Kapitel 5:
Rechtliche Regelungen

Inhalt von Kapitel 5

1. Strafgesetzbuch (StGB)
2. Datenschutz (EU-DGSVO, BayDSG)
3. IT-Sicherheitsgesetz

Strafgesetzbuch — Überblick

- Strafgesetzbuch (StGB) regelt Strafrecht
- Verletzungen der Normen werden im Strafverfahren verhandelt
- Antragsdelikt: Tat wird nur auf Antrag (Anzeige) i.d.R. durch den „Verletzten“ (§ 77) verfolgt (§ 202a, 202b, 303a, 303b)
- Offizialdelikt: Tat wird „von Amts wegen“ (Staatsanwaltschaft) verfolgt (§ 202c)
- § 202a: Ausspähen von Daten
- § 202b: Abfangen von Daten
- § 202c: Vorbereiten des Ausspähens und Abfangens von Daten
- § 202d: Datenhehlerei
- § 205b: Strafantrag
- § 303a: Datenveränderung
- § 303b: Computersabotage
- § 303c: Strafantrag

§ 202a StGB: Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b StGB: Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft,
wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c StGB: Vorbereitung des Abfangens oder Ausspähens von Daten („Hackerparagraph“)

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 149 Abs. 2 und 3 gilt entsprechend.
(Vorbereitung der Fälschung von Geld und Wertzeichen; längere Haftstrafen)

Offizialdelikt

Diskussion von § 202c StGB

- Ist der Einsatz von IT-Sicherheitswerkzeugen generell illegal?
  - „Dual use tools“: Fast alles, was gutartig eingesetzt werden kann, kann auch missbraucht werden.
- Reaktionen bei der Einführung von § 202c (08/2007):
  - Rechtsausschuss des Deutschen Bundestages: Gutwilliger Umgang mit solchen Werkzeugen durch IT-Sicherheitsexperten wird nicht von §202c erfasst.
  - Bundesjustizministerium: Unter Strafe werden nur Vorbereitungshandlungen zu *Computerstraftaten* gestellt.
- Verfahren für mehrere Selbstanzeigen wurden eingestellt bzw. abgelehnt.
- EICAR-Empfehlung: Sorgfalt, Dokumentation, Einwilligung http://www.eicar.org/files/jlussi_leitfaden_web.pdf

§202d Datenhehlerei

- Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
- Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.
- Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen.

§ 205 StGB: Strafantrag

- In den Fällen des § 201 Abs. 1 und 2 und der §§ 202, 203 und 204 wird die Tat nur auf Antrag verfolgt. Dies gilt auch in den Fällen der §§ 201a, 202a, 202b und 202d, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

- § 202c fehlt in dieser Aufzählung; d.h. 202c ist Offizialdelikt

- „Besonderes öffentliches Interesse“ liegt im Ermessen der Staatsanwaltschaft.

§ 303a StGB: Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2)
löscht, unterdrückt, unbrauchbar macht oder verändert,
wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt §202c entsprechend.

§ 303b StGB: Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

§ 303b StGB: Computersabotage (Forts.)

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303c StGB: Strafantrag

In den Fällen der §§ 303, 303a Abs. 1 und 2 sowie § 303b Abs. 1 bis 3 wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

Beispiel: Gerichtsurteile

Amtsgericht Duisburg

Song-Klau: Musikdateien-Hacker ist wegen Ausspähens von Daten und Verstößen gegen das Urheberrechtsgesetz strafbar

"DJ Stolen" hackte Rechner internationaler Popstars - unveröffentlichte Songs von Künstlern wie Lady Gaga, Mariah Carey, Leona Lewis und Kesha zum Verkauf angeboten

Das Jugendschöffengericht des Amtsgerichts Duisburg hat zwei junge Männer aus Duisburg und Wesel wegen des Ausspähens von Daten und Verstößen gegen das Urheberrechtsgesetz verurteilt. Gegen den 18-jährigen Angeklagten verhängte das Jugendschöffengericht eine Jugendstrafe von 18 Monaten ohne Bewährung. Sein 23-jähriger Mitangeklagter erhielt 18 Monate auf Bewährung. Einer der Angeklagten erlangte unter der Bezeichnung "DJ Stolen" in der Szene "Berühmtheit".

Den beiden jetzt 18 und 23 Jahre alten Angeklagten wurden insgesamt 130 Verstöße gegen das Urheberrechtsgesetz sowie 98 Fälle des Ausspähens von Daten zur Last gelegt.Sie haben sich im Zeitraum 2009 bis 2010 unter Nutzung von Schadsoftware (Trojanern) unbefugt Zugang zu fremden Computern oder E-Mail- und Datenaccounts im Umfeld der Musikindustrie verschafft und... Lesen Sie mehr | Diskutieren Sie mit

Landgericht Verden

Sasser-Wurm-Prozess: "Sasser"-Programmierer bekommt Bewährungsstrafe

Berufsschüler ist der Datenveränderung sowie der Computersabotage schuldig

In dem sogenannten Sasser-Wurm-Prozess hat das Landgericht Verden den angeklagten 19-jährigen Berufsschüler wegen Datenveränderung in 4 Fällen sowie der Computersabotage in 3 Fällen schuldig gesprochen.

Gegen ihn wird eine Jugendstrafe von 1 Jahr und 9 Monaten verhängt. Die Vollstreckung der Jugendstrafe wird zur Bewährung ausgesetzt. Die Kammer hat in ihrer mündlichen Urteilsbegründung festgestellt, dass der Angeklagte der Datenveränderung und der Computersabotage in den oben genannten Fällen schuldig ist. Dabei hat die Kammer das umfassende Geständnis des Angeklagten, die Angaben...

Landgericht Düsseldorf

Störung von Internetportalen durch DDos-Attacken ist strafbare Computersabotage

Hacker-Angriff auf Internet-Pferdewettbüros - Verurteilung zu Freiheitsstrafe

Wer Unternehmen erpresst und deren Internetseiten zwecks Drohung lahm legt, begeht eine Erpressung in Tateinheit mit Computersabotage. Dies entschied das Landgericht Düsseldorf in einem Fall, in dem ein Arbeitsloser, der sich selbst weit reichende IT-Kenntnisse beigebracht hatte, Pferdewettportale erpresst hatte, um sich ein dauerhaftes Einkommen zu verschaffen. Erst nach mehreren erfolgreichen Erpressungen und nach dem tagelangenen Lahmlegen von verschiedenen Portalen, die dadurch erhebliche Umsatzeinbußen erlitten, war er von der Polizei dingfest gemacht worden.

