Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz – Informationssicherheit ohne Risiken und Nebenwirkungen

Isabel Münch

Bundesamt für Sicherheit in der Informationstechnik
Sicherheitsmanagement und IT-Grundschutz

IT-Grundschutz-Tag

13.06.2012

Inhalte

- Überblick BSI
- Kleine und große Gefährdungen
- IT-Grundschutz - der Weg zum Standard
- IT-Grundschutz und Entwicklungen darum herum

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

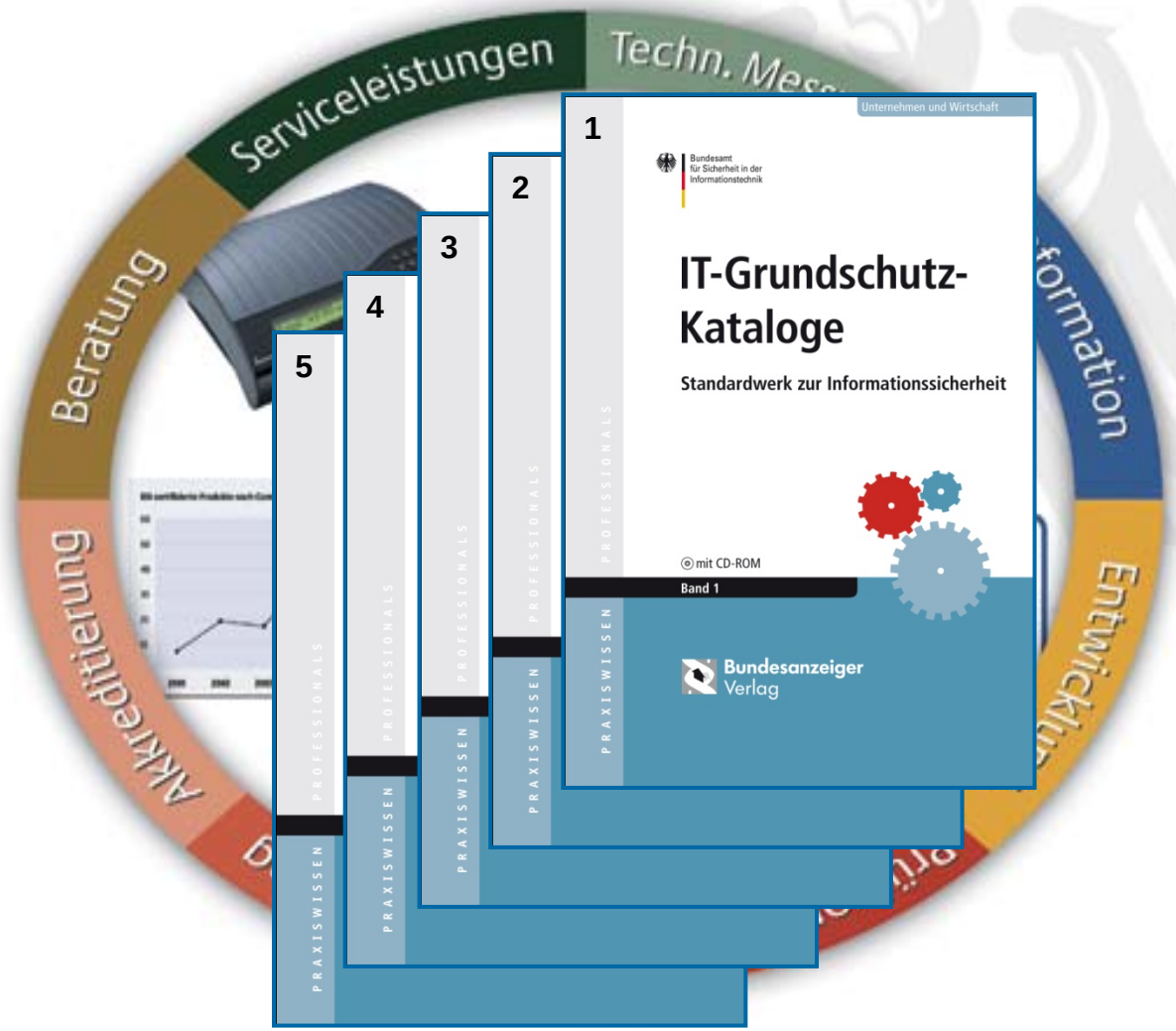
Reaktion
Wirkungsvoll bei IT-Sicherheitsvorfällen handeln

