Bundesamt
für Sicherheit in der
Informationstechnik

Rechtssicheres dokumentenersetzendes Scannen
Entwicklung einer Technischen Richtlinie

(TR RESISCAN)

Dietmar Lorenz

Bundesamt für Sicherheit
in der Informationstechnik in Bonn
Referat C12 - Cyber-Sicherheit in kritischen IT-Systemen, Anwendungen und Architekturen

Berlin - 23. September 2011
Informationstag "Elektronische Signatur“ - Gemeinsame Veranstaltung von TeleTrusT und VOI

AUSGANGSLAGE

- **Fortschreitende Digitalisierung** der Verwaltungsvorgänge
- Zunehmender Einsatz von **E-Vorgangsbearbeitungssystemen**
- **Rechtsvorschriften**, die die **elektronische Aktenführung** zulassen oder vorschreiben
- **Hohe finanzielle und organisatorischen Belastung**
- **Bedarf an Lösungen,** die eine Vernichtung des Originals bei gleichzeitiger Wahrung der Rechts- und Beweissicherheit ermöglichen

AUSGANGSLAGE

Rechtliche Aspekte

- **Technisch:**
  - Umwandlung von analogen in elektronische Daten
  - Mediumwechsel von Papier zu elektronischen Datenspeichern

- **Rechtlich bedeutsam:**
  die dem Papier immanenten Sicherheitsmerkmale zum Integritäts- und Authentizitätsschutz gehen verloren

- **drei Fragen:**
  - **(1)** Ist das ersetzende Scannen zulässig im Hinblick auf die gesetzlichen oder vertraglichen Dokumentations-, Aktenführungs- und Aufbewahrungspflichten
  - **(2)** rechtliche und technische Anforderungen an den Scanprozess und das Scanprodukt
  - **(3)** Beweiswirkung des Scanproduktes in einem Gerichtsverfahren

RECHTLICHE AUSGANGSLAGE (Status Quo)

Anwendungsgebiete, die ein ersetzendes Scannen ausdrücklich erlauben:

- **Gerichtsakten** (§ 299 ZPO für Prozessakten; §298 ZPO für eingereichte Dokumente)
- **Verwaltungsunterlagen** (§ 6 RegR für Dokumente der Bundesministerien)
- **Sozialversicherungsunterlagen** (§ 110a Abs. 2 SGB IV; Sondervorschrift § 110d SGB IV für Dokumente, die der öffentlich rechtlichen Verwaltungstätigkeit zugrunde liegen)
- **Röntgendokumentation** (§ 28 Abs. 4 RöntgenVO)
- **Kaufmännische Buchführungsunterlagen** (§ 239 Abs. 4 HGB für Handelsbücher; § 257 Abs. 3 HGB für sonstige Unterlagen)
- **Besteuerungsunterlagen** (§ 147 Abs. 2 AO).

RECHTLICHE AUSGANGSLAGE (Status Quo)

Rechtlichen Anforderungen an den Scanprozess und das Scanprodukt:

- **Bildliche** und **inhaltliche** Übereinstimmung zwischen dem Papieroriginal und Scanprodukt
- Übereinstimmungsnachweis
- Schutz vor Informationsveränderungen und Informationsverlusten
- Dauerhafte Datenträger
- **Ausnahme**: qualifizierte elektronische Signatur (§ 110d SGB IV)

PROJEKTZIELE

Technische Richtlinie soll

- **funktionale** Anforderungen spezifizieren
- **organisatorische** und **technische** Maßnahmen definieren
- **Sicherheitsziele**: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Vollständigkeit, Nachvollziehbarkeit, Lesbarkeit, Verkehrsfähigkeit und Löschbarkeit
- durch **Prüfkriterien** die objektive Beurteilung der Ordnungsmäßigkeit eines Scan-Verfahrens sicherstellen
- **Anwendern** erleichtern, adäquate Scanlösungen einzusetzen
- **Herstellern** sowie Dienstleistern notwendige Spezifikationen liefern

GEFÄHRDUNGSLAGE

Bedrohungen und Angriffsrisiken für den Scanvorgang

- höhere Gewalt
- organisatorische Mängel
- menschliches Fehlverhalten
- technisches Versagen
- vorsätzliche Angriffe von Außentätern / Innentätern
- primär bedrohte Schutzziele: **Integrität** und **Vertraulichkeit**

MÖGLICHE SICHERHEITSMASSNAHMEN

- Gegenmaßnahmen unter Berücksichtigung der **IT-Grundschutzkataloge**
- Schutz vor **Informationsverlust** (Informationsgehalt und Erscheinungsbild)
- zuverlässiges **Personal** / Schulung und Sensibilisierung der Mitarbeiter
- sichere Technische Schnittstellen zur **Datenübergabe** (s. TR-ESOR)
- geeignete **Signaturformate** und Hashalgorithmen
- Umsetzung von **Zugriffs-** und **Rollenkonzepten**
- Zutritts- und **Zugangskontrolle** für Scansystem
- sichere, verschlüsselte **Übertragungswege**
- **Signatur-** und **Zeitstempeldienste**

