Sicherheits-normen

Sicherheitsnormen

Nutzen

- Vereinfachung der Prozesse
- Senkung der Versicherungsbeiträge / Finanzierungskosten und Prozesskosten
- Senkung von Geschäfts- und Haftungsrisiken
- Zertifizierung: Stärkung der Images in der Öffentlichkeit und bei Geschäftspartnern

Sicherheitsnormen

Kosten

- **Intern**: Erstellung und Aufrechterhaltung einer Sicherheitsnorm
- **Extern**: Kosten für externe Unterstützung durch spezialisierte Beratungsunternehmen
- **Audit-Kosten**: Kosten von Zertifizierungsunternehmen

Sicherheitsnormen

Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand[9]	International Standards Organisation[10]	Bundesamt für Sicherheit in der Informationstechnik[11]
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 170 Seiten	ca. 400 Seiten	ca. 4.500 Seiten
Detaillierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Umfang des Maßnahmenkataloges	ca. 400 Maßnahmen	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

Sicherheitsnormen

Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand[9]	International Standards Organisation[10]	Bundesamt für Sicherheit in der Informationstechnik[11]
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 170 Seiten	ca. 400 Seiten	ca. 4.500 Seiten
Detaillierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Umfang des Maßnahmenkataloges	ca. 400 Maßnahmen	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

CISIS12 – ehemals ISIS12

1. Leitlinie erstellen
2. Mitarbeiter sensibilisieren
3. Informationssicherheitsteam aufbauen
4. IT-Dokumentationsstruktur festlegen
5. IT-Servicemanagement-Prozess einführen
6. Kritische Applikationen identifizieren
7. IT-Struktur analysieren
8. Sicherheitsmaßnahmen modellieren
9. Ist-Soll vergleichen
10. Umsetzung planen
11. Umsetzen
12. Revision

https://cisis12.de/

Information Security Management System

- Die organisierte und nachvollziehbare Abwehr von Bedrohungen der Informationssicherheit
- Die Sicherstellung gesetzlicher Anforderungen
- U.a. bei Ebenen übergreifenden Verfahren und bei der Anbindung an das Verbindungsnetz
- Die Optimierung der Kosten beim IT-Einsatz
- Die planbare Nutzung der IT für alle Verwaltungsabläufe
- Die Minimierung der Risiken für den Umgang mit Informationen
- Die Steigerung des Vertrauens in der Öffentlichkeit
- Die Integration in das übergeordnete Managementsystem

Fragenkatalog für einen IT-Sicherheitscheck: http://www.sitom.de/

Sicherheitsnormen

Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand[9]	International Standards Organisation[10]	Bundesamt für Sicherheit in der Informationstechnik[11]
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 170 Seiten	ca. 400 Seiten	ca. 4.500 Seiten
Detaillierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Umfang des Maßnahmenkataloges	ca. 400 Maßnahmen	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

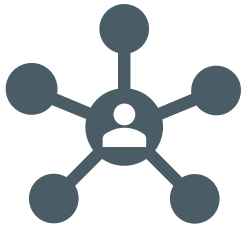
Sicherheitsnormen

Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand[9]	International Standards Organisation[10]	Bundesamt für Sicherheit in der Informationstechnik[11]
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 170 Seiten	ca. 400 Seiten	ca. 4.500 Seiten
Detaillierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Umfang des Maßnahmenkataloges	ca. 400 Maßnahmen	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

ISO 27000–Reihe

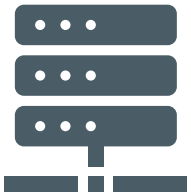
- ISO/IEC 27000 enthält Begriffe und Definitionen, welche in der Normenserie ISO/IEC 27000 verwendet werden.
- ISO/IEC 27001 enthält die Anforderungen an ein ISMS.
- ISO/IEC 27002 enthält Empfehlungen für diverse Kontrollmechanismen für die Informationssicherheit.
- ISO/IEC 27003 enthält einen Leitfaden zur Umsetzung der ISO/IEC 27001 (herausgegeben im Februar 2010).
- …

ISO 27001 – Maßnahmen



Maßnahmen für Netze:

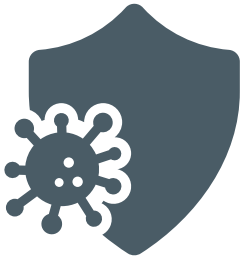
Um Netze vor Bedrohungen zu schützen, die Sicherheit von Systemen und Anwendungen in Netzen zu erhalten, sowie die übertragenen Informationen zu schützen, müssen Netze angemessen verwaltet und kontrolliert werden.



