Privacy by Design
Privacy by Default

Prof. Dr. Sachar Paulus

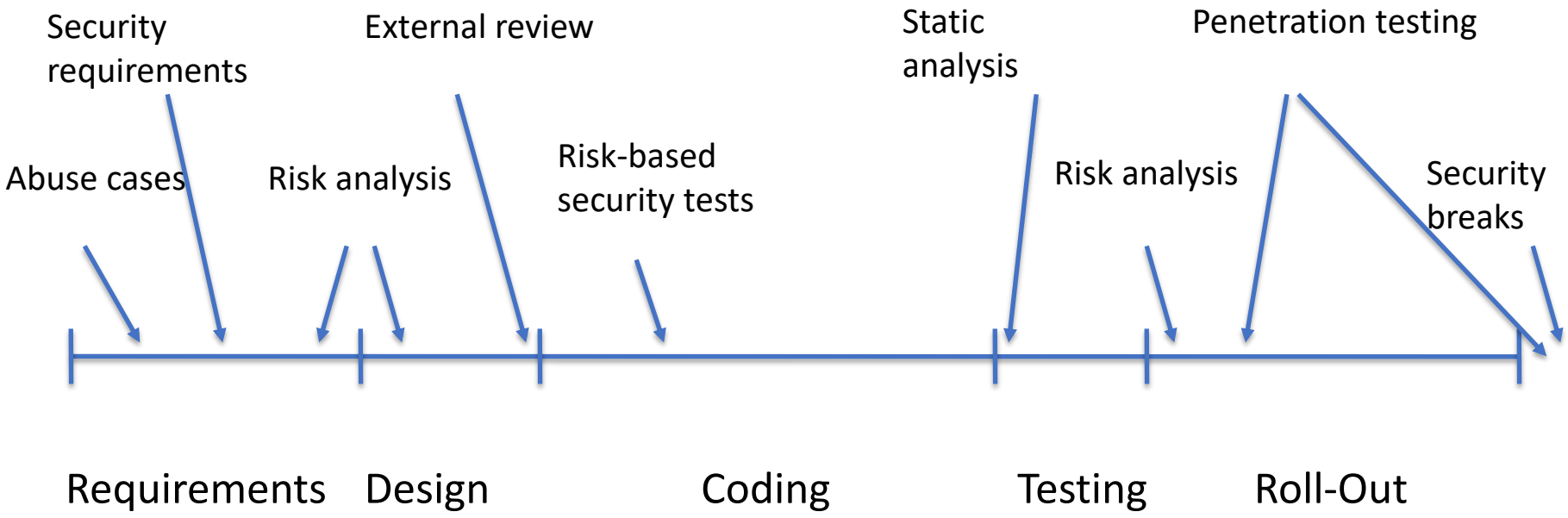
Privacy by Design

- Bundesbeauftragte für den Datenschutz: *“…etwaige Datenschutzprobleme schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen und den Datenschutz von vorneherein in die Gesamtkonzeption einzubeziehen anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme zu beheben. Dieser Ansatz wird als “Privacy by Design”(PbD) bezeichnet*.”

