Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheit in und für Deutschland

Isabel Münch

Bundesamt für Sicherheit in der Informationstechnik

Sicherheitsmanagement und IT-Grundschutz

Agenda

- Überblick BSI
- BSI-Lagebericht 2011
- Sicherheit ist mehr als Technik
- OWASP / IT-Grundschutz / BSI

Das BSI
eine Kurzvorstellung

- ... ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.

- Gründung 1991 per Gesetz als nationale Behörde für IT-Sicherheit.
- Jahresbudget: € 64 Mio. (2009)
- Mitarbeiter: über 500
- Standort: Bonn

Bundesamt
für Sicherheit in der
Informationstechnik

Das BSI - der zentrale Sicherheitsdienstleister des Bundes

Prävention
Informationsinfrastrukturen angemessen schützen

Reaktion
Wirkungsvoll bei IT-Sicherheitsvorfällen handeln

Nachhaltigkeit
Deutsche IT-Sicherheitskompetenz stärken - international Standards setzen

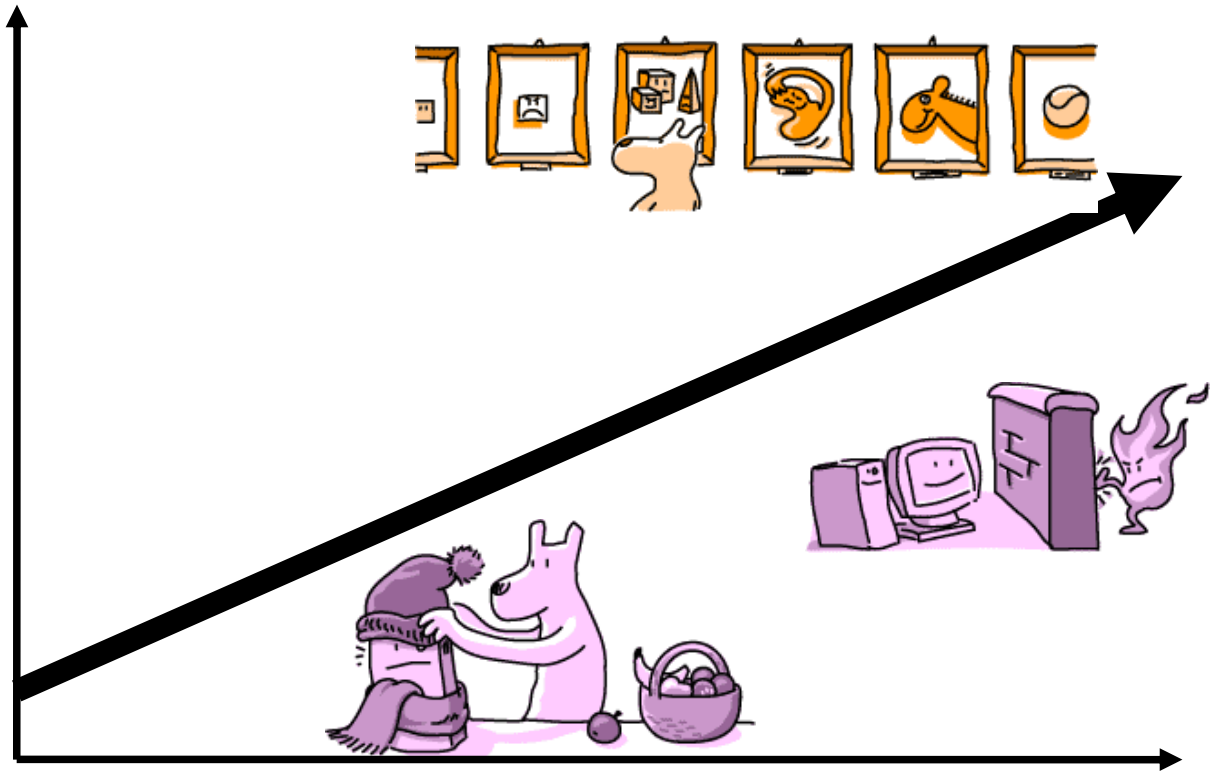
Positionierung, Kunden:

- operativ: Bundesverwaltung
- kooperativ: Wirtschaft, Wissenschaft
- informativ: Bürger

Produkt- und Dienstleistungsportfolio

Wie ist die Lage?

20 Jahre BSI



1991

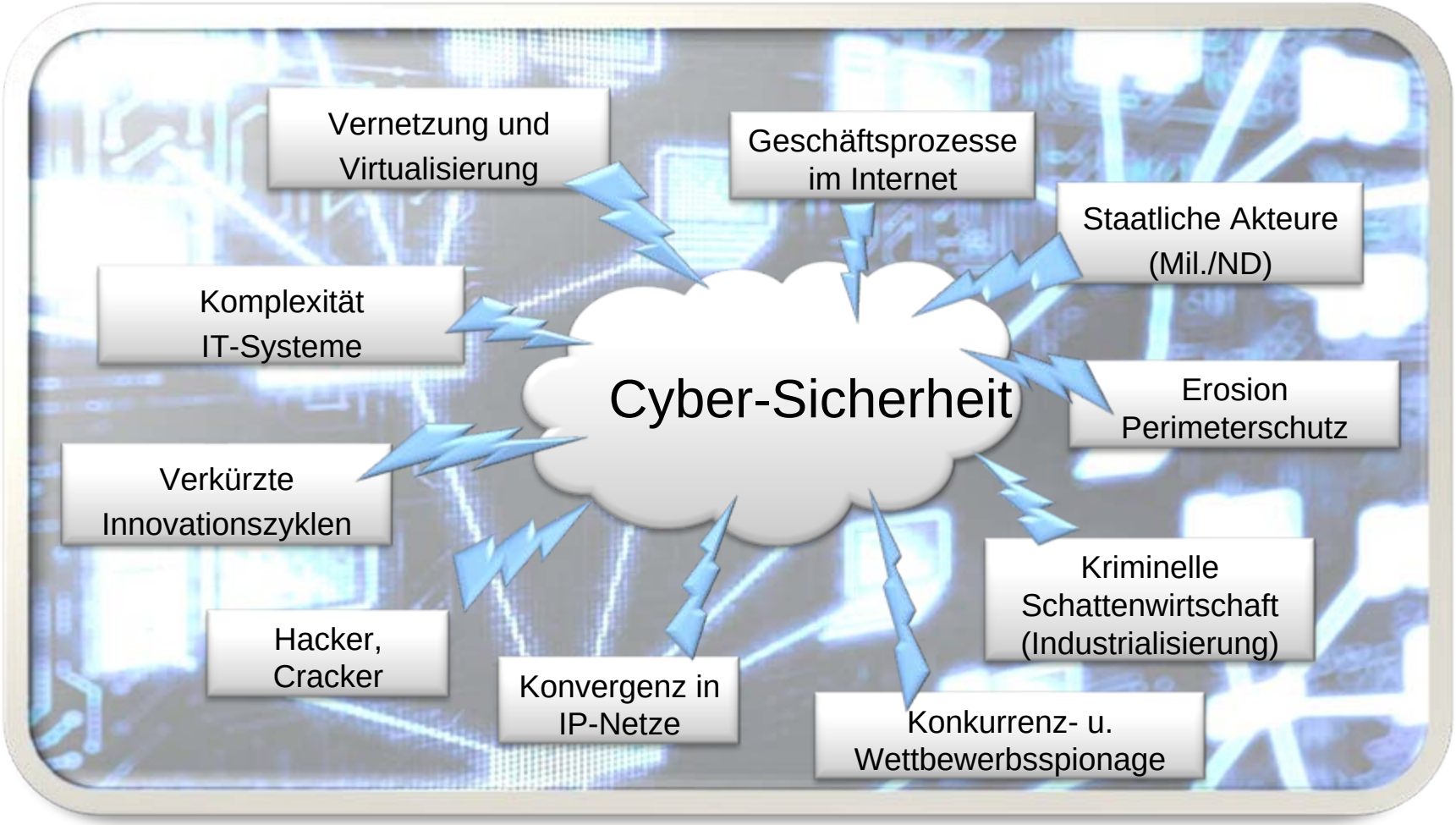
2011

- Vernetzung
- Internet-Nutzung
- Komplexität der IT
- Virtualisierung
- Cloud Computing

