Klausurtagung des
Landesausschusses
12. April 2013

Alles was Recht ist

Dinge, die Kommunen im Netz beachten sollten

The Potsdam eGovernment
ifG.CC
Competence Center

Fachhochschule
Brandenburg
University of
Applied Sciences

VORBEREITUNG EINES KOMMUNALEN INTERNETAUFTRITTS

Relevante Rechtsgebiete bei der Domainregistrierung

Namensrecht nach § 12 BGB

Schützt unter anderem den Namen von Gebietskörperschaften vor Namensanmaßung und Namensmissbrauch.

Markenrecht (MarkG)

Schützt insbesondere eingetragene Marken beim Deutschen Patent- und Markenamt (DPMA), die im geschäftlichen Verkehr genutzt werden.

Wettbewerbsrecht (UWG)

Schützt z.B. vor wettbewerbswidriger Behinderung, Irreführung des Internetnutzers durch Herkunftstäuschung.

Anzuwendendes Recht für Internetseiten und soziale Netzwerke

- Telemediengesetz (**TMG**)
- Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (**BbgDSG**)
- Bundesdatenschutzgesetz (**BDSG**)

Datenschutzregelungen des TMG gelten nicht:

- **im Dienst- und Arbeitsverhältnis** zu ausschließlich dienstlichen Zwecken
- **innerhalb von oder zwischen** öffentlichen Stellen
- ausschließlich **zur Steuerung von internen Arbeits- oder Geschäftsprozessen**.

(§ 11 Abs. 1 TMG)

Bereitstellen der Internetseite durch einen externen Dienstleister

Auftragsdaten-verarbeitung (§ 11 BbgDSG) (§ 11 BDSG)

- Betrifft **Erhebung, Verarbeitung und Nutzung personenbezogener Daten** durch andere Stellen, z. B. bei Outsourcing oder Beauftragung zentraler Rechenzentren
- die **Verantwortung** für die ordnungsgemäße Datenverarbeitung verbleibt beim Auftraggeber
- **Voraussetzungen** (schriftlicher Vertrag)
  - Umfang der Datenverarbeitung
  - Verwendete Programme
  - Datenschutz und Datensicherheitsmaßnahmen des Auftragnehmers (Sicherheitskonzept)
  - Weisungsbefugnisse des Auftraggebers bei allen datenschutzrelevanten Sachverhalten

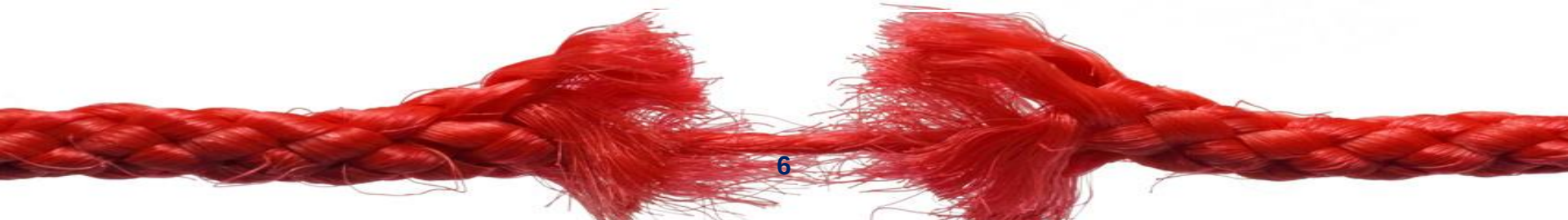
Grundlegende Standards zum IT-Sicherheits- und Risikomanagement in Verwaltungen

IT- Grundschutz

1. **BSI-Standard 100-1: Managementsysteme für Informationssicherheit**
2. **BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise**
3. **BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz**
4. **IT-Grundschutz-Kataloge**

insb. Schutzbedarfsbestimmung und ggf. ergänzende Risikoanalyse

ISO/IEC 27001	Anforderungen an Informationssicherheits-Managementsysteme (ISMS)
ISO/IEC 27002	Leitfaden zum Informationssicherheitsmanagement
Cobit	Kontrollziele für Informations- und verwandte Technologie
ITIL	IT Infrastruktur Verfahrensbibliothek