Der Angeklagte hatte selbst regelmäßig Pferde- und Fußballwetten betrieben. Da er täglich ausgiebig das Internet nutzte und enormen Spaß an der Auslotung der damit verbundenen technischen Möglichkeiten hatte, entschied er sich - zunächst auch aus einer Spielerei heraus - gewinnbringend auszutesten, wie gut der Schutz einzelner Webseiten ist und ob er ihn durchbrechen kann. So entschloss er sich, mittels eines sogenannten Bot-Netzes die Webseiten einzelner Pferdewetten-Anbieter lahm zu legen, falls sie nicht auf seine Erpressungen eingehen würden.Er mietete Server bei einem russischen Provider an und richtete E-Mail-Adressen ein....

Amtsgericht Düren

Kinderzimmer mit Webcam ausspioniert – Spanner zu Bewährungsstrafe verurteilt

44-jähriger hackt sich mittels Trojaner in Computer von Kindern und Jugendlichen ein

Das Amtsgericht Düren verurteilte einen 44-jährigen Mann zu einem Jahr und zehn Monaten Haft auf Bewährung wegen unbefugter Beschaffung von Datenbeständen (§ 202 a StGB) und Besitzes unerlaubter Bildaufnahmen (§ 201 a StGB) mittels einer Webcam.

Im zugrunde liegenden Fall hatte sich ein 44-jähriger Mann aus dem Rheinland zwischen Herbst 2009 und April 2010 in 98 Fällen Zugriff auf fremde Computer von Kindern und Jugendlichen verschafft und diese über eine Webcam ausspioniert. In zwölf Fällen erstellte er dann unerlaubt Bildaufnahmen der Opfer. Insgesamt befanden sich auf dem Computer des Angeklagten rund drei Millionen Bilder....

Quelle: http://www.kostenlose-urteile.de/

Inhalt von Kapitel 5

1. Strafgesetzbuch (StGB)
2. Datenschutz (EU-DGSVO, BayDSG)
3. IT-Sicherheitsgesetz

Informationelle Selbstbestimmung

- (Implizites) Grundrecht, selbst über Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

- Personenbeziehbarkeit liegt vor, wenn aus den Daten auf eine Einzelperson rückgeschlossen werden kann.
  - Name, Matrikelnummer, E-Mail-Adresse, Kontonummer, …
  - IP-Adresse?

- Begriffsherkunft:
  - Gutachten von Steinmüller/Lutterbeck 1971
  - Volkszählungsurteil 1983: ISD als Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 Grundgesetz mit Art. 1 Abs. 1 GG)
  - Kernidee: Wer nicht weiß oder beeinflussen kann, welche Informationen über ihn erfasst werden und was damit gemacht wird, passt aus Vorsicht sein Verhalten an — individuelle Handlungsfreiheit wird eingeschränkt.

Datenschutz-Gesetzgebung

- Europäische Datenschutzgrundverordnung (EU-DSGV)
- Bundesdatenschutzgesetz (BDSG)
- Bayerisches Datenschutzgesetz (BayDSG)
- Regelungen auch in anderen Gesetzen,
  im Umfeld von IT-Diensten besonders relevant z.B.
  - Telekommunikationsgesetz (TKG)
  - Telemediengesetz (TMG)

- Grundprinzipien:
  - Verbot mit Erlaubnisvorbehalt
    - Erhebung, Verarbeitung, Nutzung entweder gesetzlich erlaubt
    - oder der Betroffene gibt seine Einwilligung (informed consent)
  - Datenvermeidung und Datensparsamkeit (Erfordernisprinzip)
  - Zweckbindung
  - Transparenz (Was, von wem, wozu, wie lange)

Wie kommen personenbezogene Daten ins Netz?

- Durch Betroffene selbst:
  - Bewusst: Homepage, Social Media Profile, Einträge in Webforen, …
  - Unbewusst: Mail an Verteiler mit Webarchiv, Dienstpersonalisierung, …
- Freunde, Bekannte
- Schule, Universität, Vereine, Arbeitgeber usw.

- Gefahren:
  - Verknüpfung von Daten aus verschiedenen Quellen
  - Profilbildung (räumlich, zeitlich, Verhalten, Vorlieben, Interessen, …) und deren kommerzielle oder andere Nutzung
  - Kein “Recht auf Vergessenwerden” (nur Einzelurteile, z.B. Löschanträge bei Google, die sich nur im EU-Bereich auswirken)
  - Zweckbindung wird z.B. im Rahmen von AGB-Änderungen angepasst