Nachhaltigkeit
Deutsche IT-Sicherheitskompetenz stärken - international Standards setzen

Positionierung, Kunden:

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

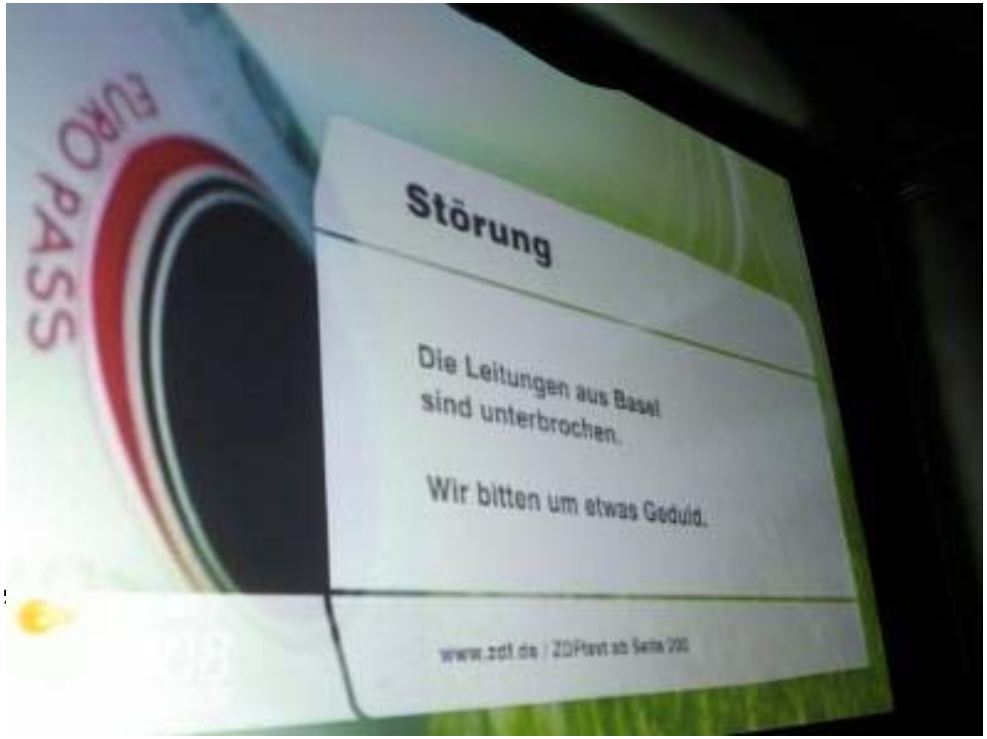
Produkt- und Dienstleistungsportfolio



Große Gefährdungen und kleine…

Fehlendes Notfallmanagement

- EM-Halbfinale am 25.6.08
- Deutschland-Türkei
- Spiel in Basel
- Gewitter über Wien
- "Mikroausfälle" von Sekundenkürze haben das Computersystem veranlasst, komplett neu zu starten.
- Die für die UEFA tätige Firma hatte offensichtlich keine Notfall-Lösung parat



Bedürfnis nach kleinen Freiheiten

- Mobile externe Speichermedien wie USB-Sticks, PDAs und Musikplayer
- Digitale Fotorahmen
- Toys and Gadgets

Bedürfnis nach Technik-Spielzeug

- http://www.pileus.net/
- „Pileus Umbrella“ (aus Japan)
  - Internet-fähig
  - GPS, digitaler Kompass, Navi
  - kann mit einer eingebauten Kamera Aufnahmen machen, diese via WLAN direkt bei Flickr hochladen und bringt sogar ein futuristisches Display mit
  - vom Regenschutz zur mobilen Projektionsfläche.