ERHÖHUNG von INFORMATIONSSICHERHEIT & RECHTSSICHERHEIT

Technisch

- **Konformitätsbewertung** im Rahmen einer Zertifizierung durch das BSI:
  - Objektive Beurteilung durch unabhängige **Prüfkriterien**
  - **Standardisierte Vorgehensweise** beim ersetzenden Scannen
- Empfehlung für Ausschreibung und Beschaffung (Anwender)
- Spezifikation für Produkte und Lösungen (Hersteller)

Rechtlich

- **Referenzpunkt** für künftige Rechtsvorschriften
- Empfehlung des BSI als **Vertrauensanker**

PROJEKTMETHODIK

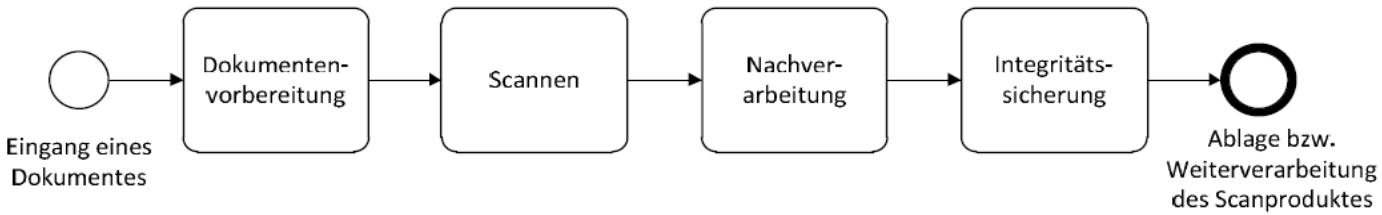
- **Strukturanalyse**
- **Schutzbedarfsanalyse**
- **Bedrohungsanalyse**
- **Risikoanalyse**
- **Sicherheitsmaßnahmen**

ENTSCHEIDUNGSMATRIX (Entwurf)

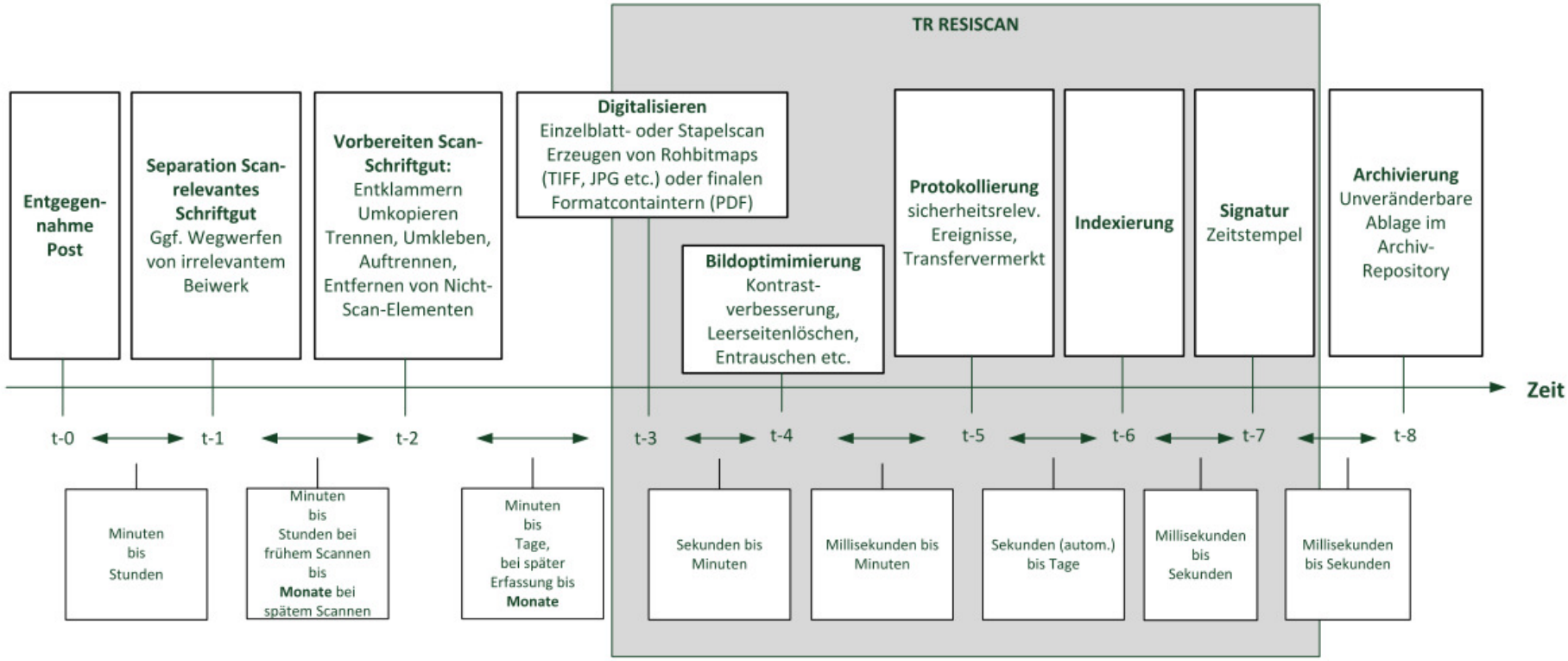
Module / Schutzziele	Technische Module							Organisatorische Module	
	Sichere Netz-an-bind-ung	Raum-zugangs-kontrolle	Signatur für ge-scannt-en Stapel	Signatur für einzelne Doku-mente	Verifi-zierung durch Einzel-sicht-prüfung	Überein-stimm-ungs-vermerk „Beglau-bigung“	Langzeit-archivier-ungs-sicheres Speicher-format	Arbeits-anweisung	
Phase 1: Vorbereitung des Originaldokuments									
räumliche Sicherheit der Scanstelle		X						X	
Phase 2: Funktionalen Anforderungen an den technischen Scanvorgang selbst									
Schutz vor Datenverlust	X						X		
Phase 3: Gewährleistung der Echtheit des Scanprodukts									
Basis-Integritätsschutz	X		X						
Hoher Integritätsschutz	X			X	X		X		
Sehr hoher Integritätsschutz	X			X	X	X	X		