- Schwachstellen
- Schadsoftware
- Risiko

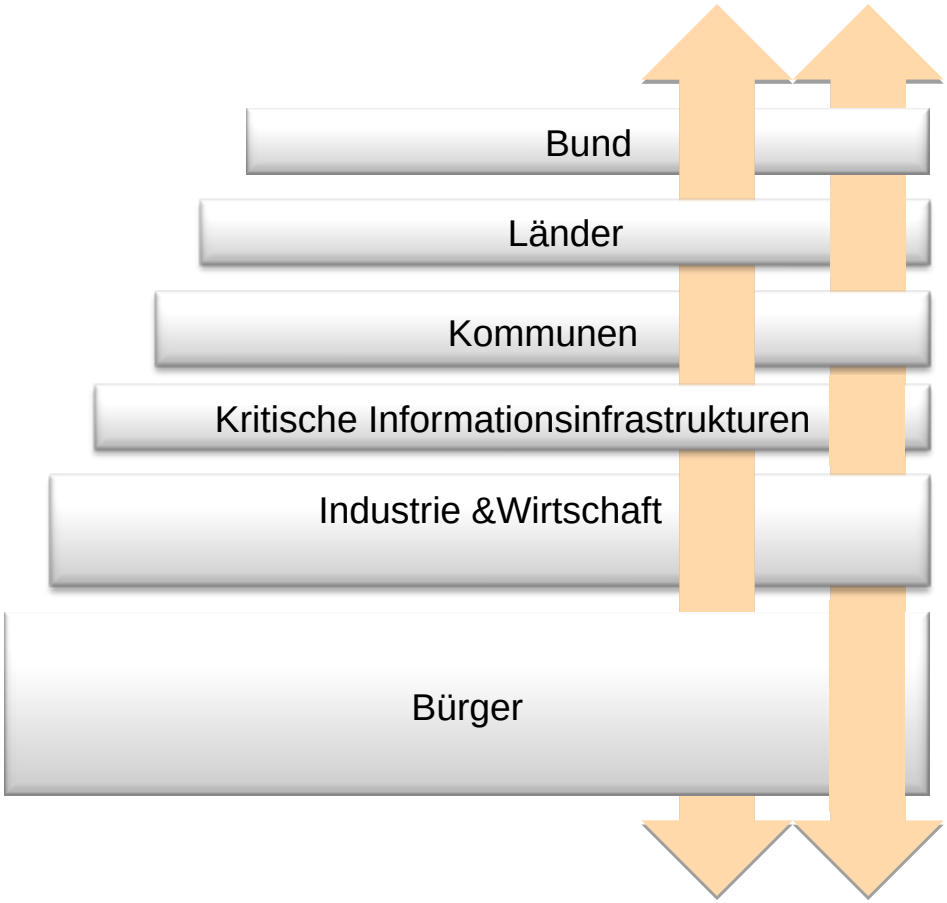
- IT-Grundschutz
  - Bedeutung
  - Umfang

Veränderung der Cyber-Sicherheitslage

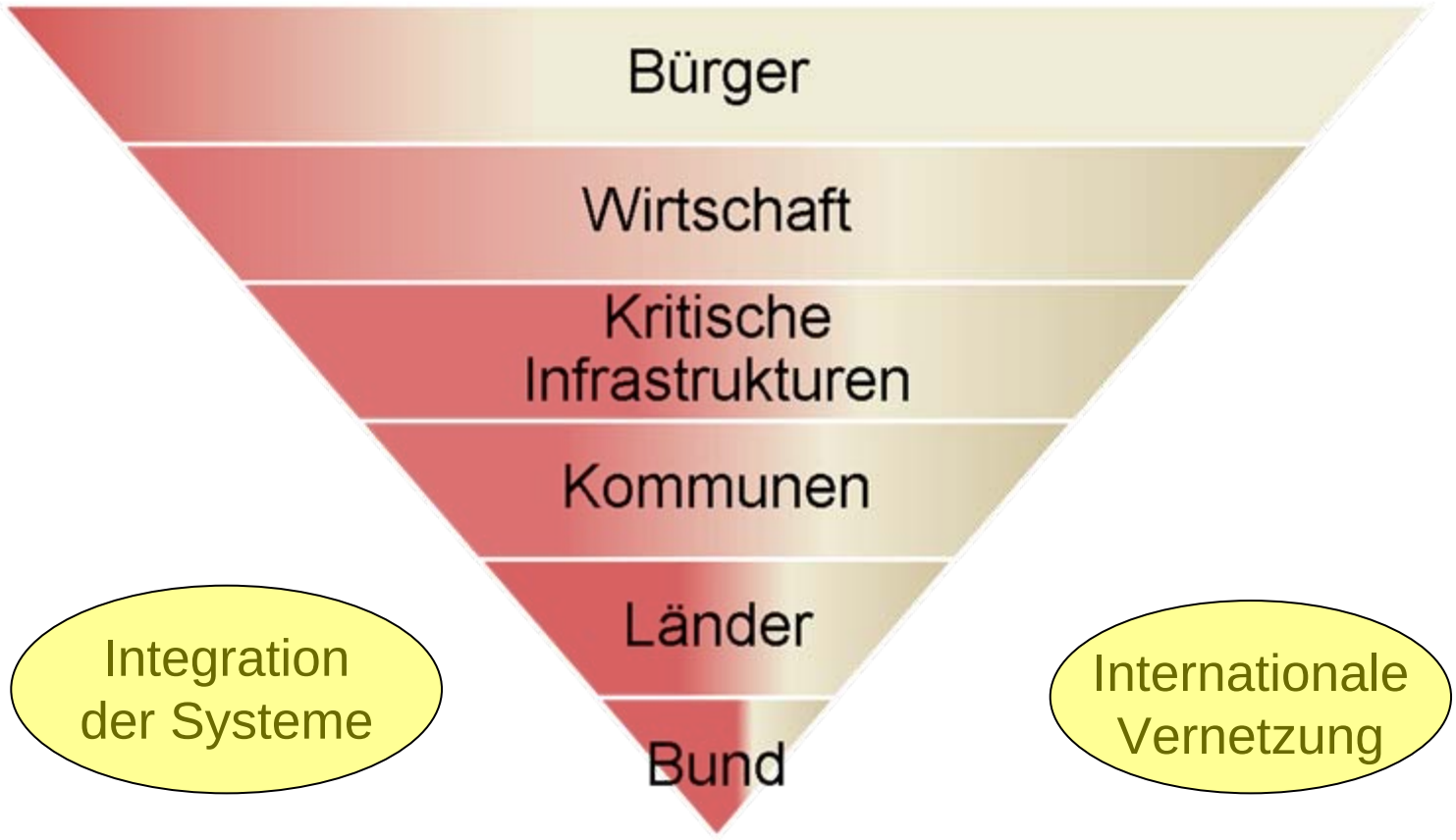


Verantwortung für Informationssicherheit

Geteilte Verantwortung, vernetztes Zusammenwirken



Verantwortung für Betrieb der IT-Systeme



BSI-Lagebericht 2011

- Risikobewußtsein vorhanden – aber zu gering
- Zunahme von Schadprogrammen, Spam-Mails, Exploits
- Gezielte Angriffe gegen Infra-strukturen, Institutionen, Personen
- Professionalisierung der Angriffe

https://www.bsi.bund.de

Was kommt auf uns zu?

