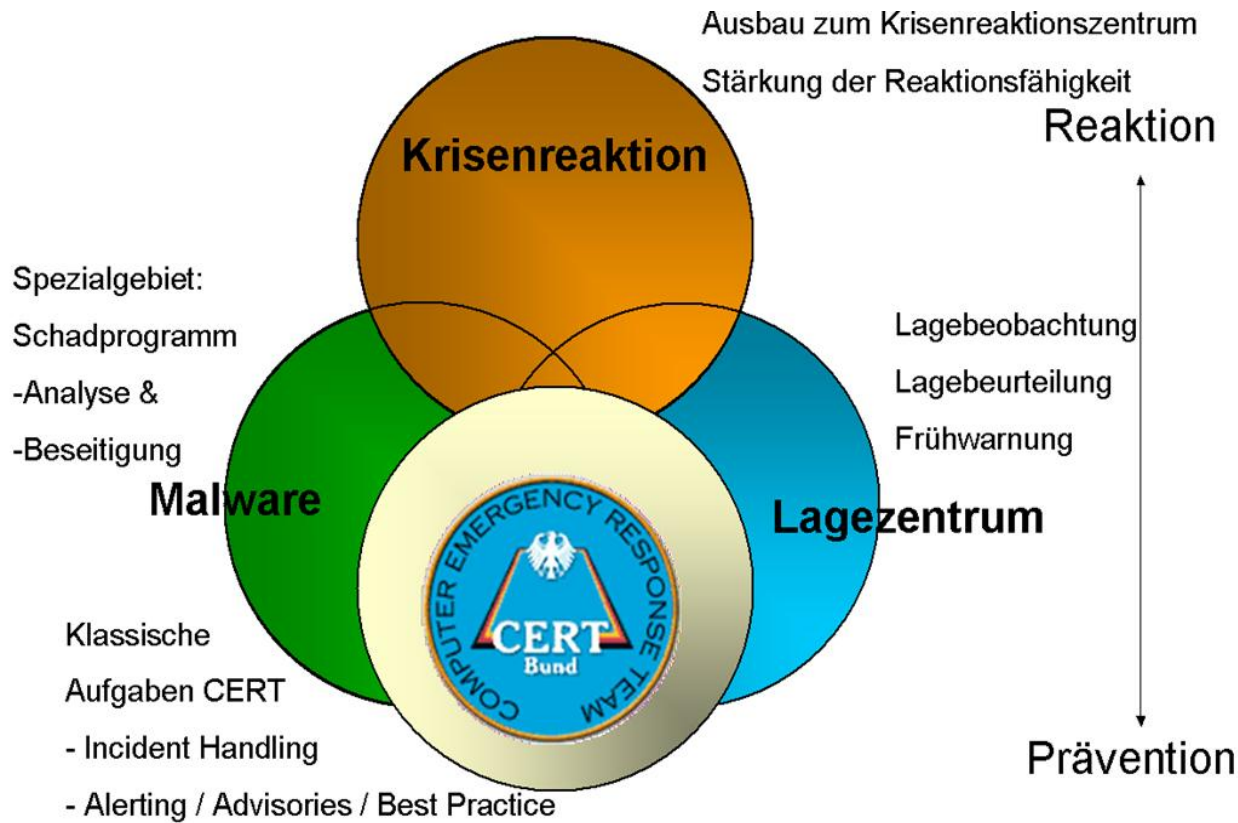
- ➔ Tägliche Lagebeobachtung
- ➔ Monats-/Quartalslageberichte
- ➔ Technische Warnmeldung
 - Advisories, Kurzinformationen
 - Bürger-CERT-Newsletter
- ➔ Zweijahresbericht "Die Lage der IT-Sicherheit in

The collage includes the following elements:

- Top Left:** Cover of the report "Die Lage der IT-Sicherheit in Deutschland 2009" by the Bundesamt für Sicherheit in der Informationstechnik.
- Top Right:** Cover of the "Lagebericht 2. Quartal 2010" from the Nationales IT-Lagezentrum BSI.
- Bottom Right:** A diagram titled "ANGRIFFE & EREIGNISSE" showing a network architecture. It includes a "Webserver" connected to a "Webseite" (website) interface. The website is linked to an "Internet" cloud, which in turn connects to three "Adserver" (Adserver 1, 2, 3). Annotations explain that Adserver 1 is used for management and maintenance, while Adserver 2 and 3 are compromised. A "Server der Schadsoftware verteilt" (malware distribution server) is also shown. Text below the diagram states: "Webserver steht in Verbindung mit mehreren Adservern, die in Abhängigkeit eines Computers oder Zeilegruppe die Werbung anzeigen." and "Durch einen kompromittierten Adserver wird über den Webbrowser mit einem eingetragenen Name Schadsoftware von einem dafür vorgesehenen Server nachgeladen." It also notes that a visitor to the website is redirected to a malicious page when the browser is infected with malware.
- Bottom Left:** A "Kommentar" (comment) box stating: "Internet-Nutzer müssen inzwischen überall mit Schadcode rechnen – der Vorfall zeigt, dass".



BSI IT-Lage- und Analysezentrum



Organisatorische und technische
Vorbereitung für den Aufwuchs
zum IT-Krisenreaktionszentrum



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 berechnigte Behörden, z. B. Polizei und Grenzkontrolle



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





Neuer Personalausweis - Anwendungsgebiete

Zugang mit Pseudonym



Altersverifikation



Bürgerdienste



Kiosksysteme / Infoterminals



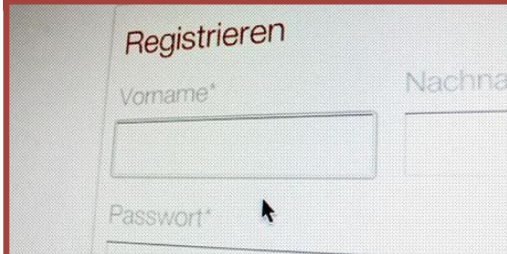
Automat. Formularbefüllung



Elektronische Signatur



Online-Registrierung



Zutrittskontrollen



Barrierefreie Internetdienste





Anti-Botnet-Beratungszentrum

www.botfrei.de

Anti-Botnet Beratungszentrum

1. INFORMIEREN

2. SÄUBERN

3. VORBEUGEN

eco



Bundesamt
für Sicherheit in der
Informationstechnik



Willkommen!

[Über das Projekt](#)
[Projektteilnehmer](#)
[Kontakt](#)
[Datenschutz](#)
[Nutzungsbedingungen](#)

Herzlich willkommen beim Anti-Botnet-Beratungszentrum, einem Service von eco – Verband der deutschen Internetwirtschaft e.V. mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

In der Rubrik [Informieren](#) erfahren Sie, was Botnetze sind, welchen Schaden sie anrichten können und wie sie die Daten auf Ihrem Computer bedrohen können. In der Rubrik [Säubern](#) steht der [DE-Cleaner](#) zur Verfügung, mit dem Sie Ihren Rechner von Schadprogrammen befreien können. Unter [Vorbeugen](#) finden Sie viele hilfreiche Hinweise, wie Sie Ihren Computer nachhaltig vor neuen Infektionen schützen.

[1. Informieren](#) | [2. Säubern](#) | [3. Vorbeugen](#)

[Impressum](#) | [Datenschutz](#)
[Nutzungsbedingungen](#)



Anti-Botnet-Beratungszentrum Anwender-Support

Anti-Botnet Beratungszentrum

1. INFORMIEREN

2. SÄUBERN

3. VORBEUGEN

eco



Bundesamt
für Sicherheit in der
Informationstechnik

Informieren:

Hintergrundinformationen zu Schadprogrammen, Botnetzen und dem Projekt

Vorbeugen

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

Über das Projekt
Projektteilnehmer
Kontakt
Datenschutz
Nutzungsbedingungen

können und wie Sie die Daten auf Ihrem Computer bedrohen können. In der Rubrik [Säubern](#) steht der [DE-Cleaner](#) zur Verfügung, mit dem Sie Ihren Rechner von Schadprogrammen befreien können. Computer nach

Säubern:

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



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-Grundschatz mit Forum Cloud Security