GENERISCHER SCANPROZESS

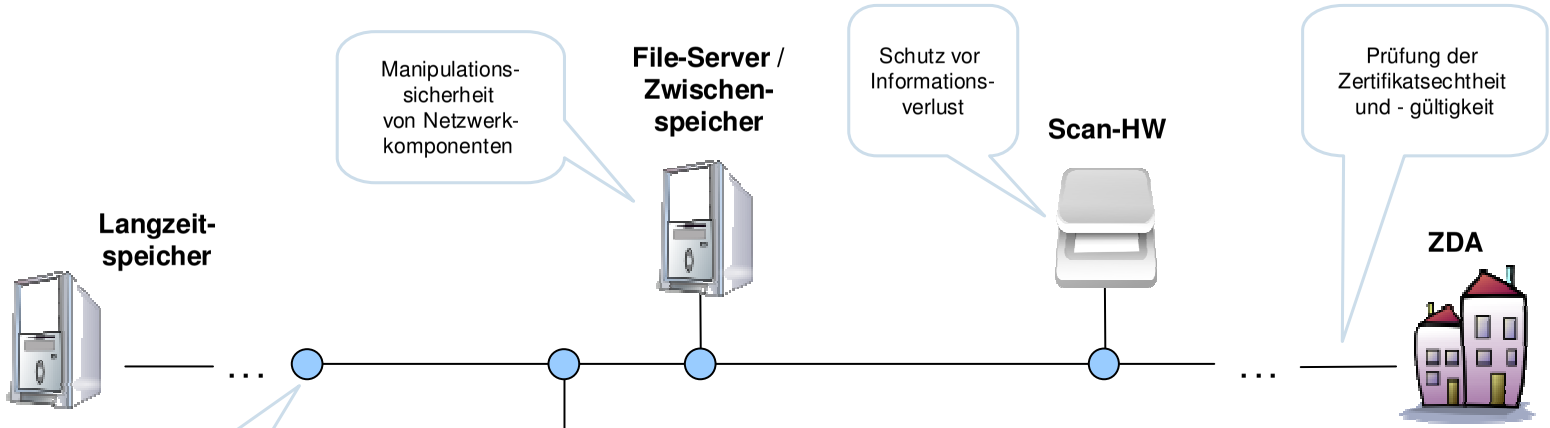
- Bedrohungs- und Risikoanalyse orientiert sich am **„generischen Scanprozess“**
- **Abgrenzung** der TR durch klar definierte Schnittstellen
- **Zuständigkeit** der TR
  - beginnt beim Eingang des Dokuments und
  - endet an der Schnittstelle zu einem DMS, VBS oder Langzeitspeicher



PROJEKTGRENZEN



SICHERHEITSANFORDERUNGEN an den SCANPROZESS



Scan-Hardware (Scan-HW)
Scan-Bibliothek (Scan-Lib)
Sichere Signaturerstellungseinheit (SSEE)
Signaturanwendungskomponenten (SAK)
Zertifizierungsdiensteanbietern (ZDA)

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat C12 –
Cyber-Sicherheit in
kritischen IT-Systemen, Anwendungen und Architekturen

Godesberger Allee 185-189
53175 Bonn

Dr. Astrid Schumacher
Dietmar Lorenz

astrid.schumacher@bsi.bund.de
dietmar.lorenz@bsi.bund.de