Gefährdungstrends

Bedrohung	2009	2011	Prognose
DDoS-Angriffe	↑	→	→
Unerwünschte E-Mails (Spam)	↑	→	→
Botnetze	↑	↑	↑
Identitätsdiebstahl	↑	↑	↑
Sicherheitslücken	–	↑	↑
Drive-By-Exploits	–	↑	→
Schadprogramme	–	↑	↑

Quelle: BSI

Entwicklung von IT-Bedrohungen nach Einschätzung des BSI [7]

↑ steigend ↓ sinkend → gleichbleibend

Was kommt auf uns zu?

Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien

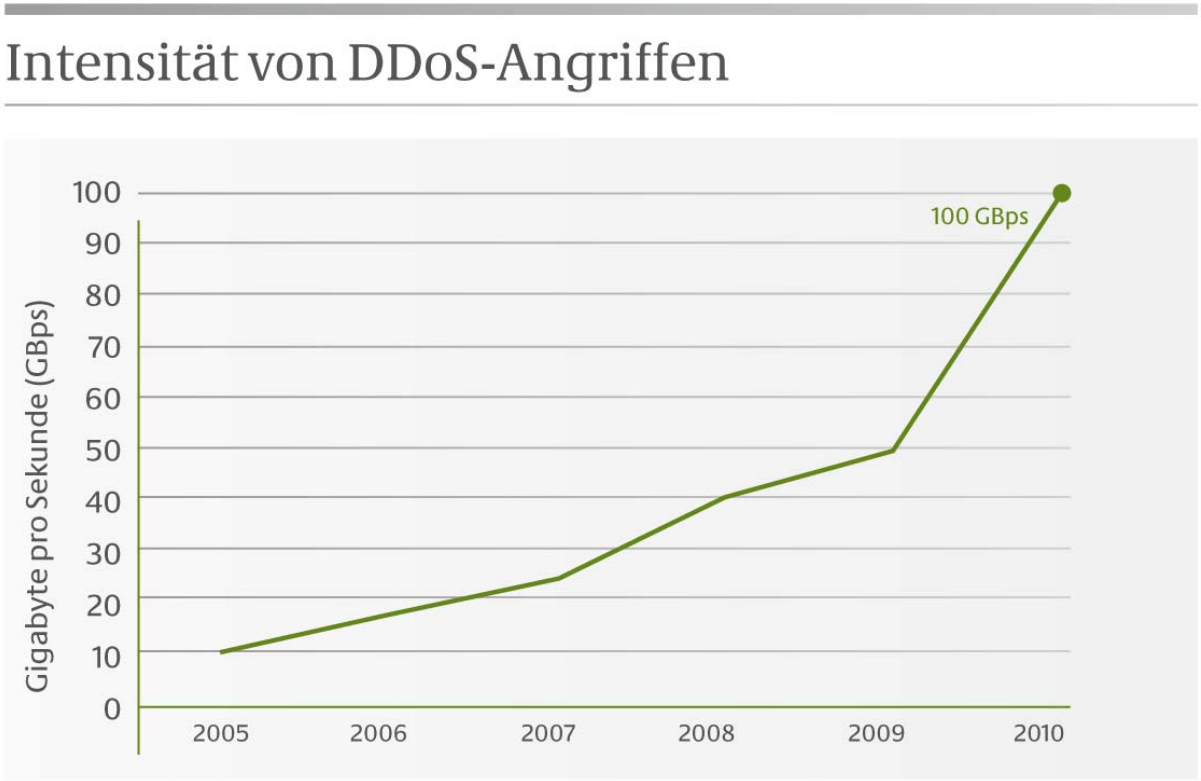
Technologie/Anwendung	2009	2011	Prognose
Mobilkommunikation	↑	↑	↑
SCADA	↑	↑	↑
DNS und BGP	↑	↑	→
Schnittstellen und Speichermedien	→	↑	↑

Quelle: BSI

Risikopotenzial für Angriffsmöglichkeiten in ausgewählten Anwendungen und Technologien nach Einschätzung des BSI [7]

↑ steigend ↓ sinkend → gleichbleibend

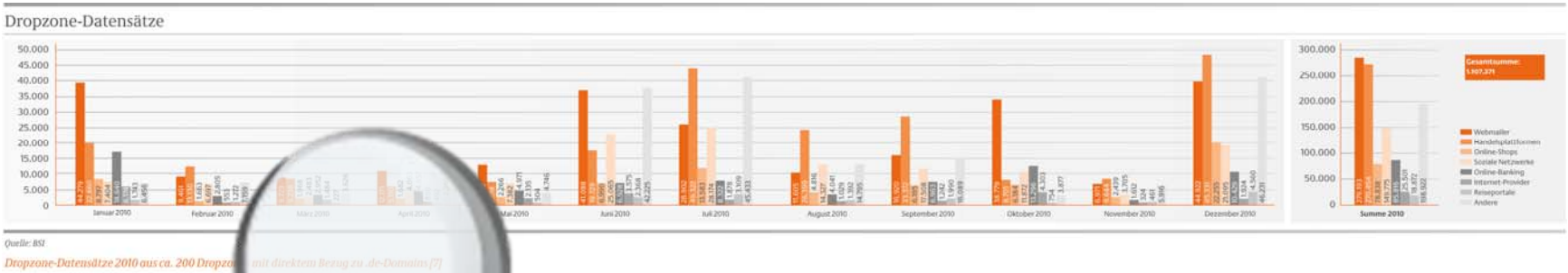
Mehr Bandbreite freut nicht nur Kunden



Quelle: Arbor Networks

Bandbreitenzuwachs bei DDos-Angriffen [9]