IT-und Datensicherheit durch IT-Grundschutz

Sicherheitsbedarf,
Anspruch

Webkurs zum
Selbststudium

Software:
„GSTOOL“

ISO 27001-Zertifikat

Leitfaden
IT-Sicherheit

BSI Standard 100-1:
ISMS

BSI Standard 100-2:
IT-Grundschutz-
Vorgehensweise

BSI Standard 100-3:
Risikoanalyse

Hilfsmittel &
Musterrichtlinien

Beispiele:
„GS-Profile“

IT-Grundschutz-
Kataloge





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 unbekanntem Prozessen

Mitarbeiter

- Schulung: Technik, Social Engineering
- Sensibilisierung, Kontrolle

Daten und Informationen

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



Information und Aufklärung



IT-Sicherheit

- Das Internet
- Der Browser
- Datensicherung
- Viren & andere Tiere
- Abzocker & Spione
- Infiziert - und nun?
- Schützen - aber wie?

Themen

- Kinderschutz
- Computerspiele
- Chat - aber sicher?
- Der Staat online
- Online-Banking
- Einkaufen im Internet
- WLAN
- Phishing
- Benutzerkonten / Netzwerk
- Handy
- Internettelefonie
- Suchmaschinen
- Open Source Software
- Recht im Internet

Aktuelles

- Newsletter
- Brennpunkt

Downloads

- Programme
- Bildschirm-schoner
- Druckversion
- Linkbanner

BSI für Bürger

Startseite
Ins Internet - mit Sicherheit

Im Internet surfen ist wie Autofahren – reinsetzen und starten. Doch halt: Auch auf der Datenautobahn besteht Unfallgefahr! Um einen Zusammenstoß mit Würmern, Viren oder anderen Störenfriedern zu vermeiden, sollten Sie Ihren Computer schützen. Wie, das erfahren Sie auf dieser Internetseite.

Soziale Netzwerke

Sicher unterwegs in studiVZ, Xing, Facebook & Co.



Das Internet ist längst nicht mehr die einzigen Themen, die kontrovers diskutiert werden. Auch (IT-) als Chance erkannt und nutzen die Güter. Gefahren in sozialen Netzwerken lauern, helfen Ihnen 10 Tipps dabei, sich sicher zu bewegen.

Viel Spaß bei der Lektüre und sichere Surfzeiten!

Ihr Argus
- offizielle Sicherheitsspürnase des BSI -

[Mehr >](#)

Schnelleinstieg

Die 10 wichtigsten Tipps

Warn- und



BÜRGERCERT

Ins Internet - mit Sicherheit

- Startseite
- Über uns
- Fragen und Antworten
- Hilftexte
- Glossar
- Archiv
- Abonnieren
- Nutzerdaten



Sie sind hier: [Startseite](#)

Ein Projekt von



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 Projekt des Bundesamtes für Sicherheit in der Informationstechnik. Wenn auch Sie auf Nummer Sicher gehen wollen, abonnieren Sie unsere Dienste.

Aktuelle Sicherheitsinformation

10.02.2010: Im Februar 2010 schließt Microsoft mit dreizehn Sicherheitsupdates insgesamt 26 verschiedene Sicherheitslücken
Das Bürger-CERT empfiehlt die zeitnahe Installation der von Microsoft bereitgestellten Sicherheitsupdates, um die Schwachstellen zu schließen. Weitere Informationen entnehmen Sie bitte der Technischen Warnung [Bcert-2010-0013](#).

Technische Warnungen

18.02.2010
Mozilla Firefox 3.5.8 und 3.0.18: Mehrere Sicherheitslücken geschlossen
[4 mehr](#)

Newsletter "Sicher • Informiert"

18.02.2010
Diese Woche kursieren gefälschte DHL- und Google-Mails im Netz. Außerdem schließt Microsoft 26 Sicherheitslücken und Adobe veröffentlicht eine neue Version des Flash Players.
[4 mehr](#)

Extraausgabe "Sicher • Informiert"

21.01.2010
Kritische Sicherheitslücke im Internet Explorer: Sicherheitsupdate von Microsoft verfügbar
[4 mehr](#)





Bonner Unternehmertage 2010

Vielen Dank!

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

Bonn, 28. September 2010