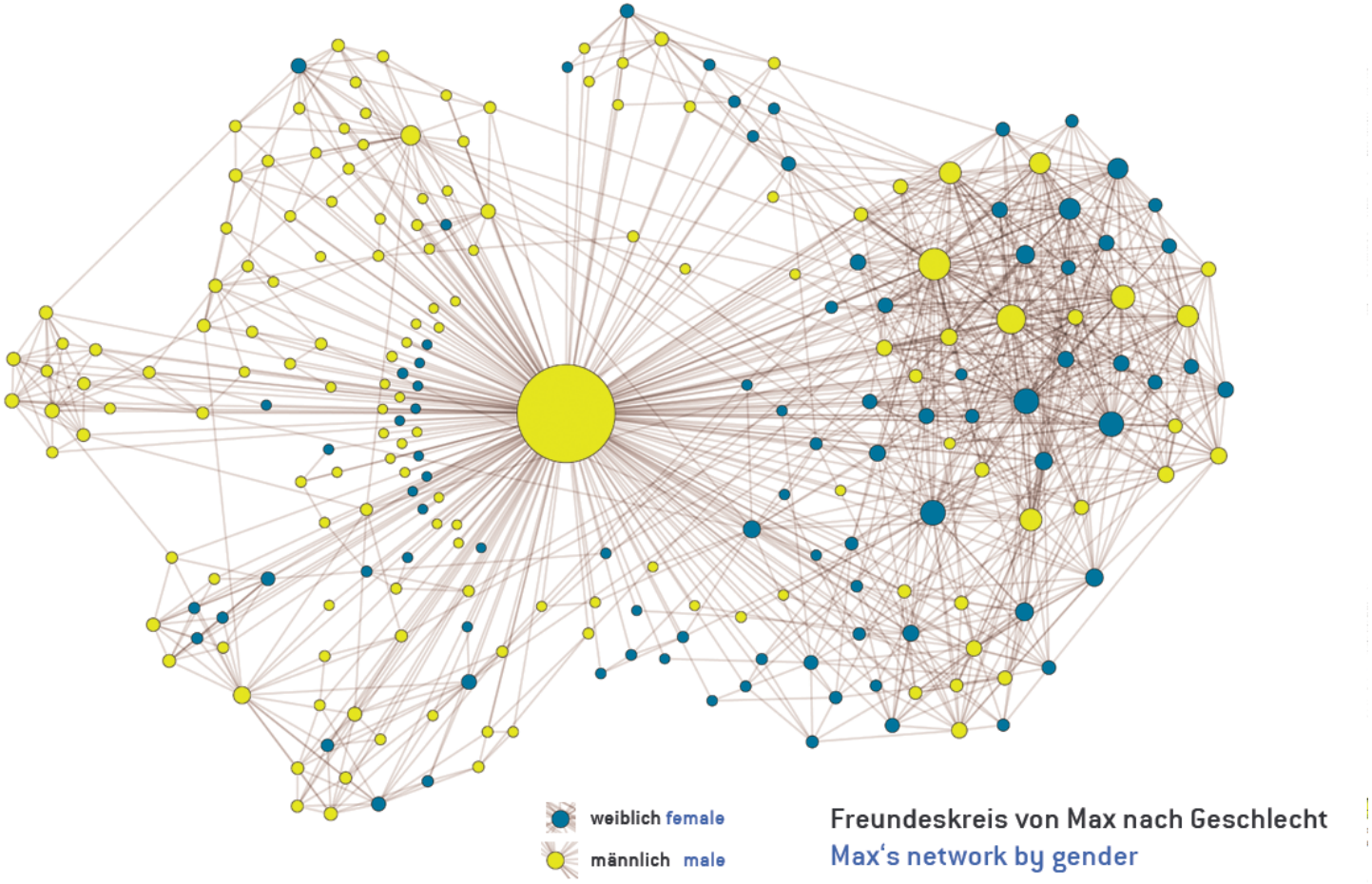
Wer hat personenbezogene Daten?

- Öffentliche Einrichtungen, u.a.:
  - Gemeinden (Meldeamt, Standesamt, Finanzamt, …) und Kirchen
  - Polizei, Staatsanwalt, Verfassungsschutz (Ermittlungsverfahren)
  - Schulen, Universitäten

- Unternehmen, u.a.:
  - Versicherungen (Krankenkasse, KFZ, …), Banken
  - Schufa, Handels- und Wirtschaftsauskunfteien
  - Telekommunikationsunternehmen (Telefon, Handy, DSL, …)
  - Adresshändler
  - Genutzte Dienstleister:
    - Transport (Fluggesellschaften, ggf. ÖPNV)
    - Einzelhandel (Versandhandel, Online-Shops, Kundenkarten, …)
    - Internet-Dienste (z.B. jeder Betreiber von Webservern, Cloud-Datenspeicher, soziale Netzwerke, …)
    - …..

Facebook Freunde von Max Schrems

- Österreichischer Datenschutzaktivist:
  - 2015: Klage vor dem EUGH bringt „Safe Harbor Abkommen“ zwischen EU und USA zur Fall
  - Beschwerde bringt EU-US Privacy Shield zu Fall (16.07.2020)



Umsetzung und Kontrolle des Datenschutzes

- In Bayern:
  - Landesamt für Datenschutzaufsicht (Ansbach) für Privatwirtschaft
  - Landesbeauftragter für Datenschutz (München) für öffentl. Einrichtungen

- Datenschutzbeauftragte (DSB) pro Organisation:
  - Ggf. extern; direkt der Leitung der öff. Stelle unterstellt; weisungsfrei.
  - Im öffentlichen Bereich: Beratend ("Hinwirken", kein "Veto-Recht"), keine Bußgelder, Landesbeauftragter als Eskalationsinstanz
  - Führen des Verzeichnis der Verarbeitungsverfahren:
    - Verzeichnis automatisierter Verfahren zur Verarbeitung personenbezogener Daten.
    - Kann mit Ausnahmen (z.B. bei Staatsanwaltschaft) von jedem kostenfrei eingesehen werden.
    - In der Regel Ausgangspunkt bei Auskunftsanträgen von Betroffenen.

Datenschutz-Gesetzgebung

- Europäische Datenschutzgrundverordnung (EU-DSGV)
- Bundesdatenschutzgesetz (BDSG)
- Bayerisches Datenschutzgesetz (BayDSG)

- Neue EU-DSGV seit 25.05.18 in Kraft

EU-DSGV

- Direkt geltendes Recht in allen Mitgliedsstaaten
- Ziele (Art 5 EU-DSGV) der Verarbeitung
  - Rechtmäßigkeit, Treu und Glauben, Transparenz (Abs. 1a)
  - Zweckbindung (Abs. 1b)
  - Datenminimierung (Abs. 1c)
  - Richtigkeit (1d)
  - Speicherbegrenzung (1e)
  - Sicherheit (!!!), Integrität, Vertraulichkeit (1f)
  - Rechenschaftspflicht (Abs. 2)
- Anwendbarkeit (sachlich und räumlich) Art. 2 und 3
  - ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen
  - Europäische Union
  - Auch für nicht in der Union niedergelassene Verantwortliche (z.B. US-Firmen die Dienste in der Union anbieten)

EU-DSGV Rechte

- Rechte für Betroffene einer Verarbeitung personenbezogener Daten
  - Informationsrecht: sofort beim Erheben der Daten (Datenschutzerklärung)
  - Auskunftsrecht: Zweck, Kategorien von Daten, Speicherdauer, ….
  - Recht auf Löschung: Speicherung nicht mehr notwendig, Wiederruf
  - Recht auf Datenübertragbarkeit (z.B. von einem sozialen Netzwerk auf ein anders)