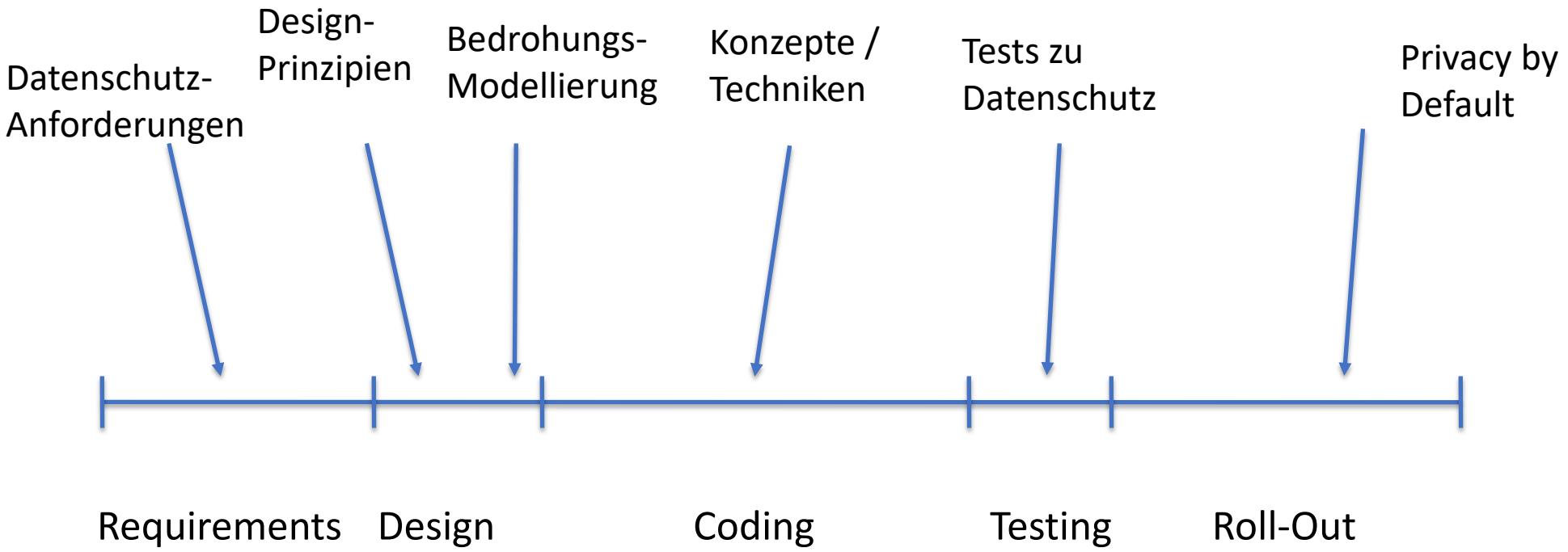
Software-Entwicklungs-Prozesse

Alle Software-Entwicklungs-Methodiken enthalten die folgenden Schritte:

Security Touch Points



Privacy Touch Points



Datenschutz-Anforderungen an Software

Funktional

- Einwilligungserklärung
- Einflussmöglichkeit auf Datenspeicherung durch Betroffene
- Alternative Prozesse, wenn keine Einwilligung gegeben
- Portabilität: Daten über Personen müssen in gängigem Format übergeben werden
- Löschkonzept

Nicht-funktional

- Korrektheit
- Integrität
- Vertraulichkeit
- Minimalität der Daten

Design-Prinzipien

Security

- Need-to-know
- Keep it simple
- Defence in depth
- Least privilege
- Secure input and output handling
- No security by obscurity
- No back doors
- Fail safe

Privacy

- Daten-orientierte Architektur
- Datenminimierung
- Nur anzeigen, was erlaubt ist
- Nach Zweck getrennte Verarbeitung
- Zweckbindung
- Aggregation auf höchstmöglicher Ebene

Bedrohungsmodellierung

- Voraussetzung: grobe Architektur
- Identifizieren von potenziellen Datenlecks
  - Durch Brainstorming und Rollenspiele
  - Alternativ: Datenflussdiagramme
- Bewertung von Angriffen an Eintrittswahrscheinlichkeit und Schaden (= risikobasierter Ansatz)
- Identifizieren von Maßnahmen (= zusätzliche Anforderungen)

- Input für eine Datenschutzfolgeabschätzung!

Konzepte/Techniken für die Software-Entwicklung

- Starke Authentifizierung
- Delegation der Authentifizierung
- Attribute Based Credentials (= Token-basiert, erlaubt Pseudonymisierung)
- Verschlüsselung der Kommunikation
- Verschlüsselung der Ablage
- Anonyme Kommunikation (Mixe, Onion Routing, …)
- Datenbanken: Respondent Privacy – Owner Privacy – User Privacy

Datenschutz bei Datenbank-Anwendungen („Big Data“)

- Respondent Privacy
  - Ziel: Schutz vor der Identifikation von „Befragten“ (= Respondents) – aus Profildaten Rückschluss auf Person ziehen
  - Methoden: Statistical Disclosure Control (Schutz in der Tabelle, Schutz bei den Zugriffen, Schutz von Mikrodaten (Maskierung – Synthese)).
- Owner Privacy
  - Ziel: Zugriff auf fremde Datenbanken, so dass ausschließlich die abgefragte Information (ohne Personenbezug) übermittelt wird
  - Methoden: Privacy Preserving Data Mining (Random Perturbation, Secure Multiparty Computation)
- User Privacy
  - Ziel: Schutz vor der Identifikation von zugreifenden Nutzern
  - Methoden: Private Information Retrieval

Testen

- Aus den Datenschutz-Anforderungen entsprechende Tests erzeugen
- Tests durchführen und dokumentieren

Privacy by Default

- *“…Privacy by Default heißt übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“ und bedeutet, dass die Werkeinstellungen datenschutzfreundlich auszugestalten sind. Nach dem Grundgedanken sollen insbesondere die Nutzer geschützt werden, die weniger technikaffin sind und z.B. dadurch nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen.* “ (intersoft consulting services ag)
- Wir betrachten Aktivitäten zwischen Softwaretest und Betrieb

Transfer

- Übliche Schutzmechanismen zur Vermeidung von Manipulation
- Hash-Erstellung, Signierung von Dateien etc.

Installation und Konfiguration

- Sichere Installation: keine PC-Administrationsrechte erforderlich, separate Berechtigung für Administratoren für diese Anwendung, Einschränkung der Berechtigungen des Service Users.
- Sichere Konfiguration: Abschalten von nicht benötigen Diensten, Konfiguration von Sicherheitseinstellungen.
- Datenschutzfreundliche Konfiguration: Sofern vorhanden, Einstellungen im Hinblick auf Datensparsamkeit und Löschung von Daten vornehmen.