Maßnahmen für Netzwerkdienste:

Sicherheitsmerkmale, Leistungsumfang und Administrationsanforderungen müssen für alle Netzdienste aufgenommen werden, unabhängig davon, ob diese Dienste intern oder von externen Dienstleistern erbracht werden.

ISO 27001 – Maßnahmen



Maßnahmen gegen Schadsoftware:

Maßnahmen zur Erkennung, Verhinderung und Wiederherstellung zum Schutz vor Schadsoftware sowie Maßnahmen und angemessene Verfahren zur Schärfung des Benutzerbewusstseins müssen umgesetzt werden.

Maßnahmen für Elektronische Nachrichten:

Informationen, die Teil einer elektronischen Nachrichtenübermittlung sind, müssen angemessen geschützt werden.

Sicherheitsnormen

Kriterien	ISIS12	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	Netzwerk Informationssicherheit für den Mittelstand[9]	International Standards Organisation[10]	Bundesamt für Sicherheit in der Informationstechnik[11]
Zielgruppe	Kleine und mittlere Unternehmen	Organisationen jeder Größenordnungen	Organisationen jeder Größenordnungen und öffentliche Verwaltung
Dokumentation	ca. 170 Seiten	ca. 400 Seiten	ca. 4.500 Seiten
Detaillierung	Mittel	Minimalistisch abstrakt	Maximal detailliert
Aufbau	Selektierte Bausteine + Maßnahmen	Maßnahmenempfehlungen	Umfassende Bausteine, Gefährdungen + Maßnahmen
Umfang des Maßnahmenkataloges	ca. 400 Maßnahmen	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	indirekt	grundsätzlich	ergänzend
Umsetzung	konkret formulierte Maßnahmen umsetzen	allgemeingültig formulierte Maßnahmen umsetzen	konkret formulierte Maßnahmen umsetzen
Mögliche Zertifizierung	DQS-Zertifizierung	ISO-Zertifizierung	ISO-Zertifizierung nach IT-Grundschutz

IT-Grundschutz-Methodik

- BSI-Standard 200-2
- Bildet zusammen mit dem IT-Grundschutz-Kompendium die Basis zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS)
- Führt drei Vorgehensweisen ein:
  - Basis-Absicherung
  - Kern-Absicherung
  - Standard-Absicherung

Basis-Absicherung

Voraussetzungen:

- ein Informationssicherheitsprozess wurde initiiert
- die Sicherheitsleitlinie und Informationssicherheitsorganisation wurden definiert
- eine Übersicht der vorhandenen Assets der Institution wurde erstellt
- die Basis-Absicherung wurde als IT-Grundschutz-Vorgehensweise ausgewählt

Basis-Absicherung

Festlegung des Geltungsbereichs

- Organisation
- Infrastruktur
- IT-Systeme
- Anwendungen
- Mitarbeiter

→ Auswahl und Priorisierung Relevanter Bausteine

↓

IT-Grundschutz-Check (Basisanforderungen)

↓

Realisierung der Maßnahmen

↓

Auswahl der folgenden Vorgehensweise (Kern- oder Standard-Absicherung)

Kern-Absicherung

Vorgehensweise:

- konzentriert sich auf den Schutz von besonders schützenswerten Assets
- Soll-Ist-Vergleich zwischen den im IT-Grundschutz-Kompendium aufgestellten Anforderungen
- Basis für ein umfangreicheres Sicherheitskonzept

Kern-Absicherung

Festlegung des Geltungsbereichs
(abgegrenzt und klein)

Identifikation und Festlegung der kritischen Assets (Kronjuwelen)