EU-DSGV Pflichten für Verantwortliche

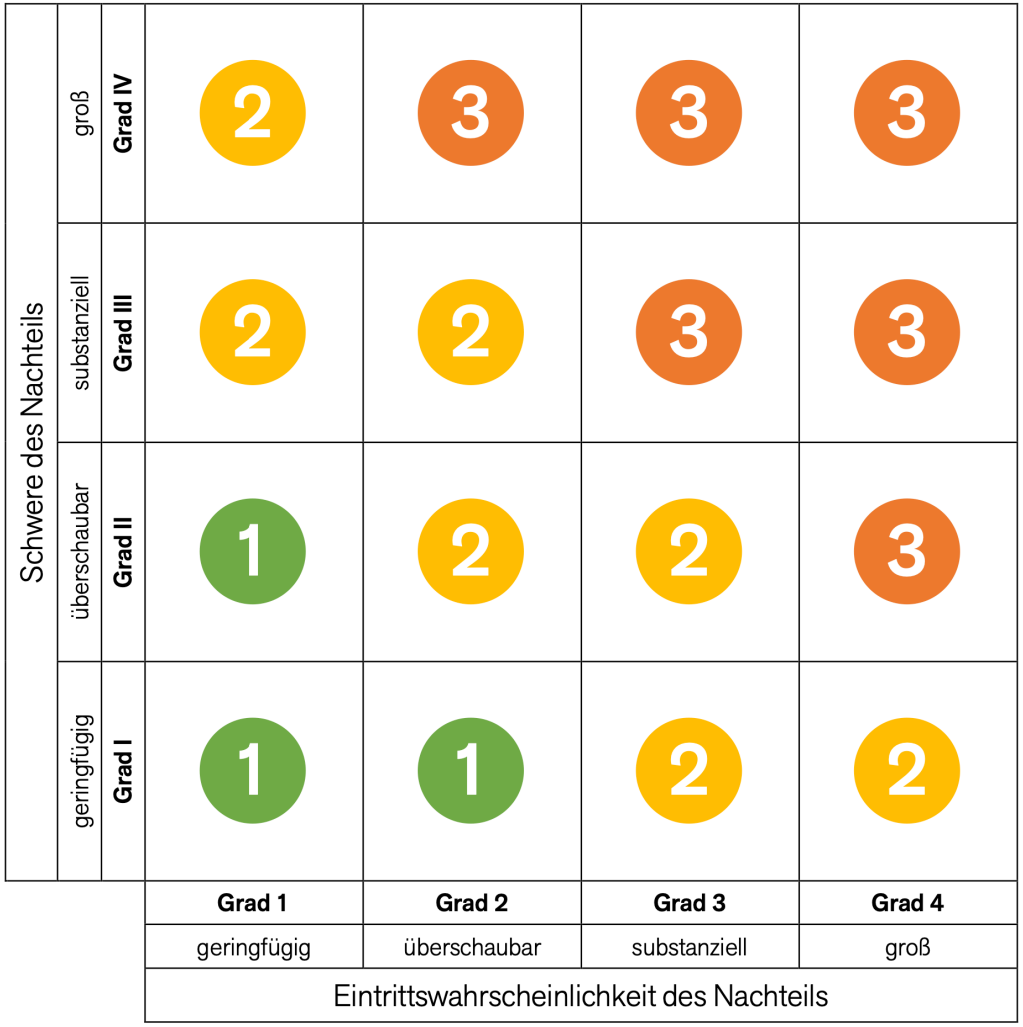
- Datenschutzfreundliche Voreinstellungen (data protection by default) Art. 25
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten (Art 30):
  - Kontaktdaten des DSB oder eines Verantwortlichen
  - Zweck der Verarbeitung
  - Fristen zur Löschung
  - Technische und Organisatorische Maßnahmen nach Art. 32
- Sicherheit der Verarbeitung (Art. 32)
  - Berücksichtigung des Stand der Technik
  - Risikoabschätzung mit angemessenem Schutzniveau
  - Pseudonymisierung und Verschlüsselung
  - Vertraulichkeit, Integrität, Verfügbarkeit u. Belastbarkeit der Systeme
  - Wiederherstellung
  - Regelmäßige Überprüfung der Wirksamkeit technischer und organisatorischer Maßnahmen

EU-DSGV Meldepflichten für Verantwortliche

- Meldung der Verletzung des Datenschutzes an Aufsichtsbehörde (Art. 33)
  - Unverzüglich und möglichst innerhalb von 72 Stunden
  - Beschreibung der Art der Verletzung
  - Name und Kontaktdaten des Datenschutzbeauftragten
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen
- Meldung der Verletzung des Datenschutzes an betroffene Person (Art. 34)
  - bei hohem Risiko für die Person unverzügliche Meldung
  - Benachrichtigung beschreibt in klarer und einfacher Sprache die Art der Verletzung personenbezogener Daten
  - Informationen nach Art. 33 Abs. 3 b bis d (s. oben)

Risikobasierte Entscheidung zur Meldung

- Bayerischer Landesbeauftragte für den Datenschutz gibt Orientierungshilfe heraus
  - Risikobasierter Ansatz in Abhängigkeit von:
    - der Schwere des Nachteils für Betroffene
    - Eintrittswahrschein-lichkeit des Nachteils



EU-DGSVO: Auskunftsrechte u. -pflichten

- Art. 12-15 EU-DGSVO
- Art 12: transparente Kommunikation, leicht verständlich
  - Verantwortlicher erleichtert Ausübung von Betroffenenrechten
  - Unverzügliche Auskunft, in jeden Fall innerhalb eines Monats
- Art 13, 14: Informationspflicht bei Erhebung PBD
  - Name des Verantwortlichen, DSB, Zweck der Verarbeitung
  - Dauer der Speicherung, Recht auf Löschung, Aufsichtsbehörde
- Art. 15: Auskunftsrecht der betroffenen Person
  - Recht auf Bestätigung ob PBD verarbeitet werden, falls ja:
  - Art der Daten, Verarbeitungszweck, Empfänger der Daten
  - Speicherdauer, Recht auf Berichtigung oder Löschung,
  - Beschwerderecht bei Aufsichtsbehörde
- Art. 16: Recht auf Berichtigung