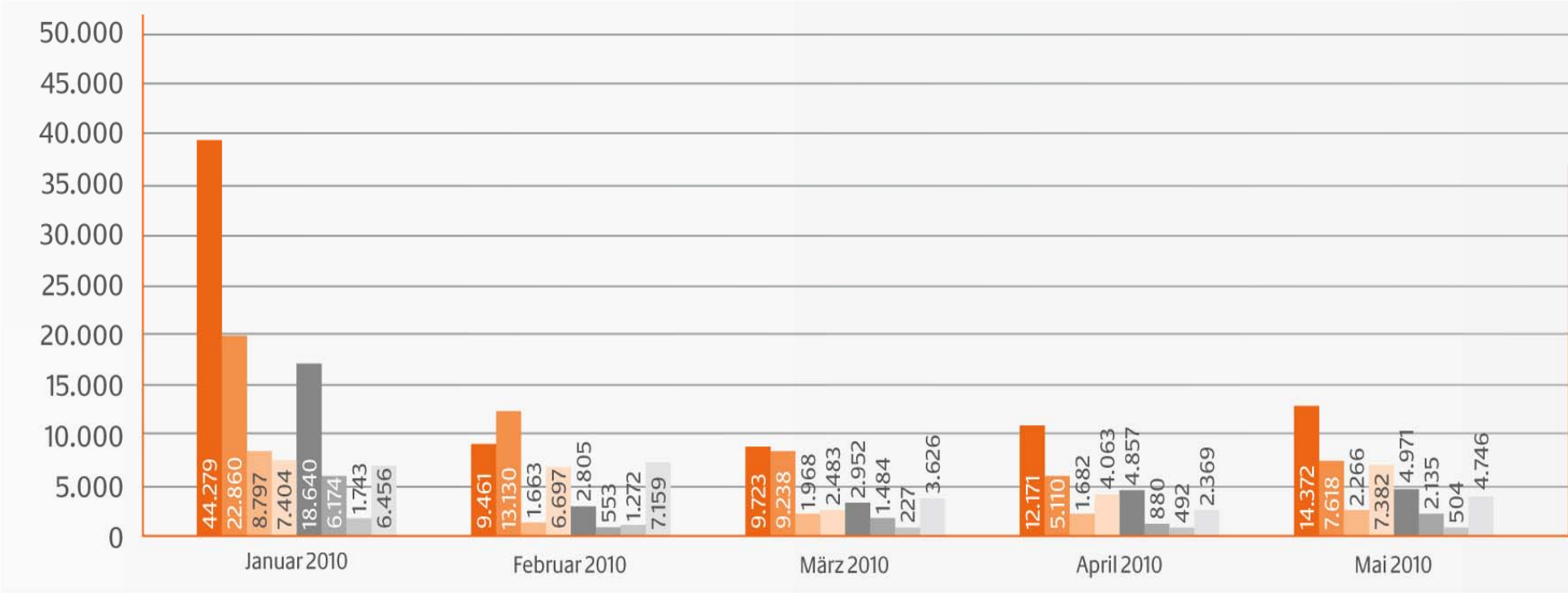
Identitätsdiebstahl und -missbrauch



- Identitätsdiebstahl und Identitätsmissbrauch haben sich als ein kriminelles Betätigungsfeld etabliert, das mit hochprofessionellen Strukturen bearbeitet wird
- Phishing ist immer weniger geworden
- Stattdessen Trojanische Pferde

Identitätsdiebstahl und -missbrauch

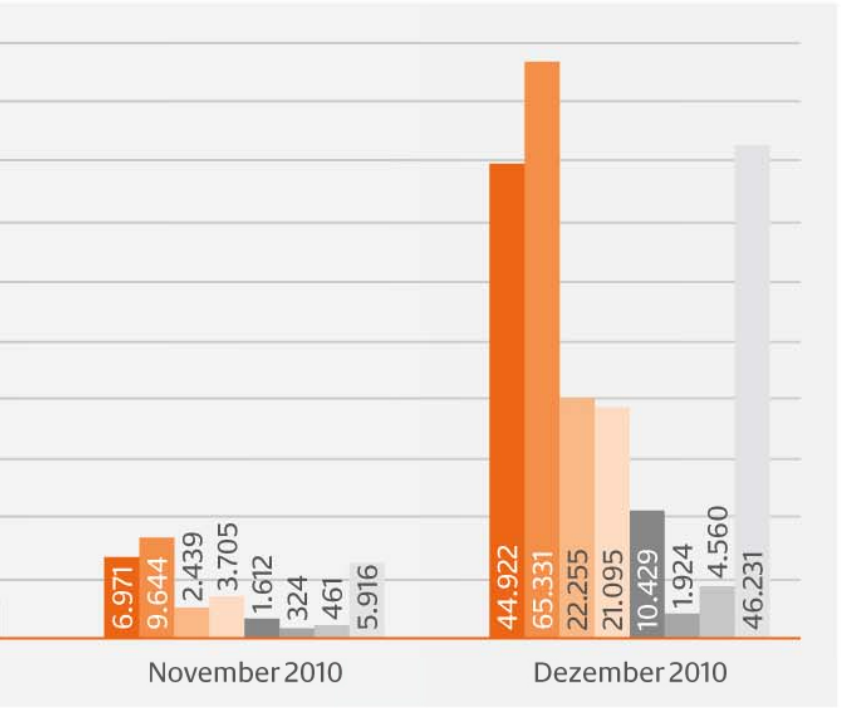
Dropzone-Datensätze

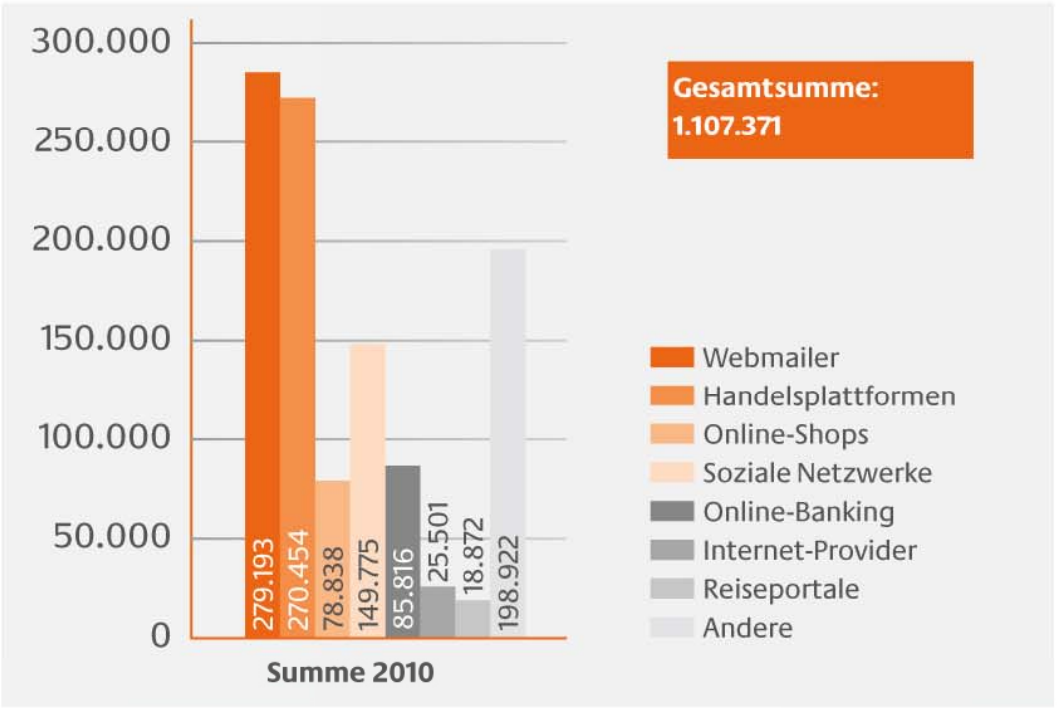


Quelle: BSI

Dropzone-Datensätze 2010 aus ca. 200 Dropzones mit direktem Bezug zu .de-Domains [7]

Identitätsdiebstahl und -missbrauch





Domain Name System

- Umsetzung von DNSSE
  Internet und bietet Schu
- Die Betreiber reagieren:
  - seit dem 15.7.2010
  - seit dem 31.5.2011
  - Domain .bund.de w
    betrieben
- Es ist daher wünschens
  ISPs die für DNSSEC e
  so die derzeit bestehen
  geschlossen wird
- Und IPSec?