GESTALTUNG UND BETRIEB EINER INTERNETSEITE / SOCIAL-MEDIA-SEITE

Impressum
(nach § 5 Abs. 1 TMG)

Inhalt	Anforderungen
▪ Name und die Anschrift der Dienststelle ▪ Vor- und Nachname des Verantwortlichen (z.B. des Dienststellenleiters) ▪ Vollständige Postanschrift ▪ sonstige Angaben, zur schnellen elektronischen Kontaktaufnahme/ unmittelbaren Kommunikation	▪ leicht erkennbar ▪ unmittelbar erreichbar ▪ ständig verfügbar ▪ bezeichnet mit "Anbieterkennzeichnung", "Kontakt" oder "Impressum"

zu beachten: § 6 TDG und § 10 MDStV wurden durch § 5 Abs. 1 TMG ersetzt

Online-Datenschutzerklärung nach § 13 Abs. 1 TMG

§ 11–15a TMG,
+ BbgDSG,
+ BDSG

Unterrichtung des Nutzers

- Zu Beginn des Nutzungsvorganges
- Über Art, Umfang, Ort und Zwecke der Erhebung und Verwendung seiner personenbezogenen Daten
- In allgemein verständlicher Form
- Beim automatisierten Verfahren mit der Möglichkeit der späteren Identifizierung – zu Beginn des Verfahrens
- Der Inhalt muss jederzeit abrufbar sein
- Soll auf jeder Seite des Internetangebots und bei Eingabe von personenbezogenen Daten leicht erreichbar sein

Online-Datenschutzerklärung

Bestandsdaten (§ 14 TMG)

dürfen nur erhoben und verwendet werden, wenn:

- für die Begründung
- inhaltliche Ausgestaltung und
- Beendigung

eines Vertragsverhältnisses notwendig.

Nutzungsdaten (§ 15 TMG)

dürfen nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen.

Nutzungsdaten sind insbesondere:

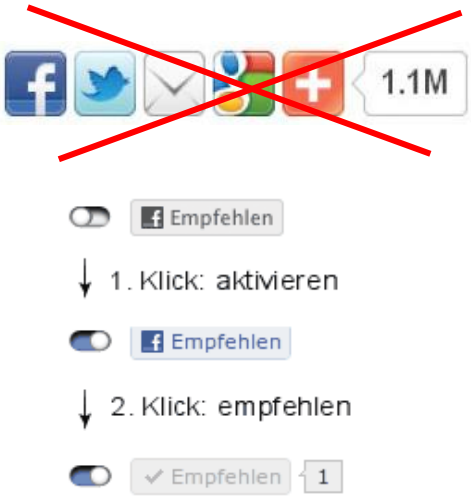
- Merkmale zur Identifikation,
- Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung,
- Angaben über in Anspruch genommenen Telemedien.

Probleme:
Verwendung von Social-Plug-Ins, Web-Analyse-Tools und Cookies

Datenschutzkonforme Lösungsansätze für Social Plug-Ins und Web-Analyse-Tools

Social Plug-Ins

- Einbindung unterlassen
- Verwendung des „2 Click Social Media Buttons“
  + Link zur Datenschutzerklärung neben den Buttons
  + Erläuterung in den Datenschutzerklärungen
- Informationen zum Zweck und Umfang der Datenerhebung



Web-Analyse-Tools

- Vertrag zur Auftragsdatenverarbeitung mit Google
- Anonymisierung der IP-Adressen
- Widerspruchsrecht der Betroffenen
- angepasster Datenschutzhinweis
- Löschung von Altdaten