Strukturanalyse
Analyse des Ist-Zustandes

Schutzbedarfsfeststellung

Modellierung
Auswahl und Anpassung von Anforderungen

IT-Grundschutz-Check
Erfüllungsstatus der Anforderungen feststellen

Risikoanalyse und weiterführende Sicherheitsmaßnahmen

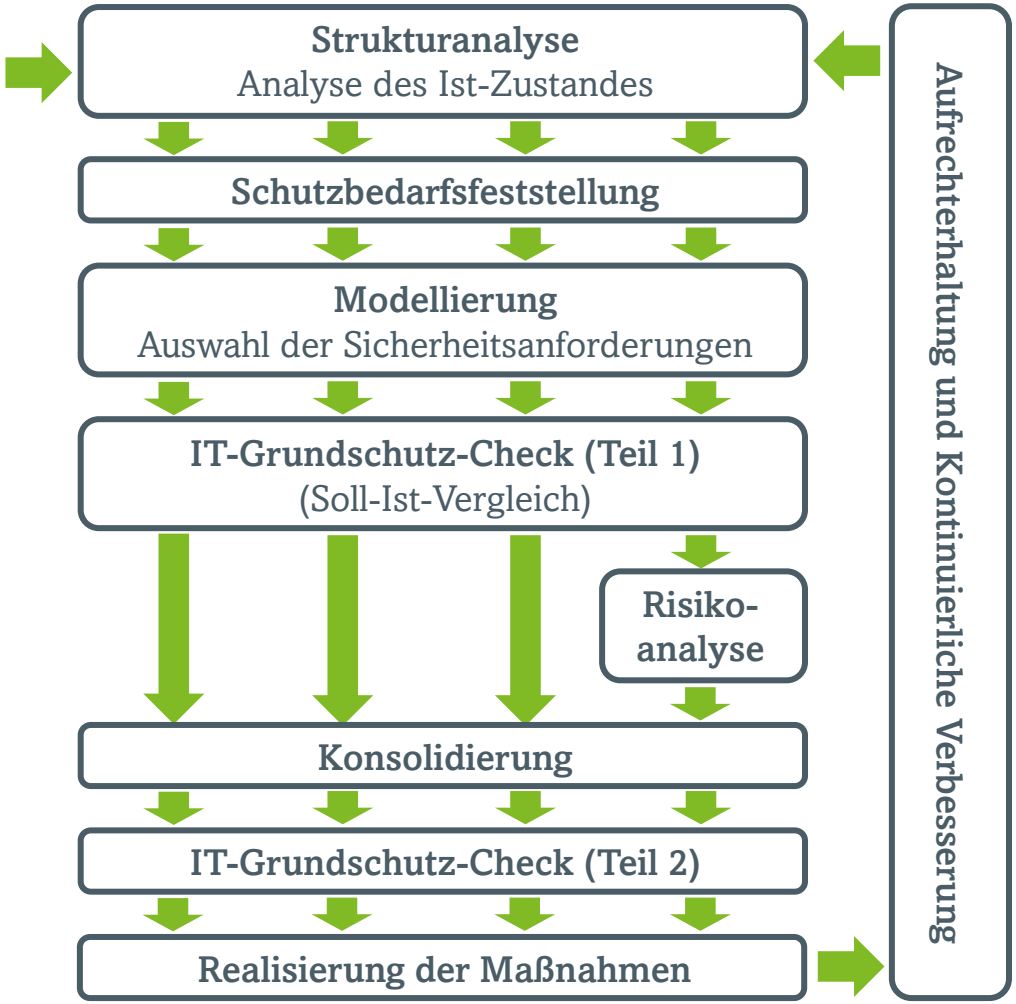
Umsetzung und weitere Schritte
Verbesserung, Erweiterung, Zertifizierung