Top-Level-Domains

Top-Level-Domain	Anzahl Second-Level-Domains	DNSSEC Unterstützung
.com	95.006.677	vorhanden
.de	14.369.495	vorhanden
.net	14.003.416	vorhanden
.org	9.639.660	vorhanden
.uk	9.373.754	vorhanden
.info	8.200.168	vorhanden
.nl	4.442.413	vorhanden
.cn	3.379.441 (Stand 28.02.2011)	nicht vorhanden
.eu	3.341.775	vorhanden
.biz	2.254.683	vorhanden

Quelle: BSI

Die zehn größten Top-Level-Domains [7]

Was kommt auf uns zu?

Risikoprofil innovativer Anwendungen und Technologien

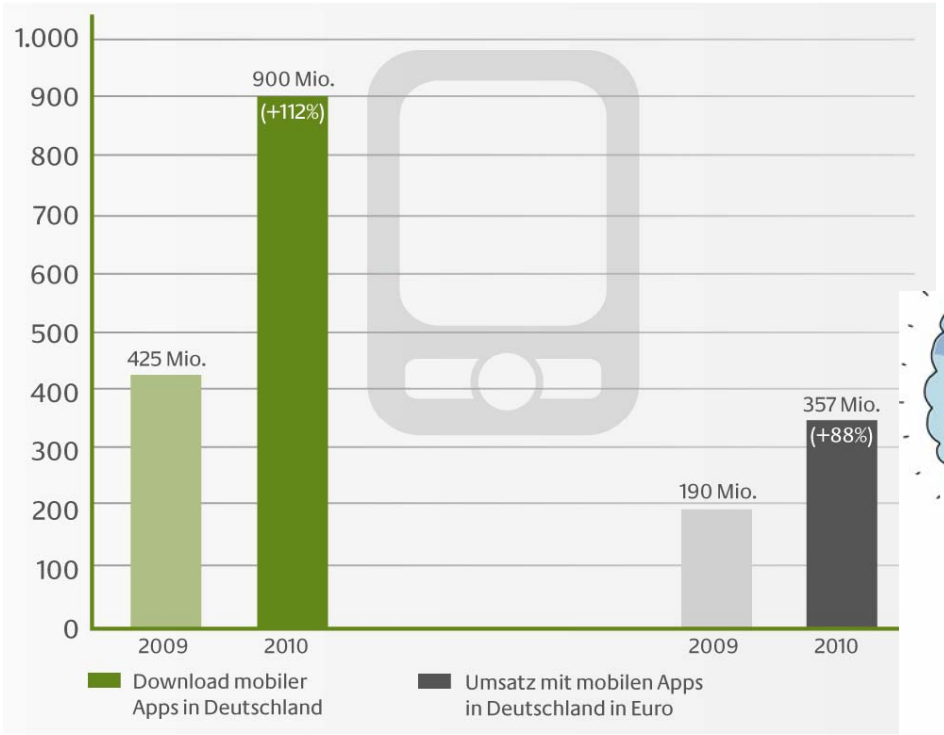
Technologie/Anwendung	2009	2011	Prognose
Cloud Computing	–	↑	↑
Smart Grid/ Smart Meter	–	↑	↑

Quelle: BSI

Risikoprofil innovativer Anwendungen und Technologien nach Einschätzung des BSI [7]

↑ steigend ↓ sinkend → gleichbleibend

Was kommt auf uns zu?

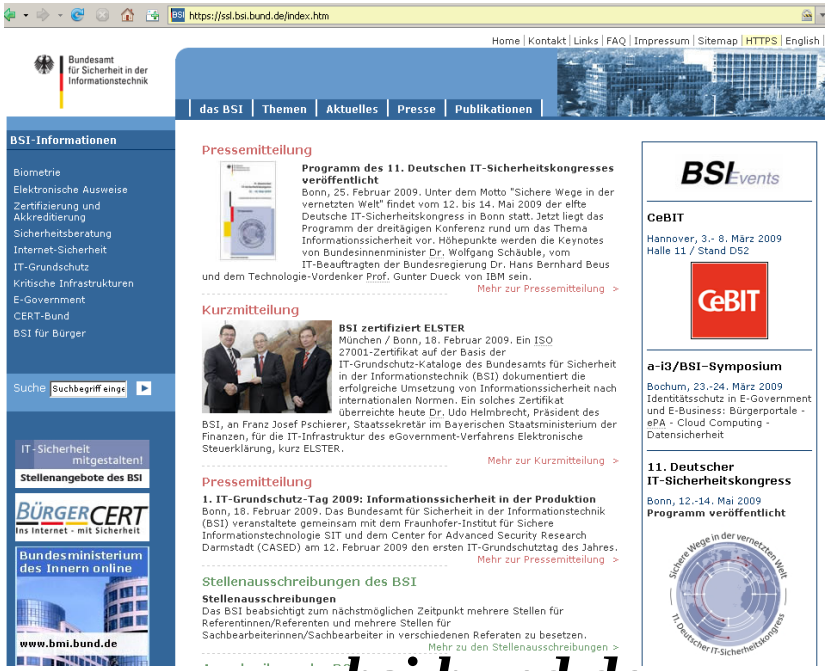


Quelle: Bitkom

Entwicklung von Download und Umsatz mobiler Applikationen für Smartphones in Deutschland [6]

BSI-Angebote

- Vielzahl von Informationen zur Informationssicherheit
  - Technische Richtlininen
  - Schriften zur Internet-Sicherheit
  - Hochverfügbarkeit
- IT-Grundschutz
- Zertifizierung
- Für Behörden: Beratung
  und weitere Serviceleistungen