Piwik

Google Analytics

„_anonymizeIp()“

Inhalt und Gestaltung von Social Media Sites

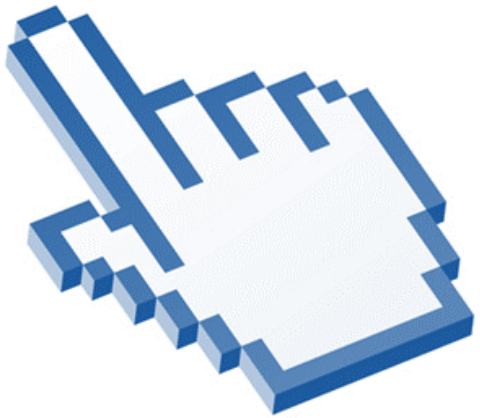
- **Gleiche Regeln wie für die Webseiten von Verwaltungen**
- **Fotos, Videos und sonstige Inhalte**
  - Urheberrechte beachten!
  - Recht am eigenen Bild beachten (Einverständnis der Abgebildeten)
- **Nutzer generierte Inhalte**
  - jeder haftet für eigene Inhalte
  - Haftung für fremde Inhalte ab Kenntnis (keine Überwachungspflicht, aber schnelles Handeln nach Kenntnis erforderlich)
- **Weiterhin zu beachten:**
  - Social Media Guidelines
  - Einwilligung für Werbenachrichten

Datenschutzrecht in sozialen Netzwerken
- ausgewählte Anforderungen -

- zugängliche und verständliche Informationen zum Erhebungszweck
- Voreinstellungen nach Einwilligungsprinzip
- Betroffenenrechte vereinfachen
- Speicherung biometrischer Daten nur mit Einwilligung
- Pseudonyme Nutzung und Löschverpflichtungen nach TMG
- technische und organisatorische Maßnahmen zur Datensicherheit

Gästebücher, Internet-Foren, externe Links

- **Datenschutzrechtlicher Betrieb von Gästebücher und Internet-Foren**
  - nicht anonym, sondern selbst gewähltes Pseudonym
  - Hinweis in Nutzungsbedingungen oder Datenschutzerklärungen
  - geringe Anzahl von Einträgen = Moderation
  - hohe Anzahl von Einträgen = tägliche Überprüfung
- **Verlinkung auf externe Webseiten**
  - klare Kennzeichnung von externen Links
  - möglichst immer in neuen Browser-Fenstern öffnen
  - vermeiden von "Deep-Links"
  - Datum der Verlinkung angeben
  - regelmäßige Überprüfung gesetzter Links



Barrierefreiheit - Relevante Regelungen

Gesetz zur Gleichstellung behinderter Menschen

(BGG, vom 27. April 2002)

Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz

(BITV 2.0, vom 12. September 2011)

Verordnung zur Zugänglichmachung von Dokumenten für blinde und sehbehinderte Menschen im Verwaltungsverfahren nach dem BGG

(Verordnung über barrierefreie Dokumente in der Bundesverwaltung, VBD, vom 17. Juli 2002)

Barrierefreiheit
Inhalte der BITV 2.0

Priorität I (muss)	Priorität II (soll)	Prinzip 1 **Wahr-nehmbarkeit**	▪ Alternativen für Bilder, Videos etc. ▪ Alternativen für zeitgesteuerte Medien ▪ Inhalte ohne Informations- oder Strukturverlust ▪ Wahrnehmung des Inhalts und Unterscheidung zwischen Vorder- und Hintergrund
		Prinzip 2 **Bedienbarkeit**	▪ Tastatur-Zugänglichkeit ▪ ausreichend Zeit zum Lesen und Verwenden ▪ Orientierungs- und Navigationshilfen
		Prinzip 3 **Verständlichkeit**	▪ lesbare und verständliche Texte (vorherrschende Sprache) ▪ Aufbau und Benutzung sind klar ▪ Fehlervermeidung und -korrektur
		Prinzip 4 **Robustheit**	▪ Kompatibilität mit Benutzeragenten (Syntaxanalyse, Name, Rolle, Wert)

Weitere Aspekte des IT-Rechts

Anschein ArchiSav ArchiSig Augenschein Beweiswert BGB
BSI IT-Grundschutz BSI TR-03125 (ESOR)
BSI TR-03138 "Ersetzendes Scannen (RESISCAN)" De-Mail ePostbrief HTML
IT-Compliance IT-Governance IT-Grundschutz
Jugendschutzgesetz Langzeitspeicherung LDAP Markenrecht nPA
Organisationskonzept elektronische Verwaltungsarbeit OSCI PDF-A
Revisionssicherheit Risikoermittlung Safe Harbor SAGA
Schriftform Schutzbedarf Sicherheitskonzept SigG SigV SOAP StGB
UP-Bund Urkundenbeweis USA PATRIOT Act VwVfG W3C
Wettbewerbsrecht XML ZPO

Fachhochschule Brandenburg
University of Applied Sciences

Vielen Dank!