EU-DSGV: Datenschutz-Folgenabschätzung

- Hat Form der Verarbeitung voraussichtlich hohes Risiko für Rechte und Freiheiten einer natürlichen Person so führt der Verantwortliche **vorab** eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge durch
- Folgenabschätzung mindestens erforderlich bei:
  - systematische und umfassende Bewertung persönlicher Aspekte, die sich auf automatische Verarbeitung oder Profiling gründet und als Grundlage für Entscheidungen dient die Rechtswirkung gegen Personen entfalten oder in ähnlich erheblicher Weise beeinflusst
  - Ausnahmetatbestände bei der Verarbeitung von Daten die grundsätzlich verboten ist: d.h. aus denen rassische u. ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit hervorgeht sowie genetische, biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung hervorgehen
  - systematische und umfangreiche Überwachung öffentlicher Bereiche

EU-DSGV: Datenschutz-Folgenabschätzung

- Enthält zumindest folgendes:
  - systematische Beschreibung, Zweck und verfolgte Interessen
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit auf den Zweck bezogen
  - Bewertung der Risiken für die Rechte und Freiheiten der Betroffen
  - Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen zur Bewältigung der Risiken und der Nachweis das EU-DSGV eingehalten wird

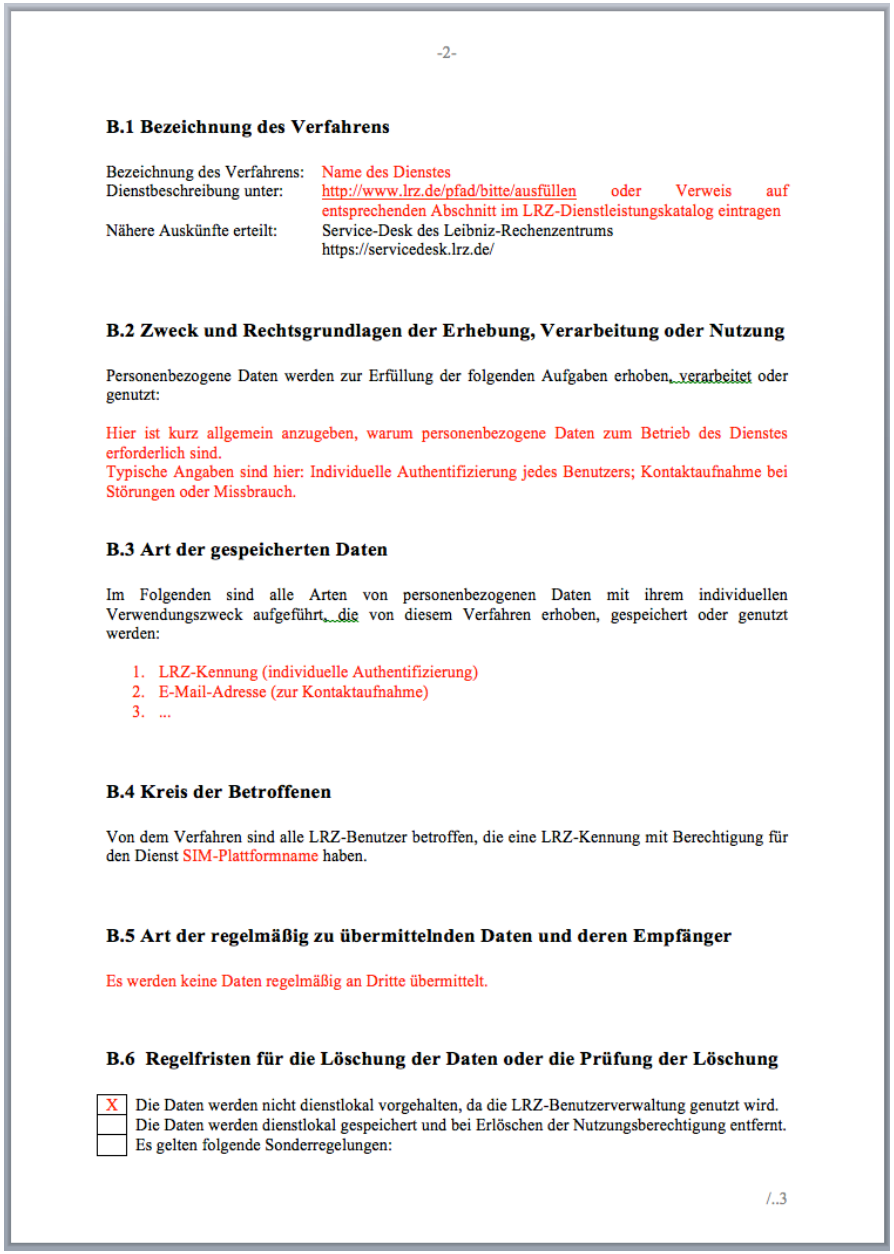
- Aufsichtsbehörde sind zu beteiligen
- Betroffene sind zu beteiligen

Typische Aufgabenbereiche eines Universitäts-DSB

- Videoüberwachung von Bereichen / Räumen
- Anwesenheitslisten und Notenaushänge
- Personal-, Studierenden-, Alumniverwaltungswerkzeuge
- Online-Learning Management Systeme (LMS)
- Nutzung von Cloud-Diensten (Office 365, Dropbox, LMS, …)
- Arbeitszeiterfassungssysteme, Schließsysteme
- Studierenden-/Mitarbeiterausweise
- BYOD, E-Mail-Weiterleitungen
- Telefonanlagen, elektronische Telefonbücher und Personenverzeichnisse
- Social-Media-Auftritte der Universität
- Forschungsprojekte (Medizin, Psychologie, …)
- Umfragen per E-Mail
- …

Beispiel: Verfahrensverzeichnis/-beschreibungen LRZ

Lfd. Nr.	Verfahrensbezeichnung	Stand V-Beschreibung
BAdW/LRZ		
1	Datensicherung und Archivierung	19.07.2013
2	Desktop Management	19.06.2013
3	DHCP-Server (Dynamic Host Configuration Protocol)	06.07.2012
4	DNS-Server	17.10.2012
5	Exchange	11.10.2013
6	Grid-Dienste	09.08.2012
7	High Performance Computing (HPC) Dienste	30.07.2012
8	Identity Management	10.10.2013
9	Intrusion Detection	10.07.2012
10	Modem-/ISDN-Einwahl	15.10.2012
11	Netzdokumentation	06.07.2012
12	Nyx	15.10.2012
13	Online-Speicher im MWN	20.06.2013
14	Secomat	10.07.2012
15	Security Information & Event Management (OSSIM)	12.08.2013
16	Service Desk und Incident Management	15.10.2012
17	Sharepoint	19.06.2012
18	Softwarelizenzierung	29.06.2013
19	Sophos-Antivirus	19.06.2012
20	Sophos-Antivirus (managed)	22.12.2012
21	Telefonanlage	20.06.2013
22	Virtuelle Firewalls	06.07.2012
23	VPN-Einwahl ins MWN	14.06.2012