www.bsi.bund.de

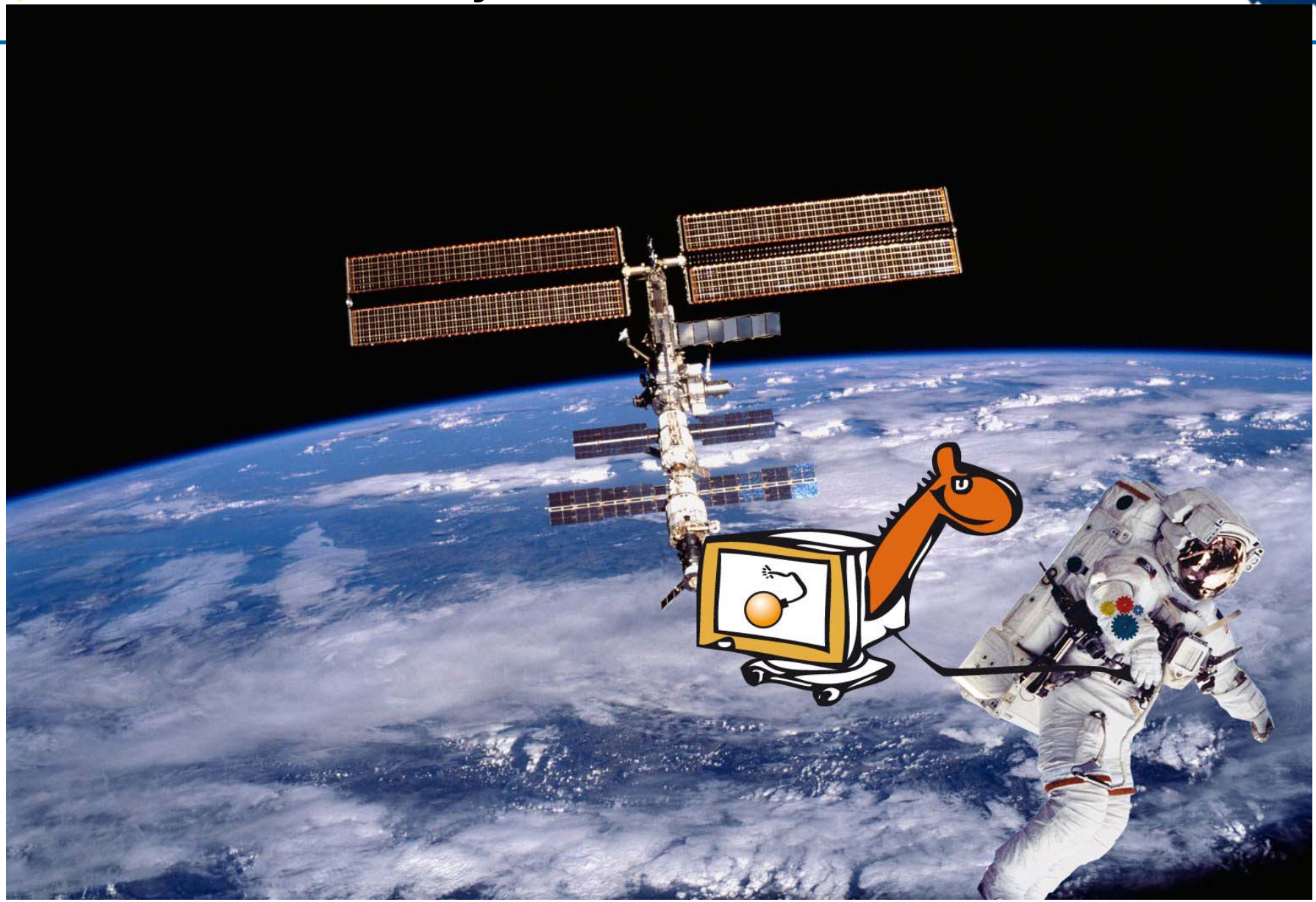
Nichts ist unmöglich!

- BSI bearbeitet viele, viele Felder!
- Daher viele Gigabyte Informationen
- Auch IT-Grundschutz-Kataloge werden immer umfangreicher
- **Aber:**

  Auch unsere esoterischsten Überlegungen wurden wahr!

Bundesamt
für Sicherheit in der
Informationstechnik

Trojaner im Weltall



Bundesamt
für Sicherheit in der
Informationstechnik

Trojaner im Weltall

Heise-Meldung vom 27.08.08

heise Security

Statt "Schweine im Weltall" gibts nun "Malware im Weltall". US-Medienberichten zufolge waren **mehrere Laptops auf der bemannten internationalen Raumstation ISS mit dem Schädling W32.Gammima.AG infiziert**, der Login-Daten für Online-Spiele ausspäht und per HTTP verschickt. Gammima verbreitete sich vermutlich über USB-Sticks oder Flash-Karten innerhalb der Raumstation. Wie er allerdings in die Raumstation hineingelangte, ist noch unklar. Vermutlich wurde er mit einem bereits infizierten Laptop eingeschleppt, da die Raumstation keinen direkten Internetzugang hat. Unklar ist auch, welche Nation für die initiale Infektion verantwortlich ist.

Nach Angaben der Webseite Spaceref.com, die als erste über den Vorfall berichtete, **weisen einige der eingesetzten Laptops auf der ISS keinen Virenschutz auf**. Allerdings gibt es offenbar regelmäßige Checks von Systemrechnern, wofür laut der ISS-Logeinträge wohl Norton Antivirus eingesetzt wird.

Gegenüber dem Magazin Wired sagte eine Sprecher der NASA, dass der Wurm kein Problem für den Betrieb der Raumstation darstelle. Er habe nur Laptops befallen, die für E-Mail und Ernährungsexperimente benutzt würden. **Zudem sei es nicht das erste Mal, dass auf der ISS ein Schädling aufgetaucht sei.**

Hackerangriff auf Kaffeemaschine möglich

Hackerangriff auf Kaffeemaschine möglich

- Heise News vom 18.06.2008: australischer Sicherheitsspezialist wies auf Sicherheitslücken des Internet Connection Kit des Kaffeemaschinenherstellers Jura hin
- Hacker könnten Ihnen über das Internet in der Kaffeemaschine die Einstellungen zur Zubereitung ändern!
- Wenig Pulver mit viel Wasser käme dabei wohl für viele Kaffeetrinker sicherlich einer Denial-of-Service-Attacke gleich.

Ohne die Menschen geht es nicht!

Gadgets and Gizmos

- Bedürfnis nach kleinen Freiheiten
- Praktisch?
- Sinnvoll?
- Und die Sicherheit?

Gadgets und Consumerization

- Klare Spielregeln nötig!
- Über USB-Devices, Web-Dienste, Applikationen können auch Trojanische Pferde verteilt werden!
- Nicht nur USB-Weihnachtsbäume, sondern auch Skype oder iPads
- Web 2.0: Was machen die Mitarbeiter in Facebook, Google+ etc.?
- Vernünftige Balance zwischen Restriktion und Freiheit nötig!

Was kann man tun?

- Kontrolle?
- Verbote?
- Technische Mittel?
  - Schnittstellen entfernen oder deaktivieren, z.B. Ports sperren -> Effektivität der IT-Infrastruktur leidet
  - Spezielle Sicherheitsprodukte, z.B. DeviceWall, DLP
- **Awareness!**
- ⇨ Thema aufgreifen
- ⇨ Konzept für Umgang mit Technikspielzeug etc.
- ⇨ Passende Sicherheitsrichtlinien

Einsatz von technischen Sicherheitslösungen

- Firewalls
- Virenschutz
- Intrusion Detection
- Intrusion Prevention
- ...

Aber...

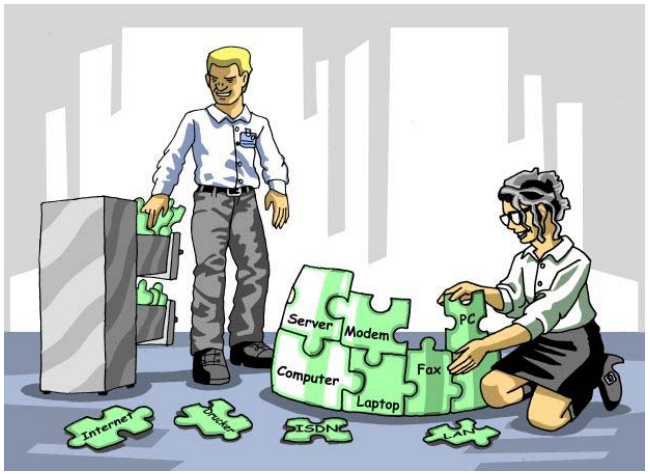
- Wird die einwandfreie Funktion der Geschäftsprozesse gewährleistet?
- Kommen vielleicht trotzdem Unbefugte an kritischen Informationen?
- Wurden die Investitionen an richtiger Stelle getätigt und sind sie angemessen?