Mario Tönse

Dipl. Betriebswirt (FH)
Dipl. Informatiker (FH)
M. Sc. Security Management

IfG.CC – The Potsdam eGovernment Competence Center
Am Neuen Markt 9c, 14467 Potsdam
eMail: mtoense@ifg.cc,
Web: www.ifg.cc

Bildnachweis

Urheber:

© opicobello - Fotolia.com

© ferkelraggae - Fotolia.com

© bröc - Fotolia.com

© Aleksandr Bedrin - Fotolia.com

© Marco2811 - Fotolia.com

© bluedesign - Fotolia.com

© Sashkin - Fotolia.com

© Schlierner - Fotolia.com

© fotos4u - Fotolia.com

© Fineas - Fotolia.com

© virtua73 - Fotolia.com

Online-Datenschutzerklärung
- Einwilligung -

BDSG

Formale Erfordernisse für eine Einwilligung
(insb. § 4a BDSG)

Freiwillige Entscheidung	Keine Kopplung mit anderen Rechtsfolgen (z. B. Erbringung anderer Leistungen)
Informationspflicht • zum Zweck der Erhebung • zu seinen Rechten • zu den Folgen einer Ablehnung der Einwilligung • zu den Konsequenzen seiner Einwilligung • welche Daten erhoben werden • wer die Verantwortliche Stelle ist (Erreichbarkeit, ggf. Ansprechpartner) • an wen die Daten übermittelt werden	Zusammenhang mit anderen Erklärungen ist hervorzuheben Bedarf der Schriftform (Ausnahmen möglich!) muss vor dem fraglichen Vorgang erfolgen (Erhebung, Verarbeitung, Nutzung) besonders hervorheben wenn mit anderen Erklärungen abgegeben

TMG

Einwilligung kann elektronisch erklärt werden, wenn sichergestellt wird, dass:

- der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung freiwillig abgegeben wird,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

BSI-Standards zur IT-Sicherheit

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 100-1:
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2:
IT-Grundschutz-Vorgehensweise

BSI Standard 100-3:
Risikoanalyse auf der Basis von IT-Grundschutz

BSI Standard 100-4:
Notfallmanagement

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

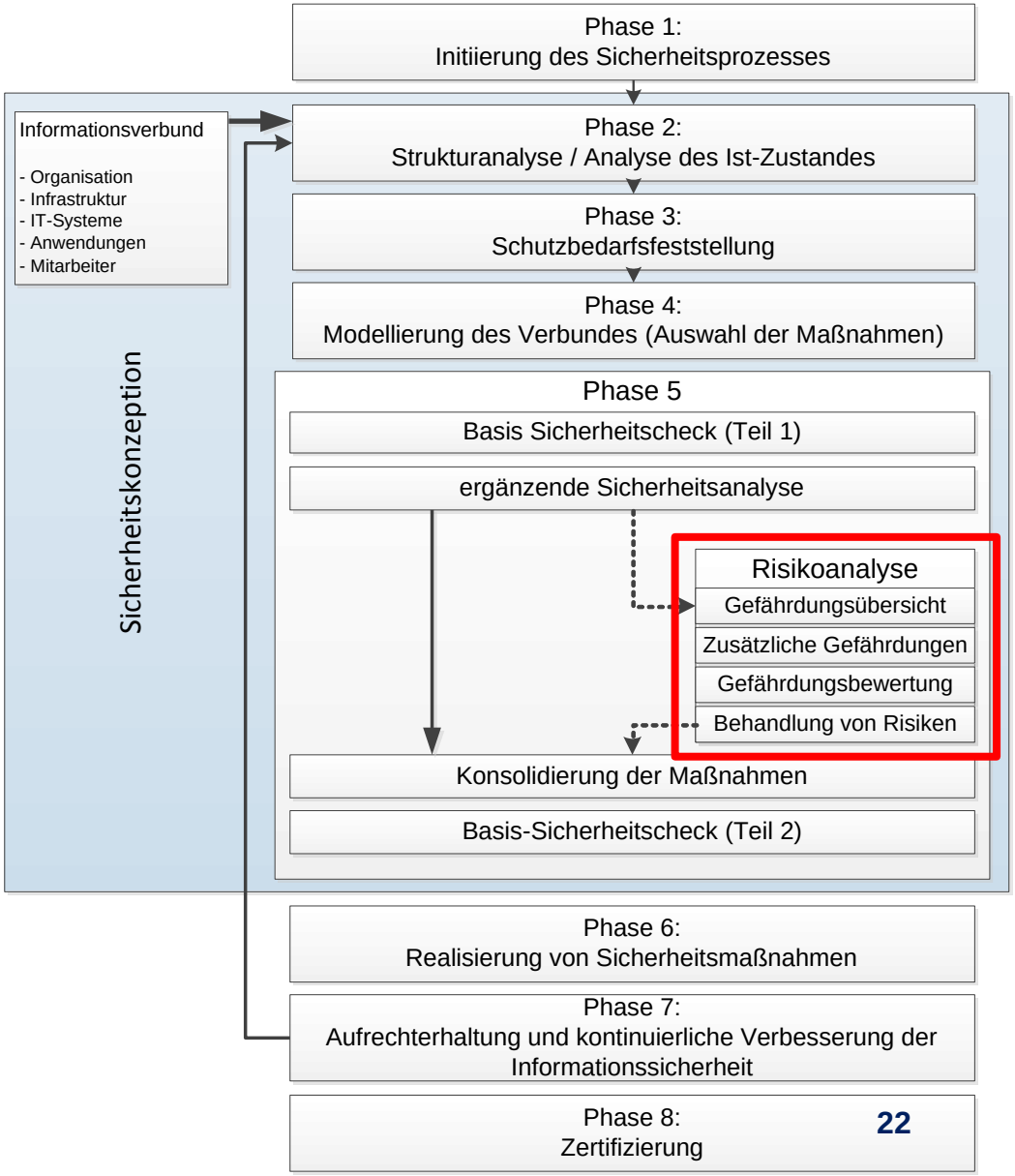
Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