Standardabsicherung

Standard-Absicherung

Festlegung des Geltungsbereichs

- Organisation
- Infrastruktur
- IT-Systeme
- Anwendungen
- Mitarbeiter

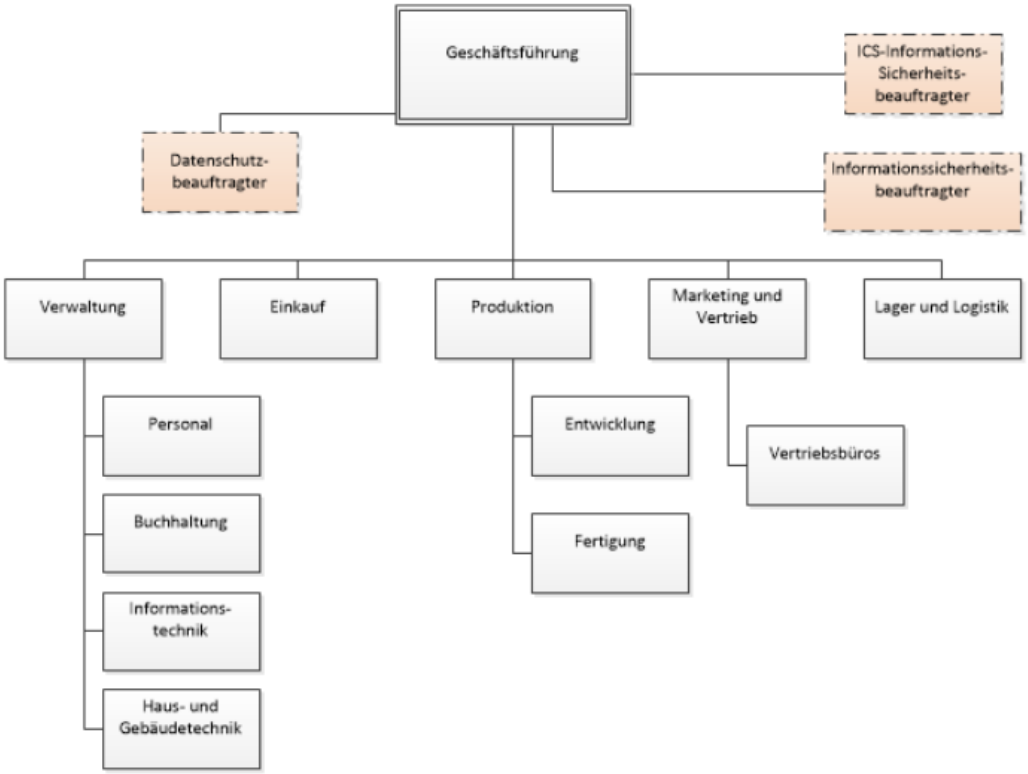


Arbeitsbeispiel RECPLAST GmbH

- Beispiel, um die IT-Grundschutz-Methodik nach BSI-Standard 200-2 am fiktive Beispielunternehmen „RECPLAST GmbH“ darzustellen.
- Referenzdokumente für eine Zertifizierung nach ISO 27001

Geltungsbereich

- Organisatorische Gliederung



Geltungsbereich

- **Organisatorische Gliederung**
- **Standorte und Mitarbeiter**
  - Beschreibung der Standorte und Mitarbeiter:innen
- **Vereinfachter Netzplan der RECPLAST**
  - Darstellung des Aufbaus des Netzes mittels eines Diagramms
- **Informationstechnik**
  - Beschreibung der eingesetzten Clients sowie der Server pro Standort

Informationstechnik (Auszug)

Im Netz des Standorts Bad Godesberg (siehe Abbildung 3) werden die folgenden Server für folgende Zwecke eingesetzt:

- Zwei Server dienen als Virtualisierungshosts,
- Ein virtueller Server dient als Domänen-Controller (Virtualisierungshost 1),
- ein virtueller Server dient der Dateiablage (Virtualisierungshost 1),
- ein virtueller Server dient als Druckserver (Virtualisierungshost 1),
- ein virtueller Server dient als internes Ticketsystem (Virtualisierungshost 2),
- ein Server dient als Backupserver,

Sicherheitsmanagement

- Initiierung des Sicherheitsprozesses
- Entwicklung der Leitlinie zur Informationssicherheit
- Inhalt der Leitlinie zur Informationssicherheit

Strukturanalyse

- **Erfassung der Geschäftsprozesse, Anwendungen und Informationen**
  - Zuordnung der Prozesse zu den Standorten

Geschäftsprozess	Standort Bad-Godesberg	Standort Beuel	Standort Vertriebsbüros
GP004 Einkauf	X		
GP005 Disposition		X	
GP007 IT-Betrieb	X	X	X
GP007a Betrieb Server	X	X	