-2-

B.1 Bezeichnung des Verfahrens

Bezeichnung des Verfahrens: Name des Dienstes
Dienstbeschreibung unter: http://www.lrz.de/pfad/bitte/ausfüllen oder Verweis auf entsprechenden Abschnitt im LRZ-Dienstleistungskatalog eintragen
Nähere Auskünfte erteilt: Service-Desk des Leibniz-Rechenzentrums https://servicedesk.lrz.de/

B.2 Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung

Personenbezogene Daten werden zur Erfüllung der folgenden Aufgaben erhoben, verarbeitet oder genutzt:

Hier ist kurz allgemein anzugeben, warum personenbezogene Daten zum Betrieb des Dienstes erforderlich sind.
Typische Angaben sind hier: Individuelle Authentifizierung jedes Benutzers; Kontaktaufnahme bei Störungen oder Missbrauch.

B.3 Art der gespeicherten Daten

Im Folgenden sind alle Arten von personenbezogenen Daten mit ihrem individuellen Verwendungszweck aufgeführt, die von diesem Verfahren erhoben, gespeichert oder genutzt werden:

1. LRZ-Kennung (individuelle Authentifizierung)
2. E-Mail-Adresse (zur Kontaktaufnahme)
3. ...

B.4 Kreis der Betroffenen

Von dem Verfahren sind alle LRZ-Benutzer betroffen, die eine LRZ-Kennung mit Berechtigung für den Dienst SIM-Plattformname haben.

B.5 Art der regelmäßig zu übermittelnden Daten und deren Empfänger

Es werden keine Daten regelmäßig an Dritte übermittelt.

B.6 Regelfristen für die Löschung der Daten oder die Prüfung der Löschung

[X] Die Daten werden nicht dienstlokal vorgehalten, da die LRZ-Benutzerverwaltung genutzt wird.
[ ] Die Daten werden dienstlokal gespeichert und bei Erlöschen der Nutzungsberechtigung entfernt.
[ ] Es gelten folgende Sonderregelungen:

/..3

Vertrag zur Verarbeitung im Auftrag (VVA)

- Outsourcing: VVA liegt vor, wenn eine andere Stelle im Auftrag Daten speichert und verarbeitet.
- Beispiel: LMU, TUM, HM, … nutzen E-Mail-Dienst des LRZ
- Verantwortung i.S.d. DSG verbleibt beim Auftraggeber (AG)
- AVV-Vertrag regelt u.a.:
  - Zweck und Umfang der AVV
  - Technische und organisatorische Sicherheitsmaßnahmen beim Auftragnehmer (AN)
  - Berichts- und Kontrollpflichten
  - Einbezug von Subunternehmern
  - Weiterleitung von Daten in Drittländer
- AVV: AG erteilt Weisungen an den AN
- Alternative: Funktionsübertragung statt AVV — AG gibt Verantwortung an AN ab, verliert aber Kontrollmöglichkeiten
- Alternative: gemeinsame Verantwortung für die Daten

Exemplarische Regelungen am LRZ

- Gleitlöschung von Protokolldateien
  - Default: 7 Tage
  - Ausnahmen z.B. Greylisting 36 Tage, Bandarchivierung 1 Jahr
  - Kopieren und Aufbewahren von Auszügen bei Anfragen von Ermittlungsbehörden (nicht Privatpersonen; keine sofortige Herausgabe)
- Entsorgung von Datenträgern
  - Schreddern von Papier entsprechend Stufe 4 nach DIN 32757
  - Physische Vernichtung von Festplatten und anderen Datenträgern
- Z.T. Aufzeichnung von Administratortätigkeiten, Auswertung nur anlassbezogen mit Vier-Augen-Prinzip
- Jährliche Schulung, schriftliche Verpflichtung von Administratoren auf das Datengeheimnis (§ 5 BDSG)