Kapitel 4: Rollen

- **Bausteinkataloge**
  - Kapitel B1 "Übergreifende Aspekte"
  - Kapitel B2 "Infrastruktur"
  - Kapitel B3 "IT-Systeme"
  - Kapitel B4 "Netze"
  - Kapitel B5 "IT-Anwendungen"
- **Gefährdungskataloge**
- **Maßnahmenkataloge**

IT-Grundschutz
Vorgehensweise nach BSI IT-Standard 100-2



Eine „Ergänzende Sicherheits-analyse“ ist durchzuführen, wenn:

- hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit
- keine oder unzureichende Bausteinen des IT-Grundschutzes
- Einsatzszenarien (Umgebung, Anwendung) ohne Betrachtung im Rahmen des IT-Grundschutzes

Schutzbedarfsfeststellung als Grundlage der Risikoanalyse

Die Schäden, die bei Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für Geschäftsprozesse oder Anwendungen einschließlich ihrer Daten entstehen können, lassen sich i. d. R. folgenden Schadensszenarien zuordnen:

1. Verstoß gegen Gesetze/Vorschriften/Verträge
2. Beeinträchtigung der informationellen Selbstbestimmung
3. Beeinträchtigung der persönlichen Unversehrtheit
4. Beeinträchtigung der Aufgabenerfüllung
5. Negative Innen- und Außenwirkung
6. Finanzielle Auswirkungen

Schutzbedarfsfeststellung als Grundlage der Risikoanalyse

Schutzbedarfsklassen

- **normal**
  → Die Schadensauswirkungen sind begrenzt und überschaubar.
- **hoch**
  → Die Schadensauswirkungen können beträchtlich sein.
- **sehr hoch**
  → Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Bildung einer Schutzbedarfsmatrix

	Schutzbedarfskategorien		
Schadensszenarien	Normal	Hoch	Sehr hoch.
	• Die Schadensauswirkungen sind begrenzt und überschaubar.	• Die Schadensauswirkungen können beträchtlich sein.	• Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.
Verstoß gegen Gesetze/ Vorschriften/ Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
Beeinträchtigung des informationellen Selbstbestimmungs-rechts	• Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.	• Es handelt sich um personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist.
Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
Beeinträchtigung der Aufgabenerfüllung	• …	• …	• …
Negative Innen- oder Außenwirkung	• …	• …	• …
Finanzielle Auswirkungen	• …	• …	• …