Datenversorgung

- Sichere Übertragung der in das System einzuspielenden Daten
- Für Tests keine echten personenbezogenen Daten verwenden!
  - Statt dessen Pseudonymisierung

Vor der Inbetriebnahme

- Technische und Organisatorische Maßnahmen vorhanden und angemessen?
  - Datenschutz-Audit durchführen und dokumentieren
- Datenschutzerklärung vorbereiten
- Dokumentation zur Transparenz (für die Nutzer) erstellen
- Meldeprozess bei Datenpannen festlegen
- Datentransfer ins Ausland angedacht? Betriebstätte im Ausland?
  - Besonderheiten klären
- Auftragsdatenverarbeitung klären!
- Verfahrensverzeichnis erstellen

Privacy by Design
Privacy by Default

Prof. Dr. Sachar Paulus

Fragen der Teilnehmer: Projekt DISTELL, Hochschule Esslingen

- Aus der Online-Befragung unseres ersten Projektes wird von Lehrenden der Datenschutz als Hemmnis benannt, um digitale Lernelemente einzusetzen oder digitale Lehrformate durchzuführen. Gerne würden wir Informationen aufbereiten, um sie an der Hochschule Esslingen multiplizieren zu können.
- Unsicherheit besteht zudem mit der Verwendung von YouTube, Skype etc. also eher aus der privaten Nutzung vertrauter Social Media. Können Sie eingesetzt werden oder bestehen (Landes-) Reglementierungen? Dazu zählen auch Blogs, was gilt es in der Nutzung von Blog, wenn sie nicht über die Lernplattform der Hochschule laufen, für Richtlinien?
- Datenschutz im Rahmen von Online-Befragungen: welche Daten (auch von Lehrenden) können erhoben werden? Was sind nach dem Landesdatenschutzgesetz Baden-Württemberg auszuschließende Daten?

Fragen der Teilnehmer: Projekt MoMoViLab, Universität Ulm

- Wie können/dürfen virtuelle Maschinen (VMs) genutzt werden, wenn personenbezogene/sensible Daten (in unserem Fall: Prüfungs(vor)leistungen) gespeichert und verarbeitet werden sollen? Bei uns werden speziell VMs innerhalb der bwCloud eingesetzt.
- Haben andere Projekte ebenfalls solche Fragestellungen und wie gehen sie damit um?

Fragen der Teilnehmer: Projekt MyMi.mobile, Universität Ulm

- Datenschutzkonzept
- Datenschutz und learning analytics
- Datenschutz bei der Speicherung vieler Daten "Big data" und Tracking/Logfiles

Fragen der Teilnehmer:
Projekt LAPS, Hochschule der Medien

- Erstellung einer Einverständniserklärung zur Nutzung der Daten.
- Kontext: Verwendung der pers. Studierendendaten zur Berechnung von Risiko- bzw.Erfolgswahrscheinlichkeit des Studienverlaufs als Grundlage für eine freiwillige Beratung

Fragen der Teilnehmer:
Projekt Digitaler Lerngarten, Univ. Hohenheim

- Bewegungsdaten von Studierenden, da sie im Projektvorhaben mittels GPS an verschiedene Lernorte geführt werden.
- Frage: wie ist das aus datenschutzrechtlicher Sicht in Bezug auf Rückverfolgung bzw. welcher Studi war wann, an welchem Ort usw. zu sehen?

Fragen der Teilnehmer: Projekt ZOERR, Univ. Stuttgart, HAW Reutlingen, Univ. Freiburg

- Neue Anforderungen an ein Verfahrensverzeichnis (falls es das so dann noch gibt)
- Datenschutz im Zusammenhang mit der Versionierung und anderen Metadaten zum Lebenszyklus
- Datenschutz ist in unserer Arbeit als E-Learning Serviceeinrichtung ein permanentes Thema, im Kontext Umgang mit Studierendendaten auf Lernplattformen, im Zusammenhang mit Online-Evaluation, Nutzung externer (Social Media) Plattformen oder auch im Zusammen der Nutzung mit Apps etc. Im Zusammenhang mit dem konkreten Projekt des OER-Repositoriums habe ich aktuell keine spezifische Frage.

Literatur

- https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/
- https://www.enisa.europa.eu/publications/big-data-protection
- https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_6.pdf
- http://ec.europa.eu/newsroom/document.cfm?doc_id=47711
- https://www.amazon.de/Datenschutz-Grundverordnung-mit-Bundesdatenschutzgesetz-Heidelberger-Kommentar/dp/3811446649/
- https://www.amazon.de/Basiswissen-Sichere-Software-Weiterbildung-Professional/dp/3898647269/