Inhalt von Kapitel 5

1. Strafgesetzbuch (StGB)
2. Datenschutz (BDSG, BayDSG)
3. IT-Sicherheitsgesetz

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

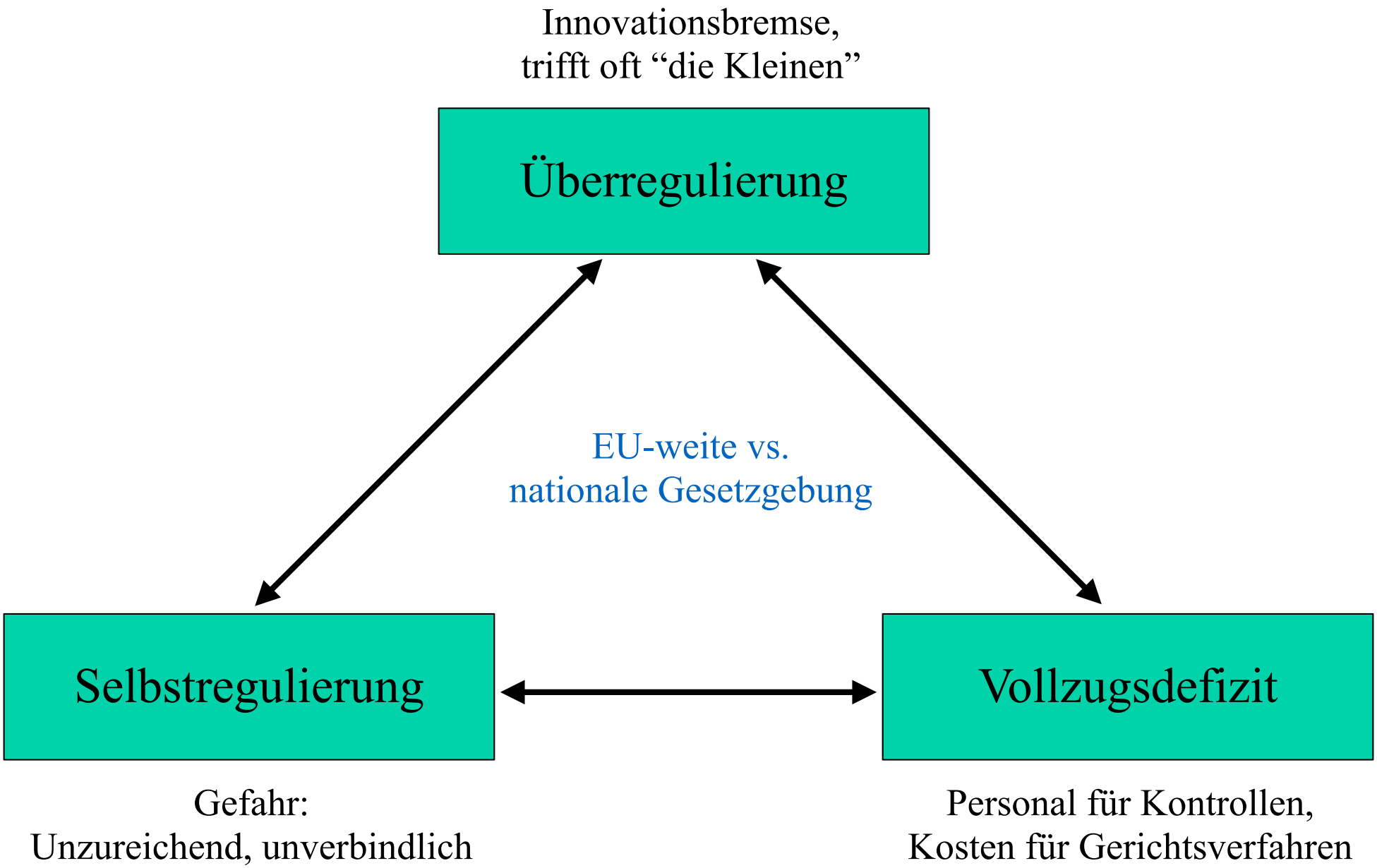
- In Kraft seit 07/2015, Bußgelder bis 100 T€ bei Verstoß

- Auswirkungen:
  - Webserver-Betreiber wie Online-Shops müssen Kundendaten “nach Stand der Technik” schützen.
  - Internet-Provider müssen auf Botnet-Infektionen hinweisen.
  - “Freiwillige Vorratsdatenspeicherung” zur Störungsabwehr (3T-6M)
  - AKW-Betreiber und TK-Anbieter müssen “erhebliche” IT-Sicherheitsvorfälle melden. (Wird noch ausgedehnt auf weitere sog. kritische Infrastrukturen, u.a. Banken, Krankenhäuser, …)

- Rolle des BSI wird gestärkt:
  - Mehr Personal und Schnittstellen zu anderen Behörden
  - Anordnungsbefugnis ggü. Produkt-/Systemherstellern, z.B. Patches

- Karenzzeit 2 Jahre, Evaluation des Gesetzes nach 4 Jahren

Spannungsfeld Gesetzgebung



Vormals freiwillige Meldung bei der Allianz für Cybersicherheit

Meldeformular für Cyber-Angriffe

Die Meldung erfolgt durch das Ausfüllen des unten folgenden Webformulars:

Alternativ können Meldungen auch direkt per E-Mail an die Meldestelle Meldestelle@bsi.bund.de gesendet werden.

Angaben zum Unternehmen

Branche:

Ich bin mir bewusst, dass - falls ich keine Kontaktdaten angebe und meine gemachten Angaben nicht plausibilisiert werden können - das BSI entscheiden kann, diese nicht für eine Lagebewertung / Reaktion zu verwenden.
Kontaktdaten werden ausschließlich für Rückfragen seitens des BSI genutzt.
Nach Erstellung des Lagebildes werden die Daten gelöscht.

Unternehmensgröße:

Unternehmensname:

Name des Melders:

Rolle im Unternehmen:
CIO
CISO
Administrator
Information Security Manager

E-Mail

Public-PGP-Key:

Angriffs-Detektionsmethode und Zeitpunkt

Der Angriff wurde festgestellt durch:
- Systemausfall
- Fehlverhalten von Systemen
- Auswertung von Log-Daten
- Veröffentlichung von gestohlenen Informationen durch Dritte
- Hinweise von Dritten
- Vertrauliche Informationen wurden in einer Dropzone gefunden
- Sonstiges:

Der Angriff fand vermutlich statt:

Zeitraum & Dauer:

Bei mehrfachen Angriffen bitte vermutete Anzahl eingeben:

Häufigkeit:

Beschreibung des Angriffs

Angriffsmethoden:
- Denial-of-Service Angriff
- Schadsoftware: Malwareverteilung über Email
- Schadsoftware: Malwareverteilung über Webseiten
- Schadsoftware: Malware-Infiltration über mobile Devices
- Schadsoftware: Mareware-Infiltration über USB-Medium
- Schadsoftware: Malwareverteilung über anderen oder unbekannten Infektionsvektor
- Identitätsdiebstahl: Phishing / Man-in-the-Middle-Angriff / Spoofing / Pharming / Andere
- Hacking: Injection-Angriff
- Hacking: Cross-Site-Scripting, Cross-Site-Request-Forgery
- Hacking: Andere
- Hacking: Missbrauch von Passwort-Zurücksetzen-Funktionen
- Spionage: Mitlesen (unverschlüsselter) Datenübertragung
- Ausnutzung einer Sicherheitslücke oder Schwachstelle in einem IT-Produkt
- Manipulation von Hardware
- Sonstiges:

Vermutete Angriffsmittel:
- Hacking
- Botnetz
- Trojanisches Pferd
- Unterstützt mit Social Engineering
- Sonstiges:

Vermutete Angriffsart:

Vermutete Täter:
- Unbekannter Täterkreis
- Innentäter
- Script-Kiddies
- Cyber-Aktivisten (vgl.Anonymous)
- Cyber-Kriminelle
- Wirtschaftsspionage
- Fremdstaatlicher Nachrichtendienst
- Sonstiges:

Angriffszweck:
- Erpressung
- Identitätsdiebstahl
- Entwendung vertraulicher Informationen
- Störung der Geschäftstätigkeit des Unternehmens
- Sabotage/Denial-of-Service
- Manipulation von Daten
- Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server)
- Defacement
- Sonstiges:

Näheres zum Angriff:

Weitere freiwillige Angaben

Entstandener Schaden:
- Es ist kein Schaden eingetreten
- Erpressungsgeld wurde gezahlt
- IT-Systeme sind ausgefallen
- Wiederherstellungsaufwand durch Bereinigung/Wiederaufsetzen der Systeme
- Folgeschäden aufgrund entwendeter Informationen werden erwartet
- Es bleibt unklar, ob sämtliche Malware gefunden/eliminiert wurde
- Renommee-Verlust
- Es waren Leib und Leben gefährdet
- Sonstiges:

Externe Unterstützung:
- Externe Forensik-Spezialisten wurden hinzugezogen
- Penetrationstest ist nach dem Angriff durchgeführt worden

Strafanzeige wurde gestellt:

Täter wurde ermittelt:

Weitere Angaben:

Quelle: https://www.allianz-fuer-cybersicherheit.de/

Zusammenfassung

- Gesetzgebung bzgl. IT-Sicherheit zunehmend komplexer
  - Grundlegende Kenntnisse für Informatiker wichtig
  - Je nach Tätigkeit: Professionelle juristische Unterstützung unverzichtbar

- Zielsetzungen partiell konfliktär, z.B.

  Möglichst viele Informationen speichern,
  um Vorfälle aufklären zu können

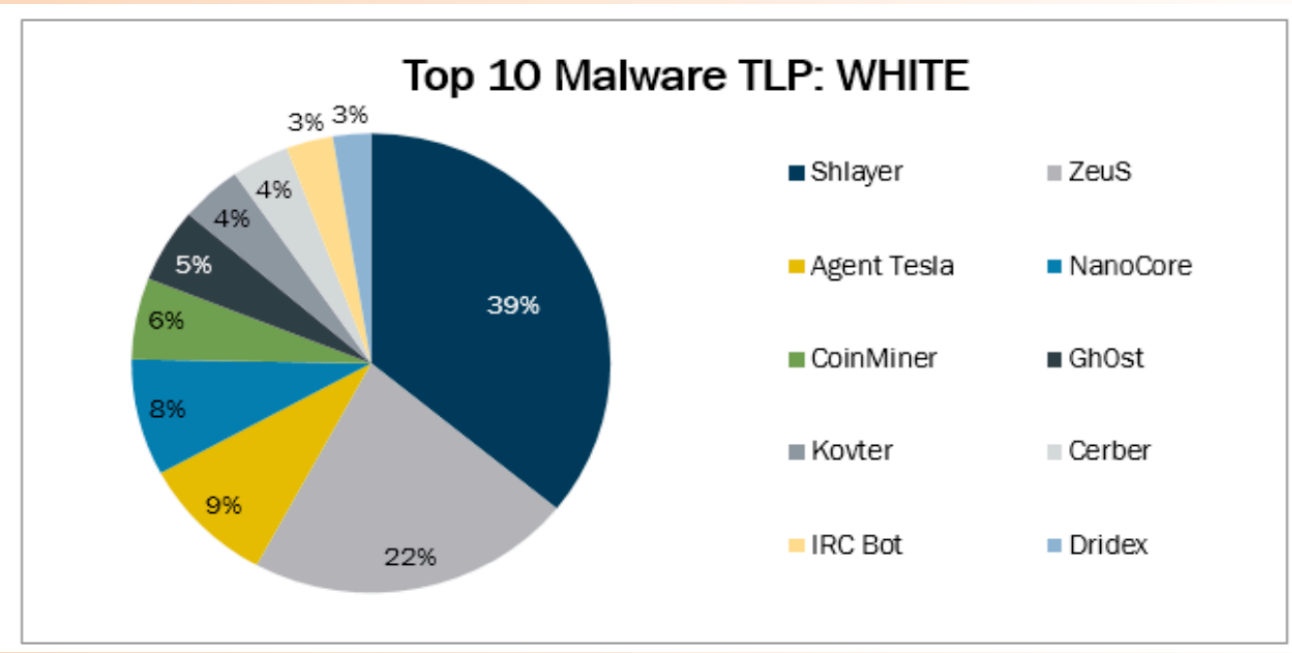
  vs.

  Datenvermeidung i.S.d. Datenschutzes

- Recht vs. Gerechtigkeit:
  - Dauer bis zum Inkrafttreten neuer Gesetze, Karenzzeiten
  - Einflussnahme durch Lobbyisten
  - Umsetzungs- und Kontrolldefizite
  - Rechtssicherheit vs. unerwartete Gerichtsurteile

US-Cert: Alert AA20-345A

- Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data
  - Targeting Kindergarten to 12th grade (K-12) educational institutions
- Threats:
  - Ransomware - School Systems and distance learning systems
    - Top 5: Ryuk, Maze, Nefilim, AKO, and Sodinokibi/REvil.
  - Malware - Top 10



US-Cert: Alert AA20-345A

- Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data
- Threats:
  - Ransomware - School Systems and distance learning systems
  - Malware
  - DDoS - distance learning systems
  - Video Conference Disruption
    - Using student names to trick hosts
    - Accessing via publicly available links
    - Students sharing links/passwords with friends
  - Social Engineering
    - Requesting personally identifiable information (PII) and passwords
    - Domain Spoofing, Homograph Attacks, Phishing, etc.
  - Exploit Data
  - End of Life Software exploited by cyber actors

US-Cert: Alert AA20-345A

- Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data
- Mitigations:
  - Plans and Policies
    - Business continuity plan, patch plan, security plan
  - Best Practices
    - Patch
    - Check configuration
    - Regularly change passwords
    - Multi factor authentication
    - Audit accounts and logs
    - Scan for open ports
    - Identify critical assets
    - Antivirus and anti-malware solutions
    - Awareness and training
    - Ransomeware: do not pay

US-Cert: Alert AA20-345A

- Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data
- Mitigations:
  - Best Practices
    - Back up data regularly - protect backups offline
    - Partnership with ISP to prevent DoS
  - Videoconferencing Best Practices
    - Use most updated versions of software
    - Password for session access
    - Avoid password sharing
    - Establish vetting process - waiting room
    - Participants should use real names not aliases
    - Only host controls screen sharing privileges
    - No entering prior to host
    - If host exits all participants exit