Strukturanalyse

- Erläuterung der wichtigsten Geschäftsprozessen

Kürzel	Name	Beschreibung	Prozess-Art
GP007	IT-Betrieb	Die IT-Abteilung sorgt für den störungsfreien Betrieb der IT-Infrastruktur der Server, Clients und Netze. […]	Unterstützender Prozess
	Mitarbeiter:	Informationstechnik	
GP007a	Betrieb Server	Teilprozess von GP007. Dieser Prozess umfasst Beschaffung, Installation, Konfiguration und Pflege der erforderlichen Hard- und Software	Unterstützender Prozess
	Mitarbeiter:	Informationstechnik	

Strukturanalyse

- Erhebung des Netzplans
- Erhebung der IT-Systeme

Kürzel	Name	Erläuterung	Anzahl	Status	Plattform
C001	Clients der Finanzbuchhaltung	Bei den Clients handelt es sich um handelsübliche Clients.	30	Betrieb	Windows 10
	Benutzer:	Buchhaltung			
C002	Clients der Geschäftsführung	Bei den Clients handelt es sich um handelsübliche Clients.	8	Betrieb	Windows 10
	Mitarbeiter:	Geschäftsführung			

Schutzbedarfsfeststellung

- **Definition der Schutzbedarfskategorien**
  - „normal“: Die Schadensauswirkungen sind begrenzt und überschaubar.
  - „hoch“: Die Schadensauswirkungen können beträchtlich sein.
  - „sehr hoch“ Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen
- **Schutzbedarfsfeststellung für Geschäftsprozesse**
- **Schutzbedarfsfeststellung für Anwendungen**

Datenschutz

Warum Datenschutz?

Schutz des Persönlichkeitsrechts

Der Datenschutz hat das Ziel, das Recht auf informationelle Selbstbestimmung des Einzelnen zu gewährleisten

Bundesdatenschutzgesetz

Aktive Maßnahmen zugunsten der Datensicherheit treffen. Durch Verstöße gegen Auflagen und Forderungen des Datenschutzgesetzes entstehen Bußgelder.

Auffinden von Sicherheitsschwachstellen

Erhöhen des Sicherheitsniveaus und profitieren von den Verbesserungsmaßnahmen im Allgemeinen.

Warum Datenschutz?

Image- und Kundenverlust bei Datenskandalen

Die Imageverluste sind enorm. Seit dem 01.09.2009 gibt es die Verpflichtung, Datenpannen zu veröffentlichen, damit die Betroffenen die Folgen gering halten können.

Kundenerwartungen

Kunden erwarten, dass ein Unternehmen Datenschutz aktiv betreibt!

Gesetze zum Datenschutz

Europäische Menschenrechtskonvention Art. 8, Abs. 1:

Jede Person hat das Recht auf Achtung […] ihrer Korrespondenz.

Bundesdatenschutzgesetz:

- Rechtmäßigkeit
- Zweckbindung
- Datenminimierung
- Wiederherstellbarkeit
- Angemessene Verschlüsselung
- Zeitliche Beschränkung der Speicherung
- Richtigkeit / Integrität und Vertraulichkeit
- Rechenschaftspflicht der Verantwortlichen

Gesetze zum Datenschutz

Europäische Menschenrechtskonvention Art. 8, Abs. 1:

Jede Person hat das Recht auf Achtung […] ihrer Korrespondenz.

Bundesdatenschutzgesetz:

- Rechtmäßigkeit
- Zweckbindung
- …

EU-DSGVO

DSGVO

Neuerungen:

- Bußgeld: bis zu 4% des Jahresumsatzes eines Unternehmens
- Einwilligung des Betroffenen (Mindestalter 16 Jahre in DE)
- Umfangreiche Informationspflichten, elektronische Kopie
- Nichtverarbeitung sehr sensibler Daten (u.a. biometrische Daten)
- System: Verfügbarkeit und Belastbarkeit […] auf Dauer
- Regelmäßige Überprüfung, Bewertung und Evaluierung
- Recht auf Datenübertragbarkeit
- Recht auf Löschung
- Widerspruch bei automatisierten Einzelfallentscheidungen (bislang waren automatisierte Einzelfallentscheidungen i.A. verboten)