Technik-Spielzeug

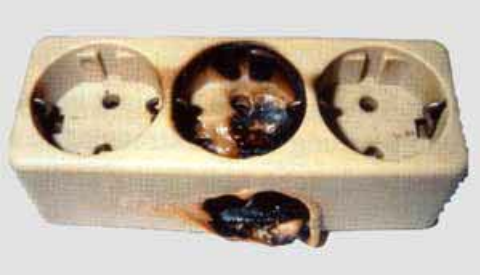
- "James-Bond-Kuli" kann schreiben und obendrein per versteckter Kamera vertonte Videos auf den internen Speicher bannen
- Oder: "Spionage" Feuerzeuge, Schlüsselanhänger, Armbanduhren, etc. ... Fotografieren, Filmen, Tonaufnahme, USB, Micro SD

Technik-Spielzeug

- Aus der Werbung: "Diese Alarmuhr in Form einer Bombe müssen Sie jeden Tag neu entschärfen. Um das laute Alarmgeräusch (Explosion) zu stoppen, müssen sie die richtige Strippe ziehen. Lässt sich auch als Wecker verwenden. Der Code wird jeden Tag automatisch neu generiert."

Bekanntes Problem

- Auch bei USB-Gadgets!



Unterhaltungselektronik im Büro

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

Was kann man tun?

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

Situation in der Praxis

Einsatz von technischen Sicherheitslösungen

- Firewalls
- Virenschutzprogramme
- Intrusion-Detection-Systeme
- Spam-Filter
- ...

Aber...

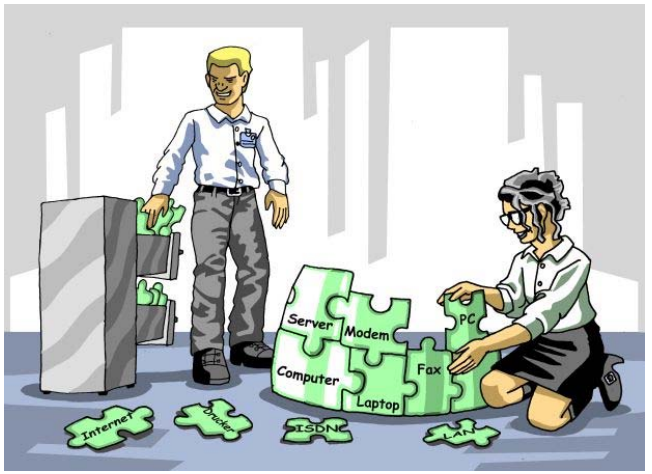
- Sind diese in Einklang mit den Geschäftsprozesse gebracht?
- Werden auch nicht-technische Aspekte berücksichtigt?
- Wurden die Investitionen an richtiger Stelle getätigt und sind sie angemessen?

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

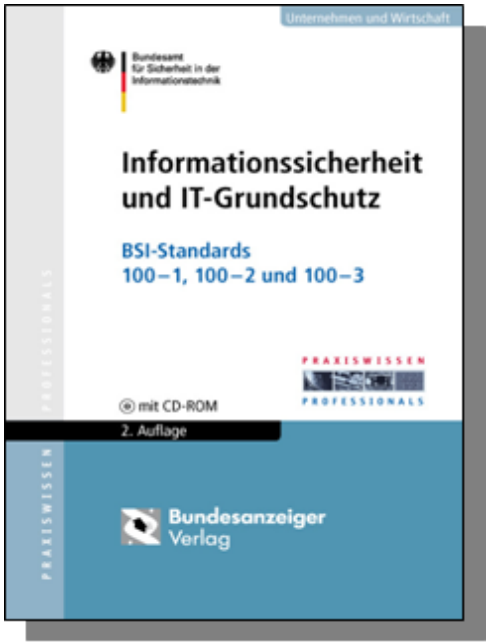
IT-Grundschutz verfolgt einen ganzheitlichen Ansatz. Infrastrukturelle, organisatorische, personelle und technische **Standard-Sicherheitsmaßnahmen** helfen, ein