Sicherheit ist...

- **Sicherheit ist kein Produkt**
  - Sicherheit kann man nicht kaufen, Sicherheit muss man schaffen!
  - Natürlich muss man zum Schaffen von Sicherheit auch auf vorhandene Produkte zurückgreifen.
- **Sicherheit ist kein Projekt**
  - Es genügt nicht, Sicherheit einmal zu schaffen, sondern Sicherheit muss aufrechterhalten werden!
  - Natürlich kann man Aufbau und Aufrechterhaltung von Sicherheit auch teilweise in Projekten abwickeln.
- **Sicherheit ist ein Prozess**
- **Sicherheit ist Chefsache**

Sicherheitsmanagement mit IT-Grundschutz

IT-Grundschutz
Die Idee ...



- Typische Komponenten
- Typische Gefährdungen, Schwachstellen und Risiken
- Konkrete Umsetzungshinweise für das Sicherheitsmanagement
- Empfehlung geeigneter Bündel von Standard-Sicherheitsmaßnahmen
- Vorbildliche Lösungen aus der Praxis - „Best Practice“-Ansätze

Ziel des IT-Grundschutzes

IT-Grundschutz verfolgt einen ganzheitlichen Ansatz. Infrastrukturelle, organisatorische, personelle und technische **Standard-Sicherheitsmaßnahmen** helfen, ein

Standard-Sicherheitsniveau

aufzubauen, um geschäftsrelevante Informationen zu schützen.
An vielen Stellen werden bereits höherwertige Maßnahmen geliefert, die die Basis für sensiblere Bereiche sind.

Dienstleistungen und Produkte rund um den IT-Grundschutz

Sicherheitsbedarf, Anspruch

\- / o / +

Leitfaden Informationssicherheit

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: Risiko-Analyse**	**IT-Grundschutz-Kataloge**
Leitfaden IS-Revision	**BSI Standard 100-4: Notfall-management**	**BSI-Empfehlungen: - Internetsicherheit - Hochverfügbarkeit**

OWASP und IT-Grundschutz

Viele Gemeinsamkeiten:

- Große Informationsmengen
- Wachsen an vielen Enden
- Schwierige Wartbarkeit
- Creative Commons

- Baustein Web-Anwendungen -> basiert auf OWASP-Empfehlungen

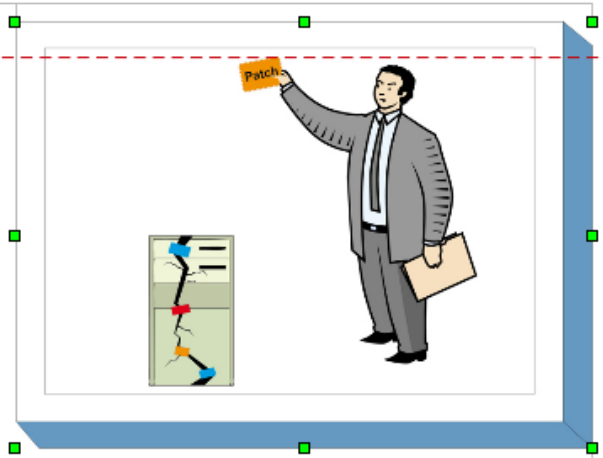
OWASP und IT-Grundschutz

IT-Grundschutz-Kataloge:

- In Planung:
- Baustein Web-Anwendungen
- basiert auf OWASP-Empfehlungen
- Zeitplan:
  - Derzeit interne QS
  - Q1 2012 externe QS
  - Veröffentlichung 13. EL

Baustein Web-Anwendung

B·X.XX→Web-Anwendung¶



Beschreibung¶

Web-Anwendungen·stellen·Funktionen·und·dynamische·Inhalte über·das·Internetprotokoll·HTTP·(*Hypertext·Transfer·Protocol*) zur·Verfügung.·Dazu·werden·auf·einem·Server·Dokumente·und Benutzeroberflächen · (z.·B. · Bedienelemente · und Eingabemasken)·erzeugt·und·in·Form·von·HTML-Seiten·an entsprechende·Clientprogramme·(Web-Browser)·ausgeliefert. Die·HTML-Seiten·werden·dabei·häufig·um·aktive·Inhalte·wie Javascript-Code·und·Flash-Objekte·erweitert.¶

Eine · Web-Anwendung · setzt · sich · aus · mehreren · IT-Systemkomponenten·zusammen·und·besteht·üblicherweise·aus·einem·Webserver·zur·Auslieferung·der Daten,·einem·Applikationsserver·für·den·Betrieb·der·Anwendung·und·zusätzlichen·Hintergrundsystemen,·die als · Datenquellen · über · unterschiedliche · Schnittstellen · angebunden · sind · (z.·B. · Datenbank · oder Verzeichnisdienst).·¶

Web-Anwendungen · werden · sowohl · in · öffentlichen · Netzwerken · (z.·B. · dem · Internet) · als · auch · in Firmennetzen·zur·Bereitstellung·von·Daten·und·Anwendungen·eingesetzt.·Dabei·müssen·Web-Anwendungen Sicherheitsmechanismen · umsetzen, · die · den · Schutz · der · Daten · gewährleisten · und · einen · Missbrauch verhindern.¶

Typische·Sicherheitskomponenten·einer·Web-Anwendung·sind:¶

– → Authentisierung¶

  Für·den·Zugriff·auf·geschützte·Ressourcen·der·Web-Anwendung·muss·sich·der·Benutzer·ausweisen (z.·B.·durch·Zugangsdaten).¶

Das v
noch
der V
Stepha
22.09.

Diese
hier e
Baust
bis zu
Gefäh
zu an
lang is
Peter K
21.09.

Antwo
(21.09

Wir w
Aufzä
hier k

Baustein Web-Anwendung

Gefährdungslage¶

Für den IT-Grundschutz werden pauschal die folgenden Gefährdungen als typisch im Zusammenhang mit einer Web-Anwendung angenommen:¶

Organisatorische Mängel¶

- G 2.1 → Fehlende oder unzureichende Regelungen¶
- G 2.4 → Unzureichende Kontrolle der Sicherheitsmaßnahmen¶
- G 2.7 → Unerlaubte Ausübung von Rechten ¶
- G 2.22 → Fehlende Auswertung von Protokolldaten¶
- G 2.27 → Fehlende oder unzureichende Dokumentation ¶
- G 2.67 → Ungeeignete Verwaltung von Zugangs- und Zugriffsrechten¶
- G 2.87 → Verwendung unsicherer Protokolle in öffentlichen Netzen¶
- G 2.103 → Unzureichende Schulung der Mitarbeiter¶
- G 2.WA01 → Mangelhafte Auswahl oder Konzeption von Web-Anwendungen¶
- G 2.WA02 → Mängel bei der Entwicklung und der Erweiterung von Web-Anwendungen¶
- G 2.WA03 → Unzureichender Schutz personenbezogener Daten bei Web-Anwendungen¶

Menschliche Fehlhandlungen¶

- G 3.16 → Fehlerhafte Administration von Zugangs- und Zugriffsrechten¶
- G 3.38 → Konfigurations- und Bedienungsfehler¶
- G 3.43 → Ungeeigneter Umgang mit Passwörtern¶