Impressum und Datenschutzerklärung

Telemediengesetz §5: Allgemeine Informationspflichten

Folgende Informationen müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein:

- Namen und die Anschrift, ggf. Rechtsform
- Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation ermöglichen, einschließlich der E-Mail
- Ggf. behördlichen Zulassung und zur zuständigen Aufsichtsbehörde
- Ggf. Handelsregister, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, etc.
- Ggf. Umsatzsteueridentifikationsnummer oder eine Wirtschafts-Identifikationsnummer

Impressum und Datenschutzerklärung

Datenschutzerklärung aufgrund des BDSG

Aufklärung über Speicherung personenbezogenen Daten

- Protokollierung am Webserver
- Cookies
- Tracking Tools und das OptOut für die eingesetzten Tools
- Falls Online-Formulare eingesetzt werden: die Verwendung, Weitergabe und Löschung der erhobenen Daten

Die Datenschutzerklärung kann Teil des Impressums sein oder muss genauso leicht zu finden sein.

Werden keinerlei personenbezogene Daten erhoben, so empfiehlt es sich trotzdem eine Datenschutzerklärung anzubieten.

Technisch organisatorische Maßnahmen (TOM)

- Art. 32 DSGVO (Sicherheit der Verarbeitung)
  - treffen von *„geeignete technische und organisatorische Maßnahmen“*

Maßnahmen:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Erhebung personenbezogener Daten

Grundsätze zur Datenverarbeitung nach TMG

- Werden personenbezogene Daten anhand von Webformularen erhoben, so muss der Benutzer sein explizites Einverständnis zur Erhebung, Verarbeitung und Nutzen der Daten geben.

- Der Nutzer muss über den Zweck der Erhebung, Speicherung und Verarbeitung sowie die Löschfristen aufgeklärt werden. Des Weiteren muss aufgeführt werden, welche Folgen eine Verweigerung nach sich zieht.

- Sollen die Daten später zu weiteren Zwecken verwendet werden, muss die Einwilligung hierfür bereits bei der Datenerhebung eingeholt werden – oder eine neue Einverständniserklärung ist nötig.

Erhebung personenbezogener Daten

Notwendigkeit einer Verfahrensbeschreibung

- Für die Erhebung und Speicherung personenbezogene Daten muss i.A. eine Freigabe beim Datenschutzbeauftragten eingeholt werden

Technisches

- Bei Online-Formularen ist auf eine sichere Verbindung zu achten
  - Sonst dürfen keine personenbezogenen Daten erhoben werden
- Der Server darf nicht offen zugänglich sein
- Gleiches gilt für die Backup-Daten

Cookie Banner

- **Datenschutzrichtlinie für elektronische Kommunikation**
  - schränkt seit einem Nachtrag 2009 Cookies ein
- **Durch die DSGVO (25. Mai 2018)**
  - Das Widerrufen muss so einfach sein wie das Einwilligen
- **TTDSG ist seit 01. Dezember 2021**
  - Strengere Regelungen für Setzen von Cookies
  - bis zu 300.000 Euro

Googles Cookie Banner

- französische Datenschutzbehörde verhängte zu Beginn 2022 eine Geldstrafe von Millionen Euro
- youtube.com

neu

- google.com

alt

Google Analytics

- Einsatz ist problematisch
- Nutzer ist anhand gespeicherter IP-Adresse identifizierbar
  - Verstoß gegen das Telemediengesetz §12 Abs 1
- Einverständnis müsste zu Beginn der Nutzung vorliegen
- Dies ist beim Einsatz von Google Analytics üblicherweise nicht der Fall

Google Analytics

Google Analytics trotzdem einsetzen:

- Anonymisierung der IP-Adresse vornehmen (Funktion "anonymizeIP")
- Hinweis an den Nutzer der Webseite, dass ein Widerspruch gegen die Datenauswertung möglich ist

Google Analytics

Google Analytics verhindern:

- Blockiere mittels Add-On
- Firefox Nutzer werden seit der Version V67.0.1 nicht mehr von Google Analytics erfasst