Standard-Sicherheitsniveau

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

IT-Grundschutz

seit 2005

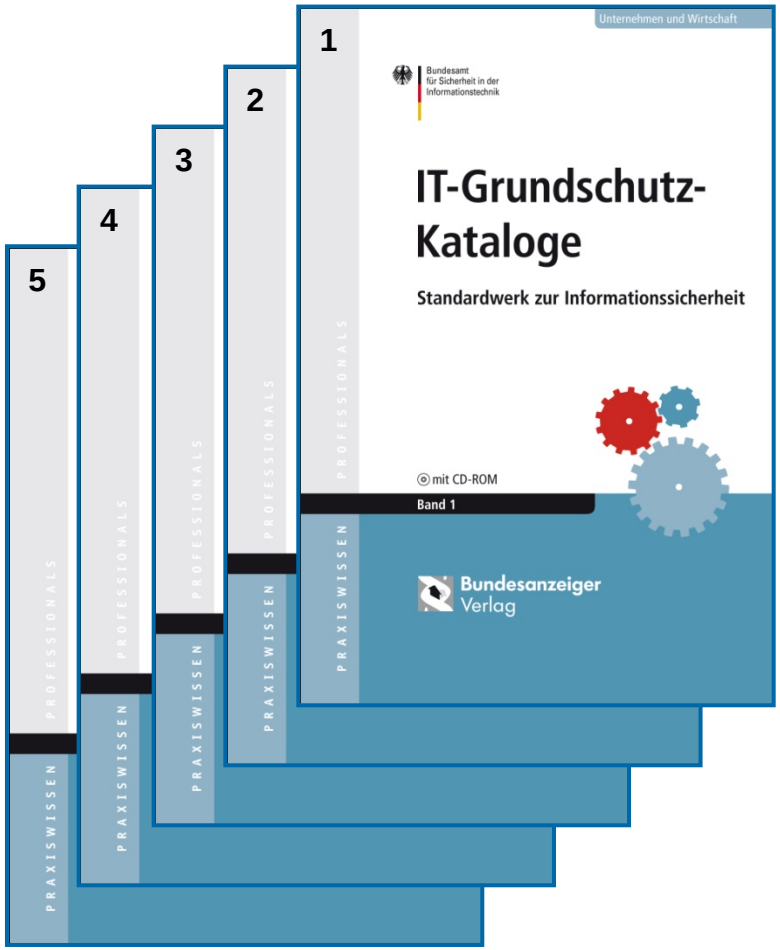


BSI-Standards + Loseblattsammlung

IT-Grundschutz
BSI-Standards

- **BSI-Standard 100-1:**
  Managementsysteme für Informationssicherheit
- **BSI-Standard 100-2:**
  IT-Grundschutz-Vorgehensweise
- **BSI-Standard 100-3:**
  Risikoanalyse auf Basis von IT-Grundschutz
- **BSI-Standard 100-4:**
  Notfallmanagement
- **Prüfschema:**
  ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz

IT-Grundschutz-Kataloge



- Einführung
- Modellierungshinweise
- Baustein-Kataloge
- Gefährdungs-Kataloge
- Maßnahmen-Kataloge

IT-Grundschutz
und Entwicklungen darum herum

Dienstleistungen und Produkte rund um den IT-Grundschutz

Sicherheitsbedarf, Anspruch

\- / ° / +

Leitfaden Informationssicherheit

Webkurse 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**

Weitere Trends bei Risiken und Sicherheitsvorkehrungen

Social Networks

- XING
- Facebook
- myspace
- linkedin
- ICQ
- twitter
- ...

Social Networks

- Plattformen im Internet zur Beziehungspflege + Kommunikation mit verschiedenen Zielgruppen
- Mitarbeiter und viele Unternehmen hier aktiv
  - Kundenansprache
  - Kontaktpflege
  - Informationsaustausch

Social Networks

Diverse Gefährdungen aus Sicht Datenschutz und Informationssicherheit

- Wer steht hinter einer digitalen Identität?
- Wer benutzt meine digitale Identität?
- Wer hat auf meine Daten Zugriff? Freunde? Fremde? Anbieter?
- Wofür können meine Informationen verwendet werden?
  - Werbung
  - Personalstelle
  - Social Engineering (von „Passwort-Raten“ bis zum Identitätsdiebstahl)