Technisches Versagen¶

- G 4.22 → Software-Schwachstellen oder -Fehler¶
- G 4.33 → ~~Schlechte oder fehlende Authentikation~~ Unzureichende oder fehlende Authentisierung¶
- G 4.35 → Unsichere kryptographische Algorithmen¶
- G 4.WA03 → Unzureichende Validierung von Ein- und Ausgabedaten bei Web-Anwendungen¶
- G 4.WA05 → Fehlende oder mangelhafte Fehlerbehandlung durch Web-Anwendungen¶
- G 4.WA06 → Unzureichende Nachvollziehbarkeit von sicherheitsrelevanten Ereignissen bei Web-Anwendungen¶

Baustein Web-Anwendung

Vorsätzliche Handlungen

- G 5.18 → Systematisches Ausprobieren von Passwörtern
- G 5.19 → Missbrauch von Benutzerrechten
- G 5.20 → Missbrauch von Administratorrechten
- G 5.28 → Verhinderung von Diensten
- G 5.87 → Web-Spoofing
- G 5.131 → SQL-Injection
- G 5.WA01 → Unberechtigter Zugriff auf oder Manipulation von Daten bei Web-Anwendungen
- G 5.WA03a → Automation einer Web-Anwendung
- G 5.WA03b → Fehler in der Web-Anwendungslogik
- G 5.WA04 → Umgehung clientseitig umgesetzter Sicherheitsfunktionen einer Web-Anwendung
- G 5.WA05 → Unzureichendes Session-Management
- G 5.WA06 → Cross-Site Scripting (XSS)
- G 5.WA07 → Cross-Site Request Forgery (CSRF, XSRF)
- G 5.WA08 → Umgehung der Autorisierung bei Web-Anwendungen
- G 5.WA09 → Einbindung von fremden Daten und Schadcode bei Web-Anwendungen
- G 5.WA10 → Injection-Angriffe
- G 5.WA11 → Clickjacking

Baustein Web-Anwendung

Maßnahmenempfehlungen¶

Um eine Web-Anwendung abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.¶

Der Betrieb einer Web-Anwendung setzt den Einsatz weiterer Komponenten voraus. Daher muss der Baustein B 3.1 *Allgemeiner Server* und abhängig von dem eingesetzten Betriebssystem beispielsweise Baustein B 3.2 *Server unter Unix* oder B 3.8 *Windows Server 2003* berücksichtigt werden. Darüber hinaus wird für den Betrieb einer Web-Anwendung ein Webserver (siehe B 5.4 *Webserver*) benötigt.¶

Funktionalität oder Daten werden bei Web-Anwendungen gewöhnlich in Hintergrundsystemen ausgelagert (z. B. Datenbank und Identitätsspeicher). Aus diesem Grund sind in Abhängigkeit der eingesetzten Hintergrundsysteme weitere Bausteine, wie beispielsweise B 5.7 *Datenbanken* und B 5.15 *Allgemeiner Verzeichnisdienst* (bzw. B 5.16 *Active Directory*), zu berücksichtigen.¶

Baustein Web-Anwendung

Planung und Konzeption

Bei der Planung einer Web-Anwendung muss üblicherweise entschieden werden, ob die Anforderungen an die Web-Anwendung durch Standardprodukte abgedeckt werden können oder eine Eigenentwicklung notwendig ist. Wird eine Web-Anwendung auf Basis von Standardsoftware umgesetzt, so sind gewöhnlich Anpassungen erforderlich, die neben Konfigurationsänderungen hinausgehen und oft auch Entwicklungsarbeiten mit einschließen. Daher müssen bei Web-Anwendungen, welche auf Standardsoftware basieren, häufig auch Vorgaben an die Entwicklung und Erweiterung definiert werden (siehe M 2.WA12 *Entwicklung und Erweiterung der Web-Anwendung*).

Bereits in der Entwurfsphase einer Web-Anwendung müssen Sicherheitsaspekte beachtet werden, um die zu verarbeitenden Daten zu schützen (siehe M 5.WA23 *Systemarchitektur für eine Web-Anwendung*). Hierbei muss auch die Integration und sichere Anbindung von IT-Systemkomponenten miteinbezogen werden (siehe M 5.WA21 *Anbindung der Hintergrundsysteme an die Web*-Anwendung).

Hier noch M 2.WA02 Dokumentation der Architektur einer Web-Anwendung einfügen.

Werden personenbezogene Daten von Web-Anwendungen verarbeitet oder aufgezeichnet und ausgewertet (z. B. Nutzerverhalten), sind rechtliche Rahmenbedingungen bei der Planung von technischen Lösungen zu berücksichtigen (siehe M 2.110 *Datenschutzaspekte bei der Protokollierung* und M 2.WA24 *Web-Tracking*).

Baustein Web-Anwendung

Umsetzung

→	M 2.62	(A)	Software-Abnahme- und Freigabe-Verfahren
→	M 2.363	(A)	Schutz gegen SQL-Injection
→	M 3.5	(B)	Schulung zu Sicherheitsmaßnahmen
→	M 4.WA04	(A)	Authentisierung bei Web-Anwendungen
→	M 4.WA05	(A)	Umfassende Ein- und Ausgabevalidierung
→	M 4.WA06	(A)	Session-Management bei Web-Anwendungen
→	M 4.WA07	(A)	Fehlerbehandlung durch Web-Anwendungen
→	M 4.WA08	(B)	Verhinderung von Automation (Brute-Force und Enumeration)
→	M 4.WA11	(A)	Sichere Konfiguration einer Web-Anwendung
→	M 4.WA13	(A)	Kontrolliertes Einbinden von Daten und Inhalten bei Web-Anwendungen
→	M 4.WA15	(A)	Schutz vertraulicher Daten bei Web-Anwendungen
→	M 4.WA16	(A)	Zugriffskontrolle bei Web-Anwendungen
→	M 4.WA19	(B)	Verhinderung von Cross-Site Request Forgery (CSRF, XSRF)
→	M 4.WA20	(A)	Sicherer Entwurf der Web-Anwendungslogik
→	M 4.WA22	(B)	Verhinderung der Blockade von Ressourcen (DoS) bei Web-Anwendungen
→	M 4.WA25	(B)	Verhinderung von Clickjacking

OWASP und BSI

- BSI begrüsst OWASP-Aktivitäten
- Gerne engere Kooperation
- Zukünftig Mitarbeit des BSI in OWASP-Projekten
- Geplant: BSI-Projekt "Vorgaben und Vorgehensweise zur Entwicklung sicherer Webanwendungen"
  - Ziele: Entwicklung eines Secure Development Lifecycle (SDL) für die Bundesverwaltung
  - Dieser SDL soll eine systematische und greifbare Anwendbarkeit von existierenden Publikationen des BSI sowie von OWASP ermöglichen und fehlende Aspekte (Schwerpunkt: Sourcecodeanalyse) ergänzen. Darüber hinaus werden Leitfäden / Checklisten zur Prüfung der Einhaltung dieser Vorgaben entwickelt.

Vielen Dank
für Ihre Aufmerksamkeit

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

IT-Grundschutz
Godesberger Allee 195-198
53175 Bonn

Tel: +49 (0)22899-9582-5369
Fax: +49 (0)22899-9582-5405

grundschutz@bsi.bund.de
www.bsi.bund.de/grundschutz

IT-Grundschutz Gruppe im XING-Forum:
https://www.xing.com/net/itgrundschutz