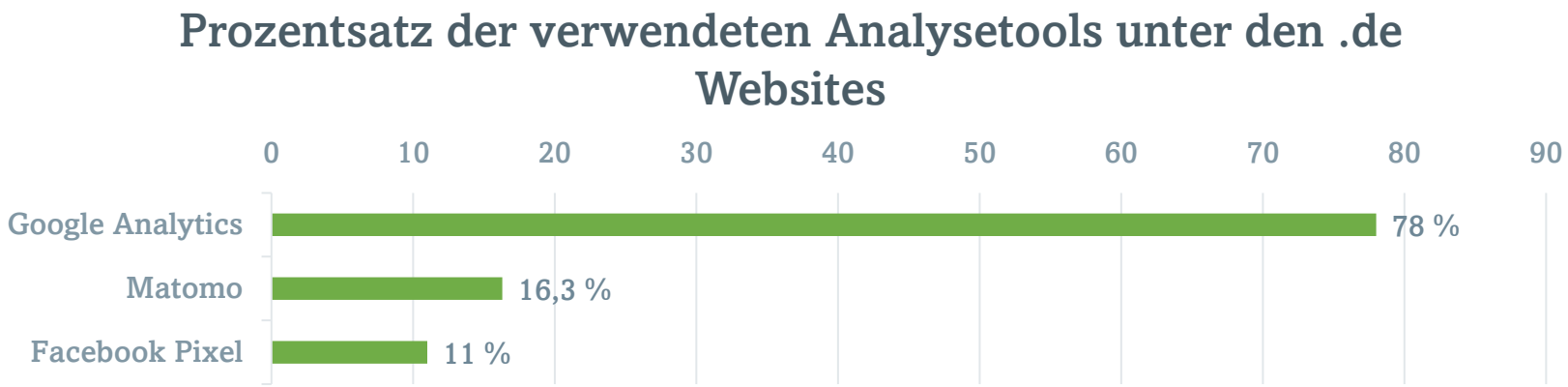
Vorsichtig!

- flixtrain.de funktionierte nicht, wenn Google Analytics blockiert wurde

Open-Source Alternative

matomo

- Open-Source-Webanalytik-Plattform
- 2007 aus „phpMyVisites“ entstanden
- DSGVO-Features



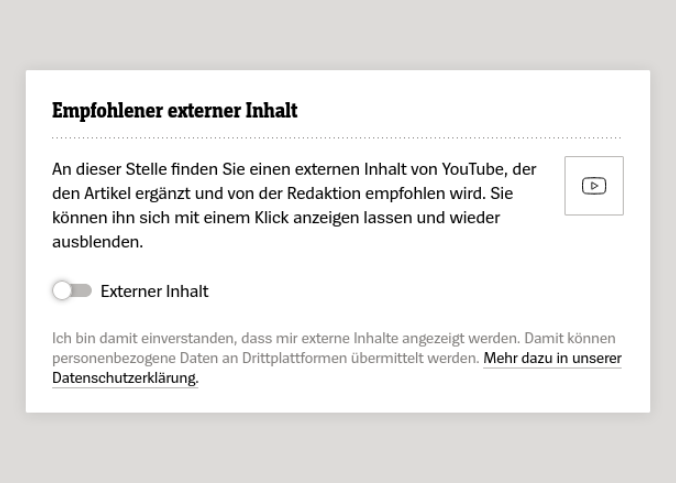
Social Plugins

- Einbindung klassischer Social Plugins (Facebook, Google+, …) ist nicht datenschutzkonform
  - https://www.datenschutz.org/social-media-buttons/ (Aufruf: 04.05.2021)
- Erhebung von Nutzerdaten seitens der Social Networks, ohne dass der Nutzer die Buttons nutzt
- Datenerhebung erfolgt unabhängig davon, ob der Seitenbesucher bei dem jeweiligen Social Network angemeldet oder registriert ist

Mögliche Alternativen:

- 2-Klick-Verfahren
- „Shariff-Buttons“: Links, die erst mit Klick die Verbindung aufbauen

Social Plugins



Datenschutz: Software im Allgemeinen

Was muss man bei Software beachten?

- Nutzerrechte
- Einsatzzweck
- Verfügbarkeit
- Registrierung
- Gewährleistung
- Haftung
- Kündigungsrecht