Social Networks

Sicherheitsmaßnahmen für Institutionen:

- Arten von Sozialen Netzwerken sichten
- Rechtliche Rahmenbedingungen klären, vor allem Geschäftsbedingungen der Anbieter!
- Nutzung regeln
  - Macht die Institution eigene Angebote?
  - Sollen Mitarbeiter in Social Networks aktiv werden?
  - Darf dabei Bezug zur Firma hergestellt werden?
  - Welcher Sprachstil ist akzeptabel?
- Mitarbeiter auf Problematik und Regelungen hinweisen

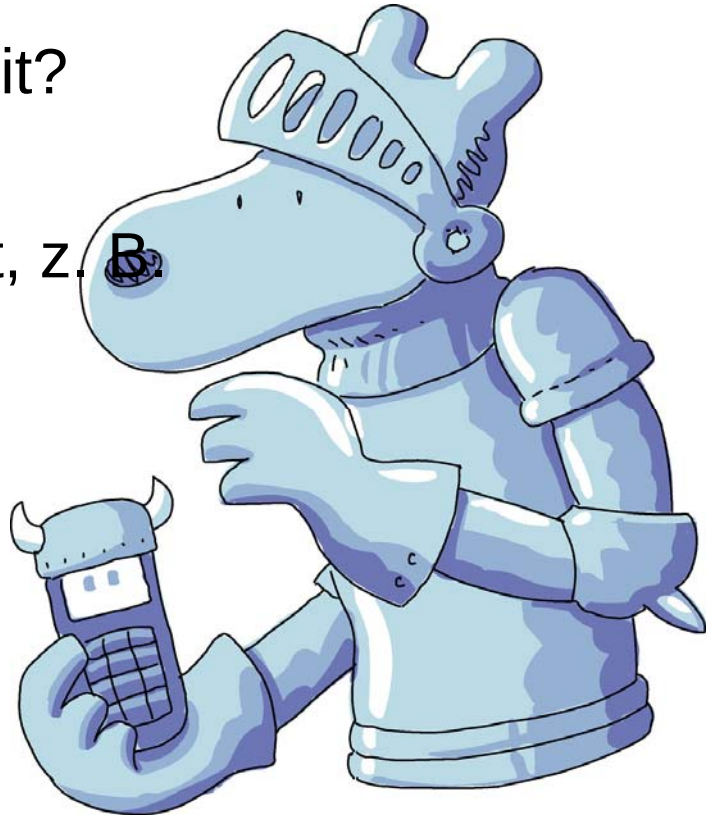
Consumerisation / BYOD

- Tolle Idee, hoher Wohlfühlfaktor
- Aber auch mehr Probleme
  für die Informationssicherheit
  und die IT-Abteilung!
  - So sicher wie zentral beschaffte und administrierte Geräte?
  - Viele wechselnde Plattformen
  - Was ist dienstlich, was ist privat?

Consumerisation / BYOD

Maßnahmen für Smartphones:

- Nutzung regeln! Wer darf was womit?
- Mitarbeiter sensibilisieren
- Und natürlich technische Sicherheit, z. B.:
  - Sichtschutzfolie für Smartphones
  - Verschlüsselung aller Daten
  - Umfassender Virenschutz
  - Regelmäßige Datensicherung
  - Regelmäßiges Patchen
  - Fernlöschung und Lokalisierung
  - Alle nicht benutzten Schnittstellen abschalten



Vielen Dank
für Ihre Aufmerksamkeit

Noch Fragen?

IT-Grundschutz-Hotline
Telefon: 0228-9582-5369
E-Mail: grundschutz@bsi.bund.de

GSTOOL-Hotline
Telefon: 0228-9582-5299
E-Mail: gstool@bsi.bund.de

XING-Forum IT-Grundschutz

https://www.bsi.bund.de/grundschutz

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Isabel Münch
Godesberger Allee 185-189
53175 Bonn

grundschutz@bsi.bund.de
Tel: +49 (0)228-9582-5369
Fax: +49 (0)228-109582-5369

www.bsi.bund.de
www.bsi-fuer-buerger.de